SECURITY CONSIDERATIONS FOR MOBILE EDGE COMPUTING

Rajeev Shorey (PhD)
Fellow INAE, Distinguished Scientist ACM
Distinguished Lecturer, IEEE Future Networks TC

CSE Department
Indian Institute of Technology, Delhi
India

LSU
16 November 2023
IEEE Future Networks – FutureNetworks.ieee.org

Collaboration

Content

Events

Research & Education

IEEE Future Networks Tech Focus Issue 16, June 2023

+ technical newsletter, podcasts, videos, articles

IEEE Future Networks World Forum 2022

+ more!

IEEE INGR International Network Generations Roadmap

+ eLearning, webinar series, white papers, tutorials

Join today! bit.ly/fntc-join
IEEE Future Networks

Be connected to IEEE Future Networks to shape future network requirements

Get monthly updates on technical workshops, summits, webinars, podcasts, and call for proposals, papers, and volunteer opportunities

Thousands are already members

Join today: bit.ly/fntc-join
Agenda of the Tutorial

- Introduction & Motivation
- Mobile Edge Security (MEC)
- MEC Architecture
- Security issues in Emerging Edge Paradigms
  - Federated Learning
  - Reinforcement Learning
- Summary and Future Directions
The Buzz on Edge Computing

Edge Computing | News, how-tos, features, reviews, and videos

IBM, Bharti Airtel partner on edge cloud offerings in India

McLaren Racing relies on edge computing at Formula 1 tracks
McLaren's Formula 1 racing team securely delivers apps and data to track crews and guests via VMware Workspace ONE.

HPE to ship a dedicated inference server for the edge
The small form factor HPE Edgeline EL8000 is designed for AI tasks such as computer vision and natural-language processing.

Cloud computing is reinventing cars and trucks

Why edge computing matters for modern software development
The next stage of cloud computing brings computing power closer to users, paving the way to better user experiences and more intelligent applications.
Edge Computing Spend

- Report by Market research firm IDC

- Edge computing spend is expected to surpass $300 billion by 2026, with a compound annual growth rate of 15% during the three year period

- Edge computing spend to be $208 billion in 2023, a 13.1% increase on 2022 spend!
The three broad use cases include enhanced mobile broadband, mission-critical services and massive IoT.

The three broad use cases are characterized by different metrics and parameters.

Ref: Leading the World to 5G, Qualcomm Technologies, Inc, 2016
The Edge Nodes Play a Key Role in Enabling 5G
The 5G Architecture

5G ARCHITECTURE
DISTRIBUTED CORE, MESH CONNECTIVITY
Edge Computing: Key Advantages

- Low Latency
- Backend Traffic Reduction
- Cloud Cost Reduction
- Network Load Reduction
- Efficient Data Management
- Rapid Access to Data Analytics
AI / ML / Deep Learning at the Edge Nodes
Learning at the Resource Constrained Edge Nodes

Security is critical when running ML / DL at the Edge
Design Space for Edge Intelligent Systems
MEC ARCHITECTURE
Secure Three Layer MEC Architecture

CHALLENGES TO THE MEC PARADIGM

- Access control
- Heterogeneity of MEC systems
- Identity authentication
- Privacy preservation
- Secure data aggregation
- Mis-configurations
- Diversity of communication technologies
- Secure content distribution
- Resilience to attacks
- Lightweight protocol design
- Establishing trustworthy data sharing practices
CHALLENGES TO THE MEC PARADIGM

• The lack of comprehensive security mechanisms render the deployment of MEC a technically challenging problem

• The security goals of MEC should be grounded on a combined objective of securing the data and ensuring the safety and resiliency of systems and processes
  • Confidentiality
  • Integrity
  • Availability
  • Safety
  • Resiliency
Proposed SecEdge-Learn MEC Architecture

EMERGING PARADIGMS AT THE EDGE

FEDERATED LEARNING

A PRIVACY PRESERVING PARADIGM
The Buzz on Federated Learning

Google is using federated learning to improve Assistant's "Hey Google" accuracy.

The Global Federated Learning Market size is expected to reach $198.7 Million by 2028, rising at a market growth of 11.1% CAGR during the forecast period.

Collaborative machine learning that preserves privacy
Researchers increase the accuracy and efficiency of a machine-learning method that safeguards user data.

Adam Zewe | MIT News Office
September 7, 2022
Applications of Federated Learning

• Application in the Healthcare Industry
• Applications for FinTech
• Applications in Insurance Sector
• Applications in IoT
• Application in other Industries and Technologies
CLASSICAL MACHINE LEARNING VERSUS FEDERATED LEARNING

• Central machine learning
  • move the data to the computation
• Federated (machine) learning
  • move the computation to the data
Federated Learning
Distributed System with ML Model Exchange

FL Key Objective: Privacy Preserving Paradigm!
Federated Learning & Network Parameters

FL Performance is also a function of the System Parameters

Network Bandwidth
Computation Power
Data Volume
Data Skewness
Aggregation Algorithm
Challenges of Federated Learning

- Heterogeneity
- Privacy
- Communication
- Efficiency
- Security
- Model Selection
- FL at the Edge
- Lack of Standardization

Server coordinating the training of a global AI model

FOCUS

Devices with local AI models
Threats, Attacks and Defences in Federated Learning
Taxonomy of Attacks on Federated Learning Systems

FL attacks

- Poisoning attacks
  - Data poisoning attacks
    - Clean-label attacks
    - Dirty-label attacks
  - Model poisoning attacks
    - Gradient manipulation attacks
    - Training rule manipulation attacks
    - Backdoor attacks

- Free-riding attacks

- Communication attacks
  - MITM attacks
  - Communications bottlenecks

- Inference attacks
  - Membership inference attacks
  - Properties inference attacks
  - Training inputs and labels inference attacks
  - GANs-based inference attacks
Attack Vectors in Federated Learning

1. **Step 1:** Model initialization.
2. **Step 2:** Local model training and upload.
3. **Step 3:** Global model aggregation and update.
Attack Vectors in Federated Learning

Fig. 1 The multi-phases framework of FL including data and behavior auditing, model training and model predicting.
Data Poisoning Attack in Federated Learning Systems
An Example of GANs-based Inference Attack in FL Systems
Federated Learning Systems: Challenges

Communications bottlenecks in FL systems

An example of free-riding attack in FL systems
An Overview of Defensive Mechanisms in FL Systems
## Federated Learning Defensive Mechanisms

<table>
<thead>
<tr>
<th>Defensive mechanisms</th>
<th>Key idea</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differential Privacy</td>
<td>Introduce noise to the client’s sensitive data before sharing individual updates with the FL server</td>
<td>• Data poisoning attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Backdoor attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inference attacks</td>
</tr>
<tr>
<td>Secure Multi-party Computation</td>
<td>Encrypt clients’ uploaded parameters</td>
<td>• Inference attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MITM attacks</td>
</tr>
<tr>
<td>Anomaly detection</td>
<td>Analyze clients’ updates to identify misbehaving clients</td>
<td>• Free-riding attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Model poisoning attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data poisoning attacks</td>
</tr>
<tr>
<td>Robust aggregation</td>
<td>Detect malicious individual updates during training process</td>
<td>• Inference attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Model poisoning attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data poisoning attacks</td>
</tr>
<tr>
<td>Federated distillation</td>
<td>Transfer knowledge from a fully trained model to another model</td>
<td>• Communications bottlenecks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MITM attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inference attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GANs-based attacks</td>
</tr>
</tbody>
</table>
Maliciousness in Worker Nodes

- How do we detect Maliciousness in Worker Nodes and incorporate the same in selection criteria?
- Malicious Nodes Definition
  - e.g.: Nodes with wrongly labelled data
- The extent of the malicious nodes could be varied
- The number of malicious nodes and the total number of nodes could be varied
- We can also test in a dynamic setting where the nodes may be initially benign and may start turning malicious after some internal of time
- Ignoring such nodes becomes quite important for the selection algorithm
Incorporating Maliciousness in Worker Nodes: Swap the Labels

**Time vs Local Loss**

- **Local Model Loss for Malicious Node Detection**
  - Total Worker Nodes: 20
  - Malicious Nodes: 4 (Labels swapped)
  - Data Distribution: Homogeneous
  - Dataset: MNIST

Considerably higher local model loss values for malicious nodes
Data Poisoning Attacks

Accuracy (data poison = 0.2) and Accuracy (data poison = 0.1)

Accuracy and Loss (Data Poison rate : 0.4)
Gradient Poisoning Attacks

Accuracy at different noise rates

- Accuracy (20% and 0.3 noise)
- Accuracy (15% and 0.2 noise)

Loss (15% manipulation) and Loss (20% manipulation)
EMERGING PARADIGMS AT THE EDGE

REINFORCEMENT LEARNING

Work in Progress
Fundamentals

- Supervised learning
  - classification, regression

- Unsupervised learning
  - clustering

- Reinforcement learning
  - more general than supervised/unsupervised learning
  - learn from interaction w/ environment to achieve a goal
New Challenges in Reinforcement Learning: A Survey of Security and Privacy

Yunjiao Lei¹, Dayong Ye¹, Sheng Shen¹, Yulei Sui¹, Tianqing Zhu¹* and Wanlei Zhou²

¹School of Computer Science, University of Technology Sydney, Broadway, Sydney, 2007, NSW, Australia.
²School of Data Science, City University of Macau, Macau, China.

Springer Nature 2021
The green car is an agent. the environment comprises the road, the traffic signs, other cars, etc.
A Simple Example of a Security Attack in Reinforcement Learning in the Context of Automatic Driving

Action attack: Tempting the agent to take an action of “turn right”, rather than the optimal action of “go straight”.

Environment Attack: Changing the road condition to mislead the agent to take a wrong action.

Reward attack: Giving a wrong reward of +1, instead of -1.
Summary of Research Addressing Security in Reinforcement Learning

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Papers</th>
<th>Target</th>
<th>Impact</th>
<th>Strategies</th>
<th>Representative/Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security of state and action in MDP</strong></td>
<td>Lee et al. [58]</td>
<td>Action</td>
<td>Reward</td>
<td>Perturbations</td>
<td>Optimization-based approaches</td>
</tr>
<tr>
<td></td>
<td>Chen et al. [56]</td>
<td>Action</td>
<td>Policy</td>
<td>Action robustness</td>
<td>Projected gradient descent</td>
</tr>
<tr>
<td></td>
<td>Zhao et al. [45]</td>
<td>State</td>
<td>Policy</td>
<td>Perturbations</td>
<td>Zero-sum game</td>
</tr>
<tr>
<td></td>
<td>Garrett et al. [64]</td>
<td>State</td>
<td>System destabilization</td>
<td>Perturbations</td>
<td>Nash equilibrium</td>
</tr>
<tr>
<td></td>
<td>Sun et al. [40]</td>
<td>State</td>
<td>Reward, Action</td>
<td>Perturbations</td>
<td>Imitation learning</td>
</tr>
<tr>
<td></td>
<td>Ye et al. [57]</td>
<td>State</td>
<td>Action</td>
<td>Model learning</td>
<td>Neural network</td>
</tr>
<tr>
<td></td>
<td>Dai et al. [65]</td>
<td>State-action</td>
<td>Policy</td>
<td>Safe exploration</td>
<td>Deep neural network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Convolutional neural network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Transfer learning</td>
</tr>
<tr>
<td><strong>Security of environment in MDP</strong></td>
<td>Rakheha et al. [43]</td>
<td>Transition</td>
<td>Policy</td>
<td>Data poisoning</td>
<td>Optimization problems having constraints</td>
</tr>
<tr>
<td></td>
<td>Chan et al. [59]</td>
<td>Features</td>
<td>Reward</td>
<td>Adversarial sample</td>
<td>Sliding-window method</td>
</tr>
<tr>
<td></td>
<td>Wang et al. [22]</td>
<td>Environment</td>
<td>Robust policy</td>
<td>Robust adversarial learning</td>
<td>Gradient function</td>
</tr>
<tr>
<td></td>
<td>Li et al. [46]</td>
<td>Non-stationary</td>
<td>Robust policies</td>
<td>Robust adversarial learning</td>
<td>Cross-entropy method</td>
</tr>
<tr>
<td></td>
<td>Lin et al. [44]</td>
<td>Features</td>
<td>Action</td>
<td>Adversarial sample</td>
<td>Actor-critic architecture</td>
</tr>
<tr>
<td></td>
<td>Li et al. [60]</td>
<td>Environment</td>
<td>Policy</td>
<td>Two-player zero-sum game</td>
<td>Minimax optimization</td>
</tr>
<tr>
<td></td>
<td>Zhai et al. [67]</td>
<td>Environment</td>
<td>Policy</td>
<td>Two-player zero-sum game</td>
<td>End-to-end learning approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Gradient-based methods</td>
</tr>
<tr>
<td><strong>Security of reward function in MDP</strong></td>
<td>Zhang et al. [54]</td>
<td>Reward</td>
<td>Policy</td>
<td>Poisoning attack</td>
<td>Nash equilibrium</td>
</tr>
<tr>
<td></td>
<td>Li et al. [68]</td>
<td>Reward</td>
<td>Policy</td>
<td>Adversarial inverse</td>
<td>Lyapunov network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>reinforcement learning</td>
<td></td>
</tr>
</tbody>
</table>
Key Findings of the Edge Security Report

• Edge deployments are increasing in scale across investments, projects, use cases, endpoints and types of endpoints
• Security is the top challenge cited by enterprises with edge deployments
• Risks to edge systems such as cyberattacks and from edge systems due to vulnerabilities and misconfigurations are on the rise

Reference:
Summary and Future Directions

- MEC Security is a critical area that needs a lot more attention considering the huge growth of the Edge.

- New paradigms at the Edge such as Federated Learning, Reinforcement Learning, etc are likely to spawn additional attack surfaces and attack vectors.

- Need robust mitigation of the attacks since Edge nodes will become more complex with each passing year.
THANK YOU

rajeevshorey@gmail.com