MELBOURNE CLOUDS LAB

THE UNIVERSITY OF MELBOURNE

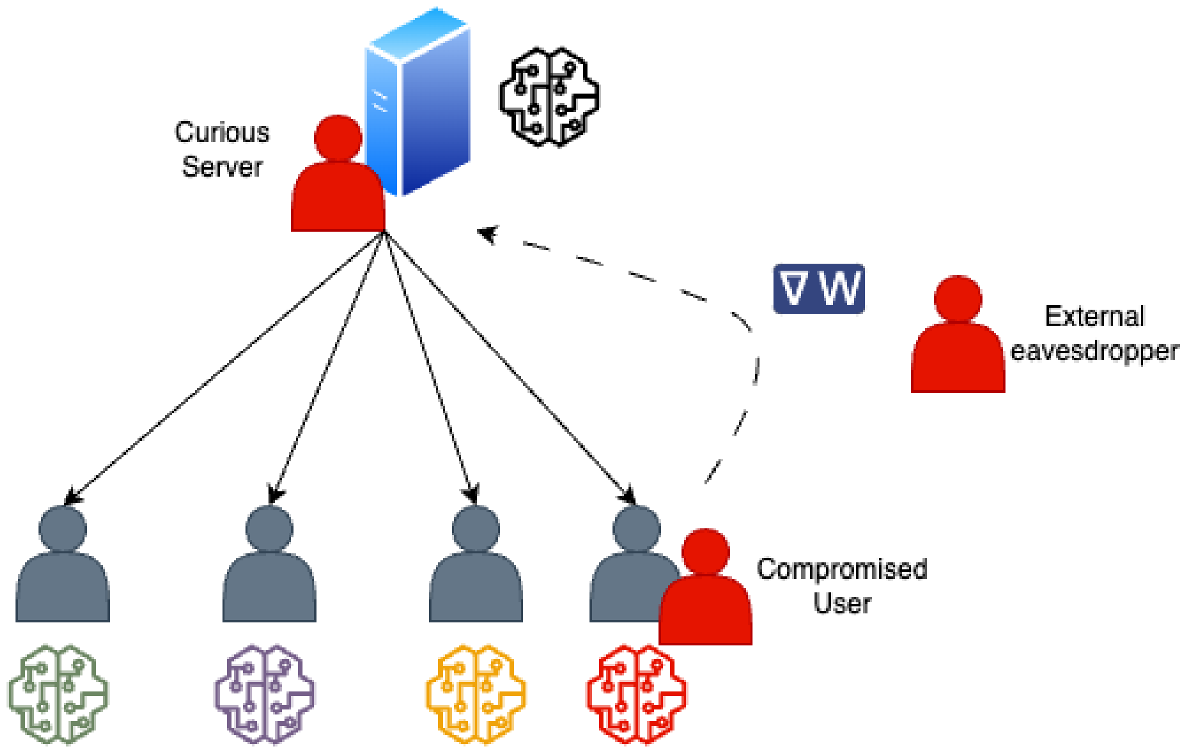
Network Structures as an Attack Surface

Topology-Based Privacy Leakage in Federated Learning

Murtaza Rangwala, Richard O. Sinnott and Rajkumar Buyya

Cloud Computing and Distributed Systems (CLOUDS) Lab
School of Computing and Information Systems
The University of Melbourne

Network Topology-Based Privacy Leakage in Federated Learning



What we're protecting against…

Gradient Inversion Attacks
Reconstructing training data from shared updates

Model Extraction
Stealing model parameters and behaviour

Membership Inference
Identifying if data was used in training

Current Defenses

Differential Privacy
Noise Addition

Homomorphic Encryption
Computation on Encrypted Data

Secure Aggregation
Cryptographic Parameter Combination

Network Topology-Based Privacy Leakage in Federated Learning

What is also exposed...
Network Topology Knowledge Structure and communication patterns
Organizational Relationships Institutional connections and hierarchies
Communication Metadata Frequency, timing, and routing information

Current Defenses
No protection for structural information
Observable coordination patterns
Persistent vulnerabilities despite strong content protection

Network Topology-Based Privacy Leakage in Federated Learning

THE UNIVERSITY OF MELBOURNE

Attack Vector 1
Communication Pattern Analysis

How it works:

- Nodes with similar data distributions converge faster
- Requires fewer communication rounds in later training phases
- Creates observable frequency patterns in message exchanges

What Adversaries Learn:

- Which nodes have similar data characteristics
- Clustering of participants based on convergence behavior
- Group-level data distribution patterns

Attack Vector 2
Parameter Magnitude Profiling

How it works:

- Data heterogeneity systematically affects parameter update magnitudes
- Rare classes produce larger, less stable gradient norms
- Homogeneous data leads to smoother optimization trajectories

What Adversaries Learn:

- Nodes training on rare or sensitive classes
- Statistical signatures of data imbalance
- Convergence stability patterns

Attack Vector 3
Structural Position Correlation

How it works:

- Real deployments correlate network position with data characteristics
- Geographic proximity reflects demographic similarities
- Organizational hierarchies determine data access patterns

What Adversaries Learn:

- Systematic assignment patterns
- Institutional data clustering
- Position-based sensitive group identification

Network Topology-Based Privacy Leakage in Federated Learning

THE UNIVERSITY OF MELBOURNE

Through a systematic evaluation of **4,720 attack instances** across **520 network configurations**, we analyzed **6 distinct adversarial knowledge scenarios.**

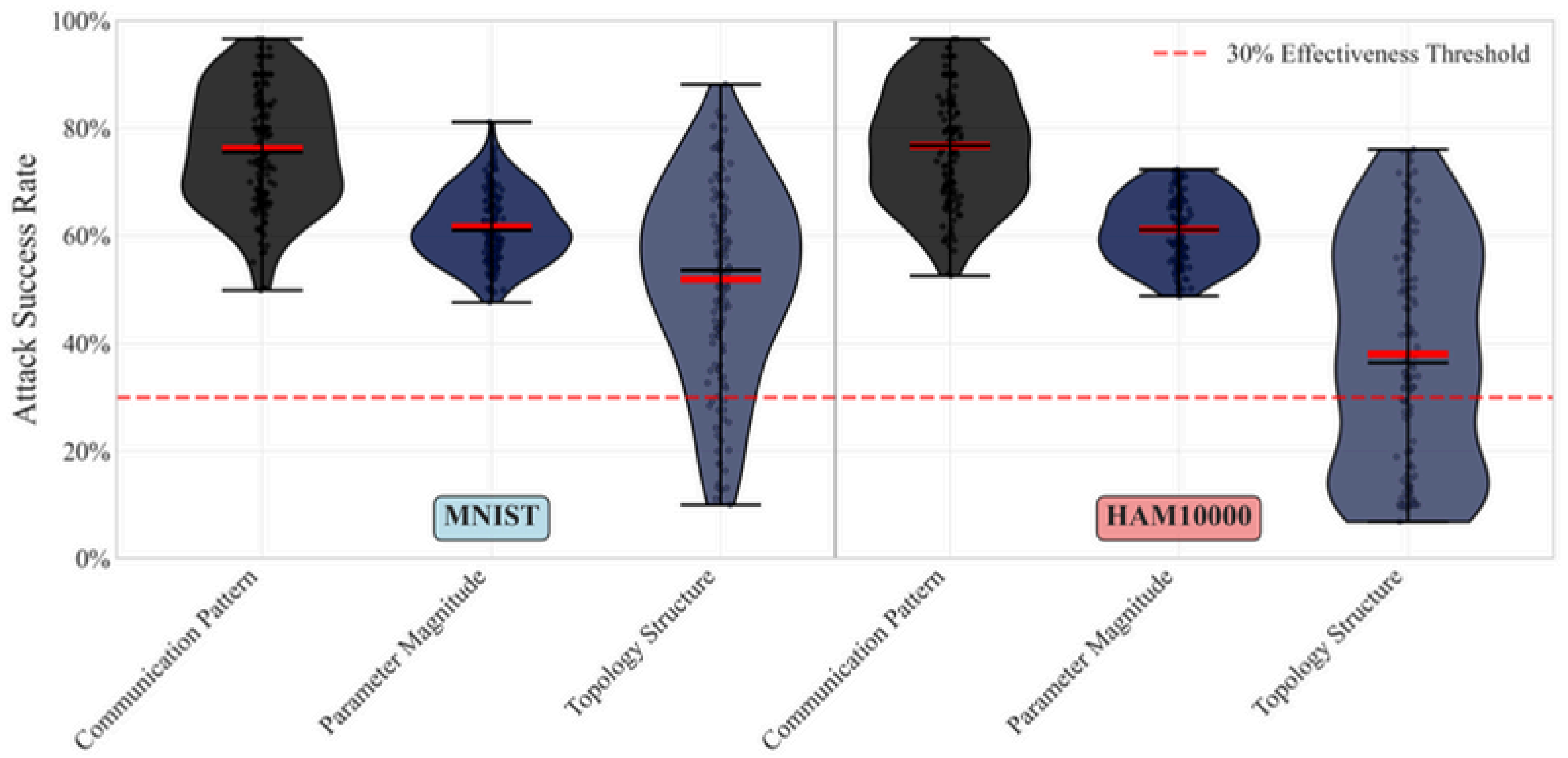
Knowledge Scenario	Communication Pattern	Parameter Magnitude Profiling	Topology Position Correlation	Overall Status
Complete Knowledge	84.1%	65.0%	47.2%	**Worst-Case Upper Bound**
1-hop Neighborhood	68.8%	47.2%	47.8%	Fully Effective
2-hop Neighborhood	76.5%	62.3%	47.9%	Fully Effective
Statistical Knowledge	86.0%	65.4%	⚠️ 27.6%	Partially Effective
Organizational (3-groups)	31.7%	42.5%	74.1%	Fully Effective
Organizational (5-groups)	53.3%	61.4%	53.6%	Fully Effective

Attack Success Threshold: 30%

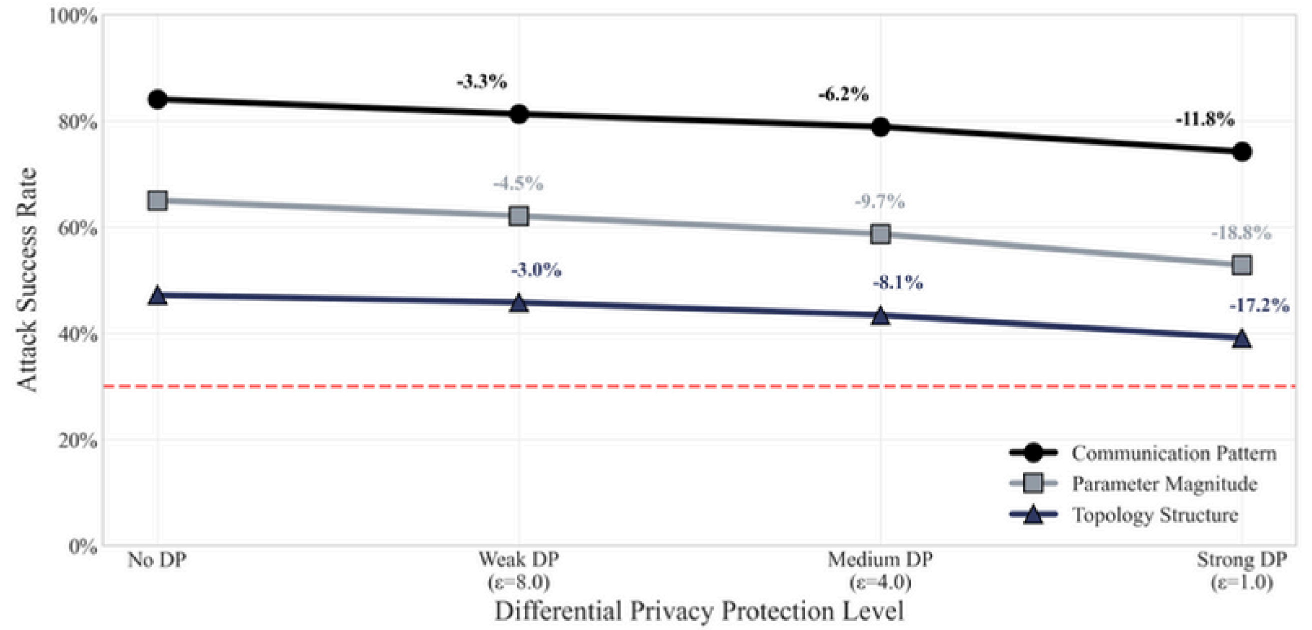
Network Topology-Based Privacy Leakage in Federated Learning

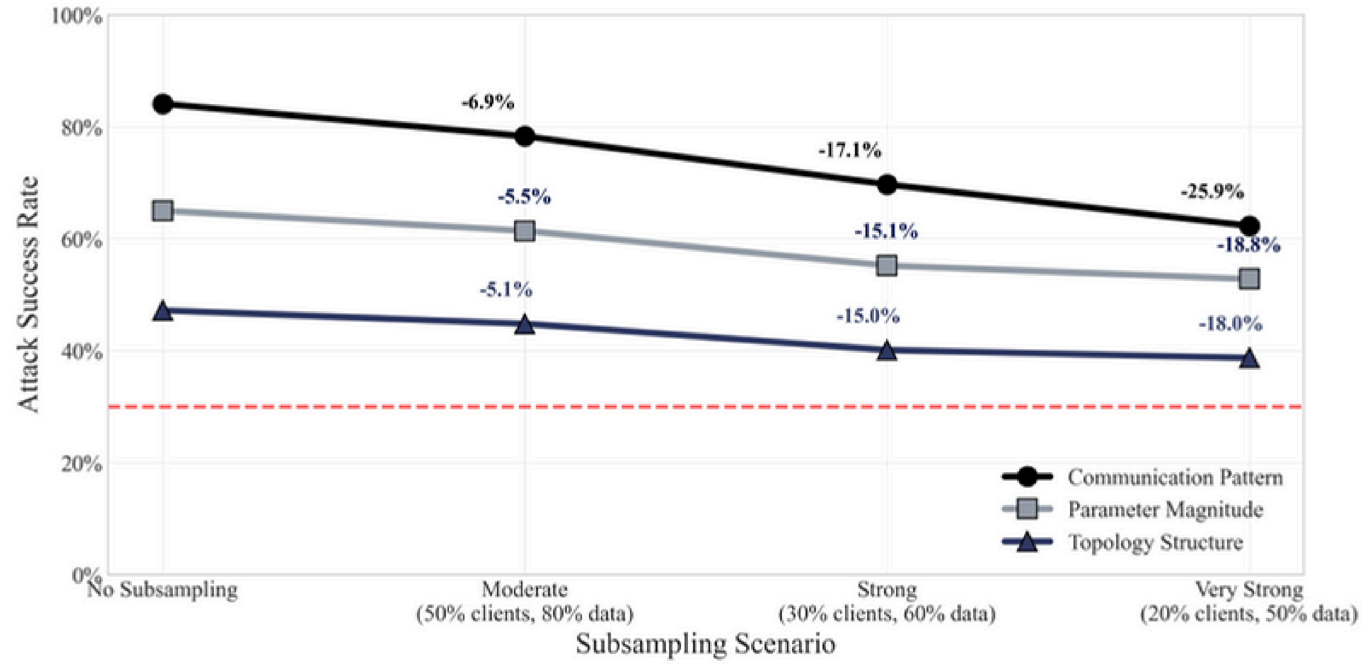
THE UNIVERSITY OF MELBOURNE

Security vulnerabilities persist across datasets



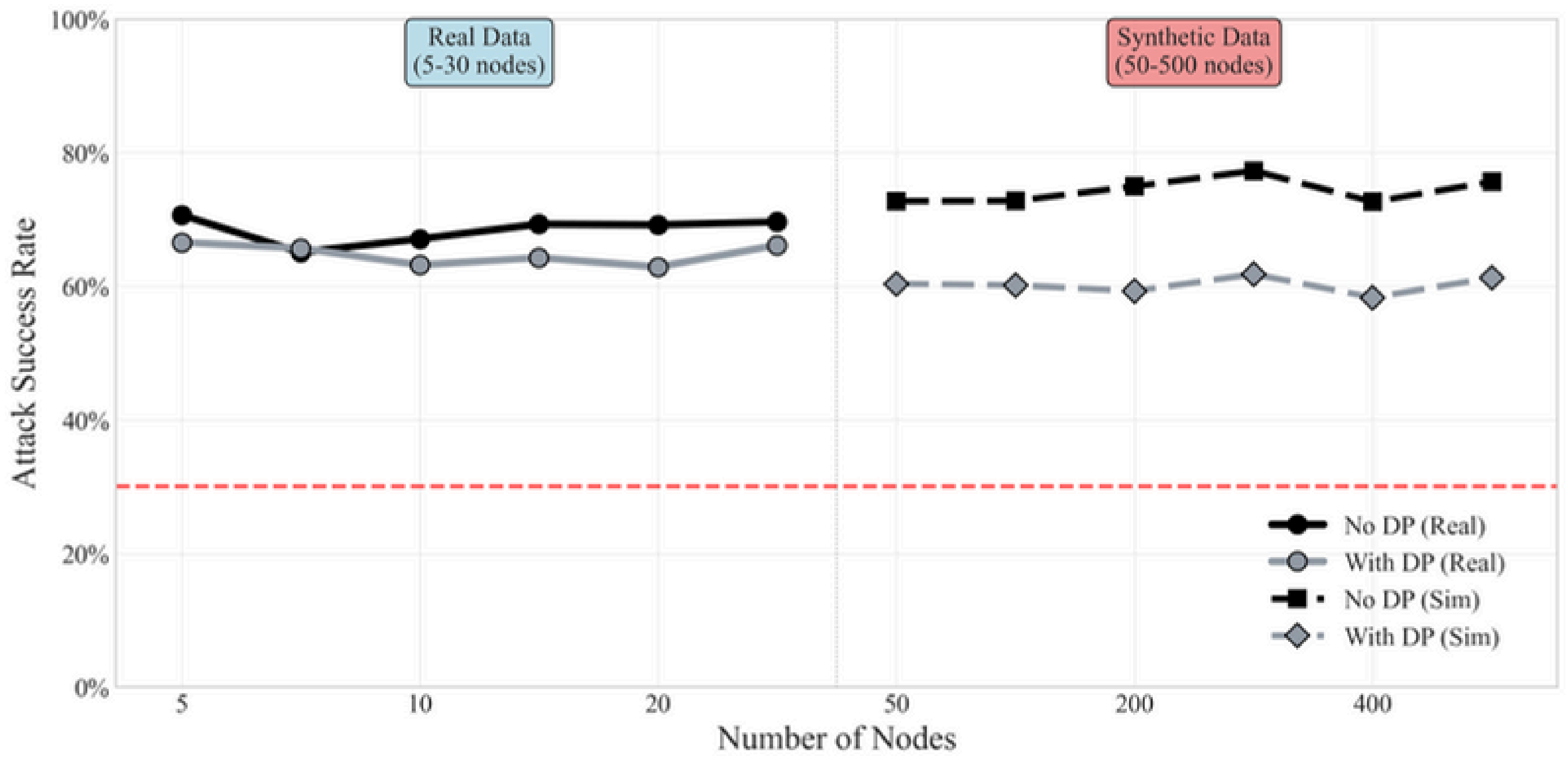
...and across varied privacy scenarios

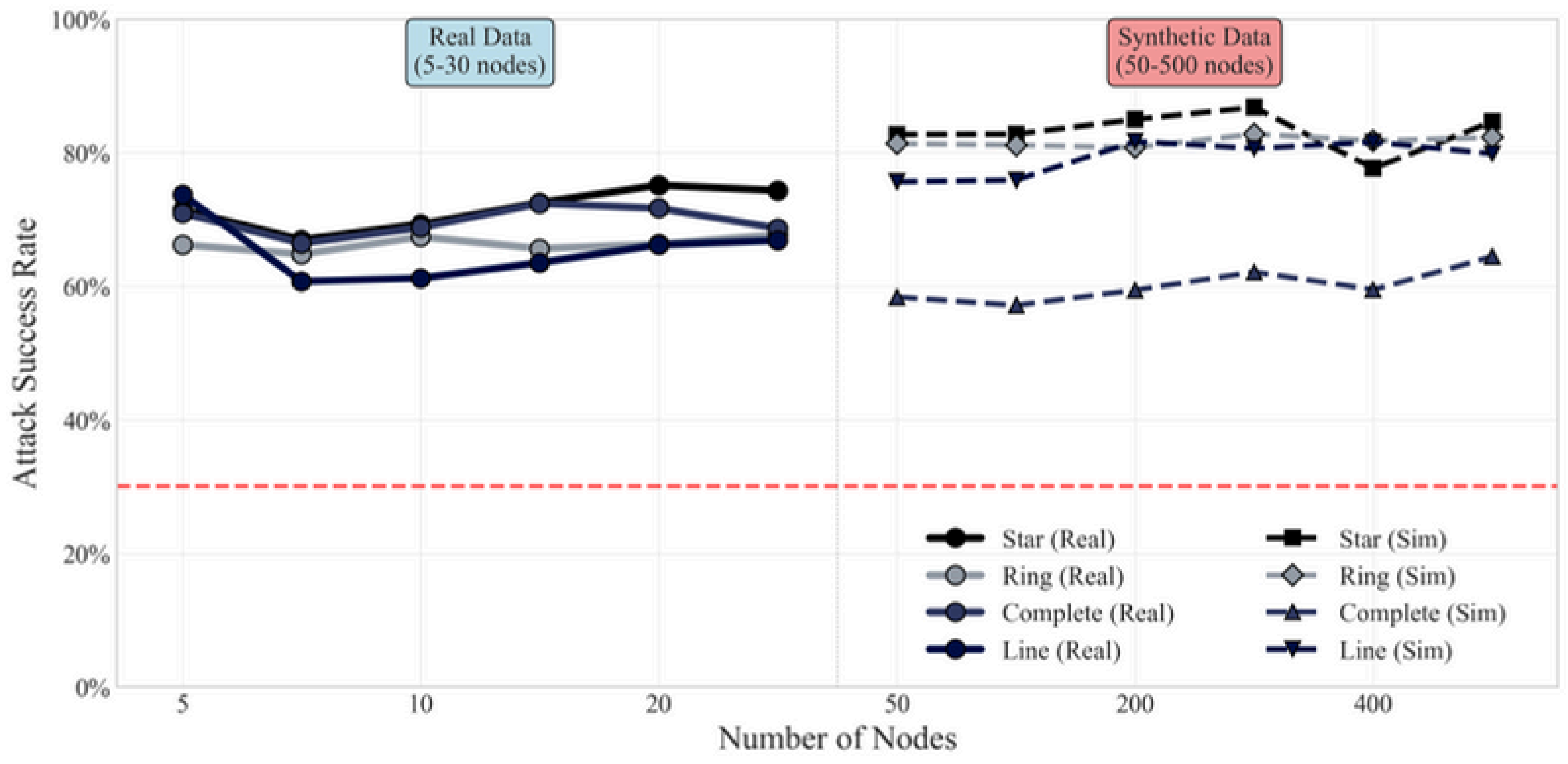




Network Topology-Based Privacy Leakage in Federated Learning

Network scale does not impact attack effectiveness





Network Topology-Based Privacy Leakage in Federated Learning

THE UNIVERSITY OF MELBOURNE

Potential Research Directions

Topology-Aware Privacy Mechanisms

- Extend differential privacy to account for network structure correlations
- Develop privacy definitions that bound inference advantages from topology knowledge
- Create structural noise injection techniques for communication patterns

Dynamic Network Reconfiguration

- Periodic topology changes to mask timing analysis
- Randomized communication scheduling with bandwidth normalization
- Decoupling of network positioning from organizational relationships

Privacy Amplification from Correlated Participants

- Account for topology-induced correlations in privacy accounting
- Develop participant sampling strategies that minimize structural leakage
- Balance coordination efficiency with structural information protection

THE UNIVERSITY OF MELBOURNE

Q&A

LinkedIn

POSTERA CRESCAM LAUDE

THE UNIVERSITY OF

MELBOURNE