Identifying Critical Nodes in Large Complex Systems Using Temporal Graph Convolutional Networks

Heng Chuan Tan[1], Zbigniew Kalbarczyk[1,2]
[1] Illinois Advanced Research Science Center at Singapore, Singapore
[2] Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, USA

Background/Problem

- Cyber-physical systems face many vulnerabilities and attack exposures due to high connectivity, heterogeneous networks, and reliance on shared resources.
- Given the scale of these interconnected systems and limited defense resources, it is challenging to determine which assets truly matter to prioritize defenses.
- Security teams rely on Common Vulnerability Scoring System (CVSS) scores to decide which vulnerabilities to address first.
- However, CVSS fails to incorporate contextual factors, such as how the devices are connected and which assets are critical.
- Without this context, CVSS can overlook vulnerabilities that pose disproportionate risks due to their position in the network.

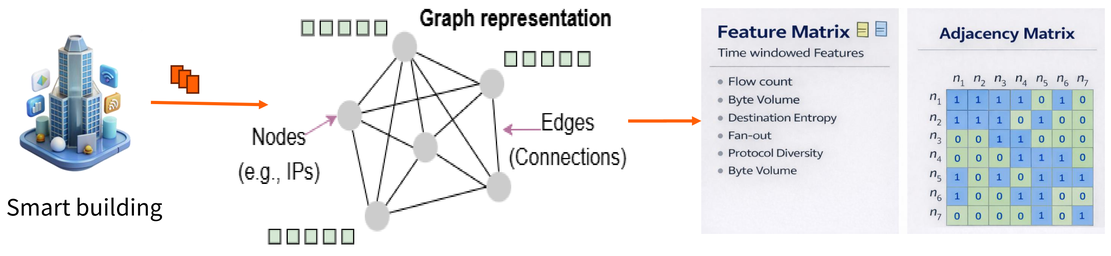
Our Approach

We develop a **Graph Convolutional Network GCN)** that learns network topology and evolving behavior to rank nodes by criticality

1 Model the System as a Graph
- Represent the cyber-physical system as $G = (V, E)$
- **Nodes:** assets (servers, PLCs, IoT, gateways)
- **Edges:** communication relationships
- Captures topology and dependencies between assets

2 Extract Traffic & Temporal Features
- Construct node feature matrix and adjacency matrix from normal traffic
- **Features:** Flow count, byte volume, destination entropy, fan-out ratio, protocol diversity
- Use sliding windows to capture evolving behavior

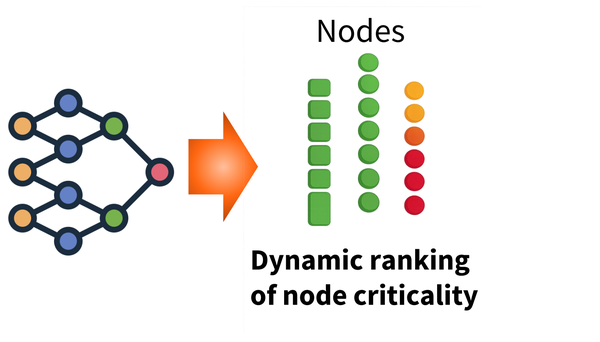
3 Learn Spatio-Temporal Patterns with GCN
- **GCN layers:** Learn structural importance from topology and node features
- **Graph Attention Network (GAT) layers:** Assign different weights to neighbors during feature aggregation.
- **Graph Recurrent Unit (GRU) layers:** Capture temporal evolution of node features and behavior.
- Train with hybrid ranking loss to preserve node ordering.



GCN → Learn network structure from traffic and topology

Graph Attention Network (GAT) → Assign different weights to neighbours

Gated Recurrent Unit (GRU) → Capture temporal patterns in traffic



Dynamic ranking of node criticality

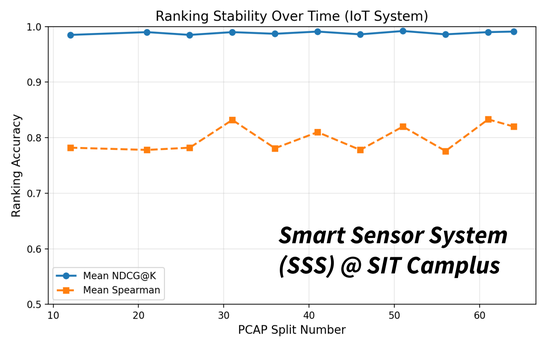
Pinpoints high-risk assets whose compromise causes largest impact

Evaluation

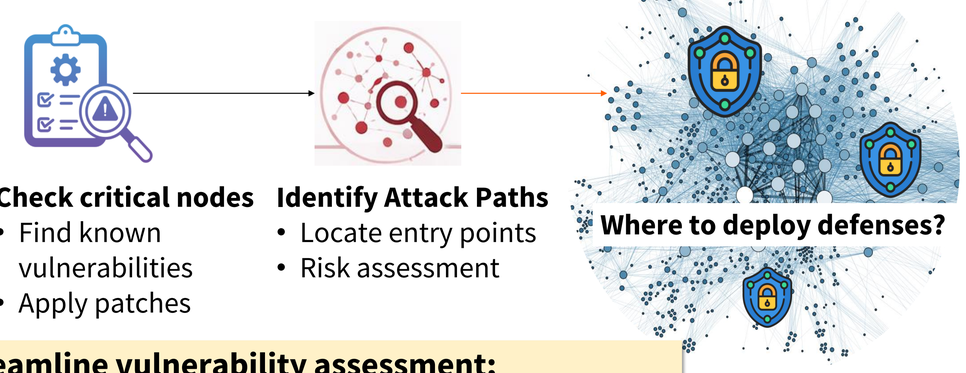
Validated using operational datasets from two real-world systems:
- **SIT Campus @ Punggol Digital District**
  - Building Automation System (BAS)
  - Smart Sensor System (SSS)

Top 10 nodes (SSS) 6 Jun 2025, 12pm to 6:30pm

```
============ Train on capture-20250603.e2mcr1.pcap.split,
============ Test on capture-20250603.e2mcr1.pcap.split11
mean_spearman: 0.7837
mean_mae: 0.0630
mean_ndcg@k: 0.9873
Top 39 critical nodes:
  1: 192.168.2.36          → 0.989343
  2: 192.168.0.23          → 0.337363
  3: 192.168.0.52          → 0.179050
  4: 192.168.0.220         → 0.174647
  5: 192.168.0.157         → 0.174369
  6: 192.168.0.253         → 0.174215
  7: 192.168.0.221         → 0.174139
  8: 192.168.0.243         → 0.173376
  9: 192.168.0.130         → 0.172422
 10: 192.168.0.45          → 0.172223
```



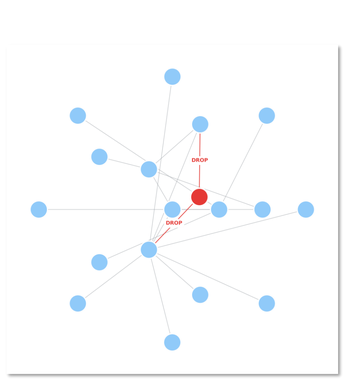
Rank nodes by criticality to prioritize defenses
Stable rankings → Normal operation
Abrupt changes → Topology / configuration updates
Unexplained changes → Possible attack (e.g., scanning, DoS)



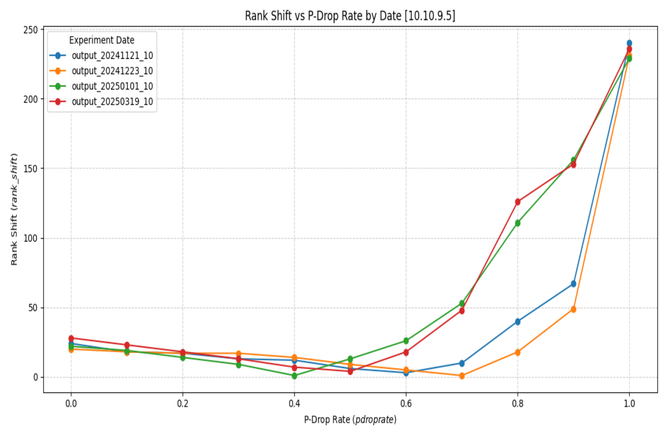
Streamline vulnerability assessment;
Improve situational awareness & guide defense

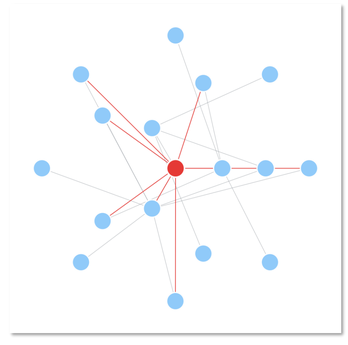
Attack Detection with GCN

- Attacks induce **abnormal rank shifts** in influential nodes
- Targeted disruptions cause **instability in node importance**
- Deviations from baseline indicate **potential compromise**
- 🔍 *Criticality drift = early indicator of cyber attack activity*

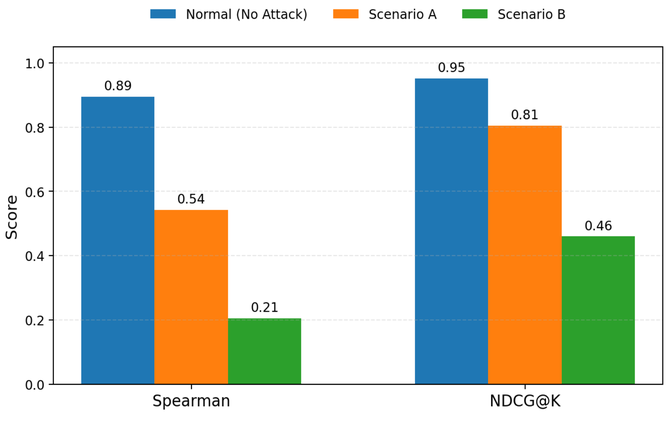


MiTM-Drop





DoS



CREATE
Campus for Research Excellence And Technological Enterprise

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme.