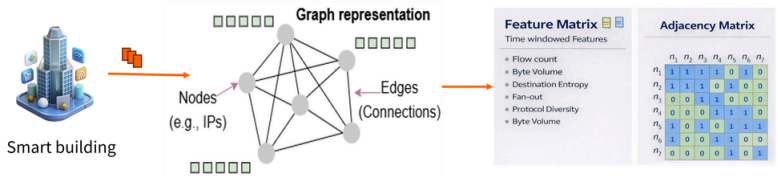
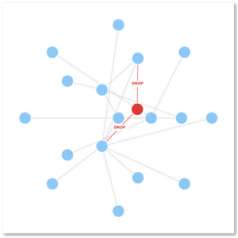
THRUST 4: EVALUATION

GRAPH CONVOLUTIONAL NETWORK (GCN)

Defending every asset on an equal scale is not feasible, especially in large-scale environments. Identifying and ranking assets based on their criticality levels is one of the primary objectives of defense strategy. While traditional approaches such as the Common Vulnerability Scoring System (CVSS) are useful for quantifying vulnerability severity, these scores do not account for the broader network context. CVSS scores fail to differentiate between high-impact assets and those with limited connectivity or low risk to the network.





MiTM-Drop

The GCN model is trained on a baseline set of normal traffic to learn high-level representative patterns. The model then ranks each device by its criticality level, which is based on the node's traffic intensity and network connectivity. As new predictions are generated, the visualization updates in real-time with color-coded severity levels, providing operators with an immediate visual cue for prioritized intervention.

Besides identifying critical nodes, the model also detects network attacks by monitoring significant shifts in nodes ranking for affected IP addresses. Sudden increase in traffic intensity which can be seen in a Denial-of-Service (DoS) attack, disrupts learned patterns and trigger drops in ranking consistency metrics such as Spearman and NDCG. These deviations signal abnormalities in conditions instantly, enabling operators to have proactive intervention rather than reactive mitigation.