**GNN trong Hệ thống Phát hiện Xâm nhập (IDS)**

Trong GNN-IDS, mạng nơ-ron đồ thị được sử dụng làm công cụ suy luận để phát hiện xâm nhập. Bằng cách học kết nối mạng, mạng nơ-ron đồ thị có thể định lượng tầm quan trọng của các nút lân cận và các đặc điểm của nút để đưa ra các dự đoán đáng tin cậy hơn. Hơn nữa, bằng cách kết hợp một đồ thị tấn công, GNN-IDS không chỉ có thể phát hiện các bất thường mà còn xác định các hành động độc hại gây ra các bất thường đó.

**Biểu diễn mạng máy tính thành đồ thị**

* Các thiết bị (server, host, gateway, IoT) → node
* Luồng dữ liệu mạng, kết nối TCP/IP, event log → edge
* Thuộc tính node: địa chỉ IP, dịch vụ, profile bảo mật
* Thuộc tính edge: loại giao thức, thời gian kết nối, nhãn tấn công,...
* Attack graph: sử dụng trong các kỹ thuật phân tích đa tầng, mô hình hóa đường đi tấn công, mối liên quan giữa yếu điểm, event, privilege escalation

**Mục tiêu phát hiện**

* Node embedding và message passing: Phát hiện node bất thường nhờ embedding bị lệch đi khỏi quỹ đạo bình thường sau khi lan truyền thông tin nhiều lớp.
* Phát hiện tấn công phân tán (coordinated attacks): Dạng tấn công phân tán đặc biệt khó phát hiện bằng truyền thống, nhưng GNN có thể học được pattern này thông qua aggregation đa .
* Tính thời gian thực: Nhờ khả năng inference local trực tiếp trên đồ thị hiện thời, kỹ thuật GNN thích hợp chạy trên gateway, thiết bị biên để cảnh báo sớm.