Graph Neural Networks: Revolutionizing DDoS Attack Detection

Kartikeya Sharma

Senior Associate Information Security Engineer at Equinix

What are Graph Neural Networks?

Graph Neural Networks (GNNs) are a class of deep learning models designed to work with graph-structured data. They have gained significant attention in recent years due to their ability to capture complex relationships and patterns within graphs.

What are Graph Neural Networks?

Nodes (also known as vertices) represent entities or objects in a graph.

Edges represent the relationships or connections between nodes.

What are Graph Neural Networks?

GNNs learn rich node representations, called embeddings using Message Passing

What are Graph Neural Networks?

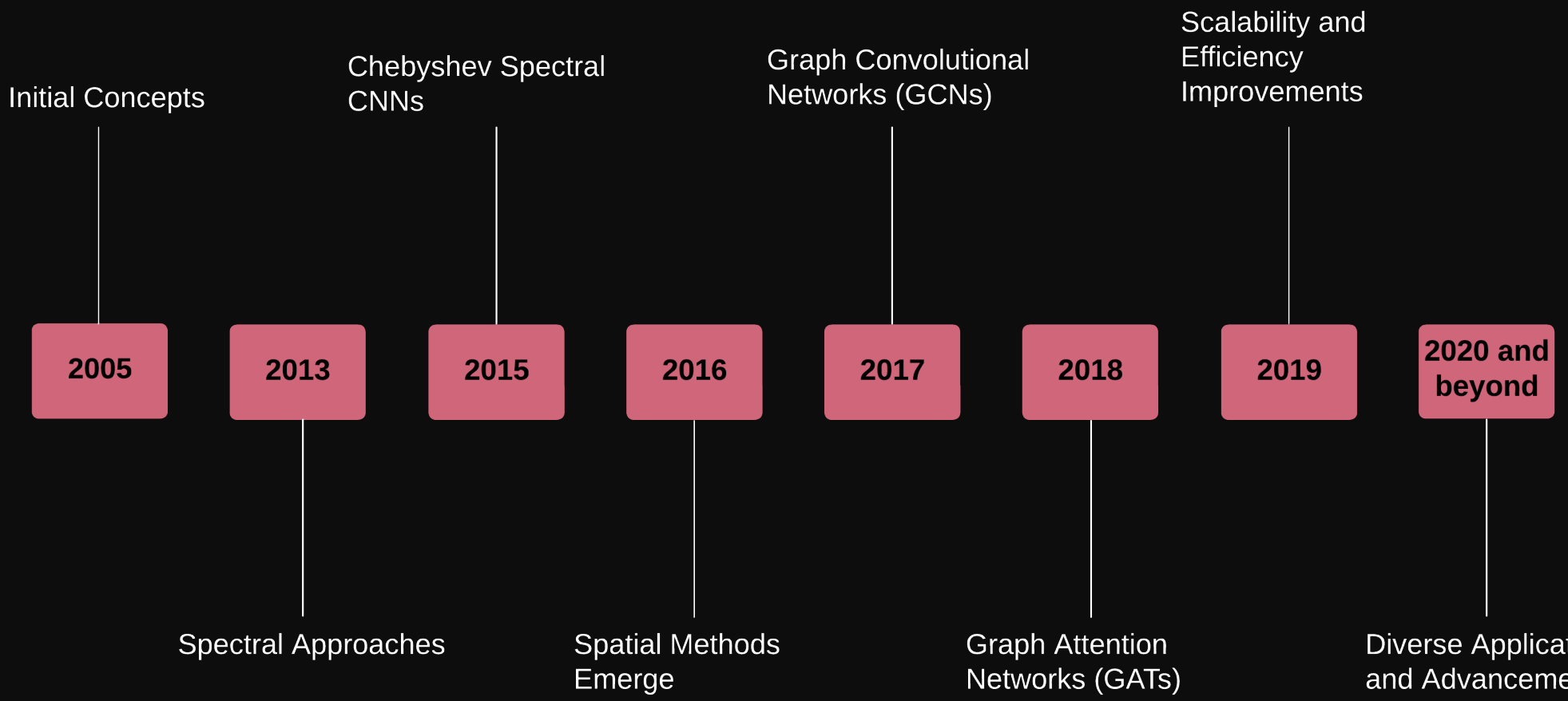
GNNs have found applications in various domains, including:

- ❑ Social network analysis
- ❑ Molecular property prediction
- ❑ Knowledge graph completion
- ❑ Recommender systems

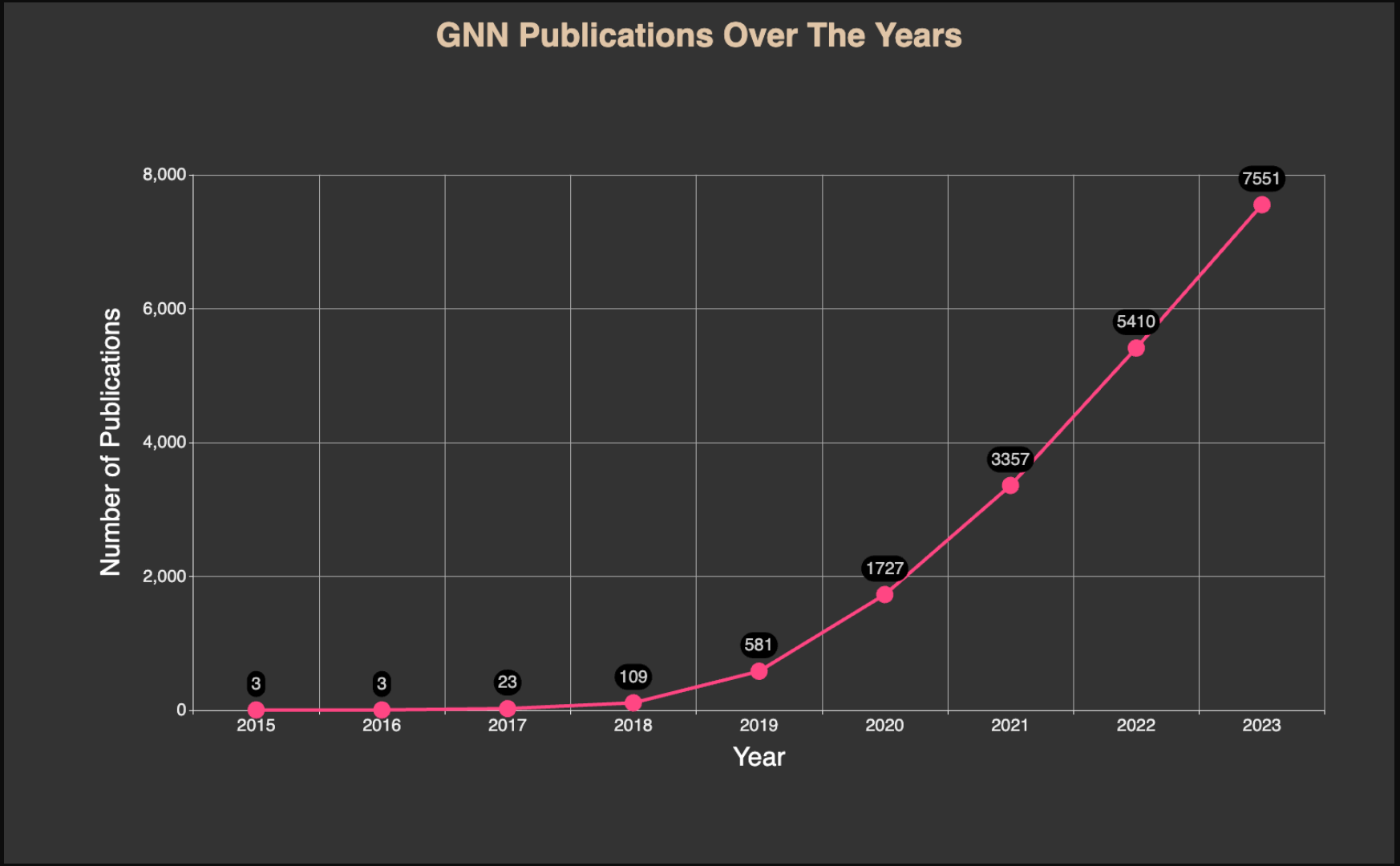
GNNs vs Traditional Neural Networks

Aspect	Graph Neural Networks	Traditional Neural Networks
Input Structure	**Graphs with variable size and connectivity**	**Fixed-size, grid-like input (e.g., images, sequences)**
Relationships	**Models and learns from relationships between entities**	**Assumes independence between input features**
Node-level Tasks	**Node classification, node regression, node clustering**	**Not applicable**
Edge-level Tasks	**Link prediction, edge classification**	**Not applicable**
Graph-level Tasks	**Graph classification, graph regression**	**Sample-level classification, regression**
Permutation Invariance	**Inherently permutation-invariant due to message passing**	**Requires explicit techniques (e.g., pooling) for permutation invariance**
Interpretability	**Can provide insights into important nodes, edges, and subgraphs**	**Often difficult to interpret learned features**

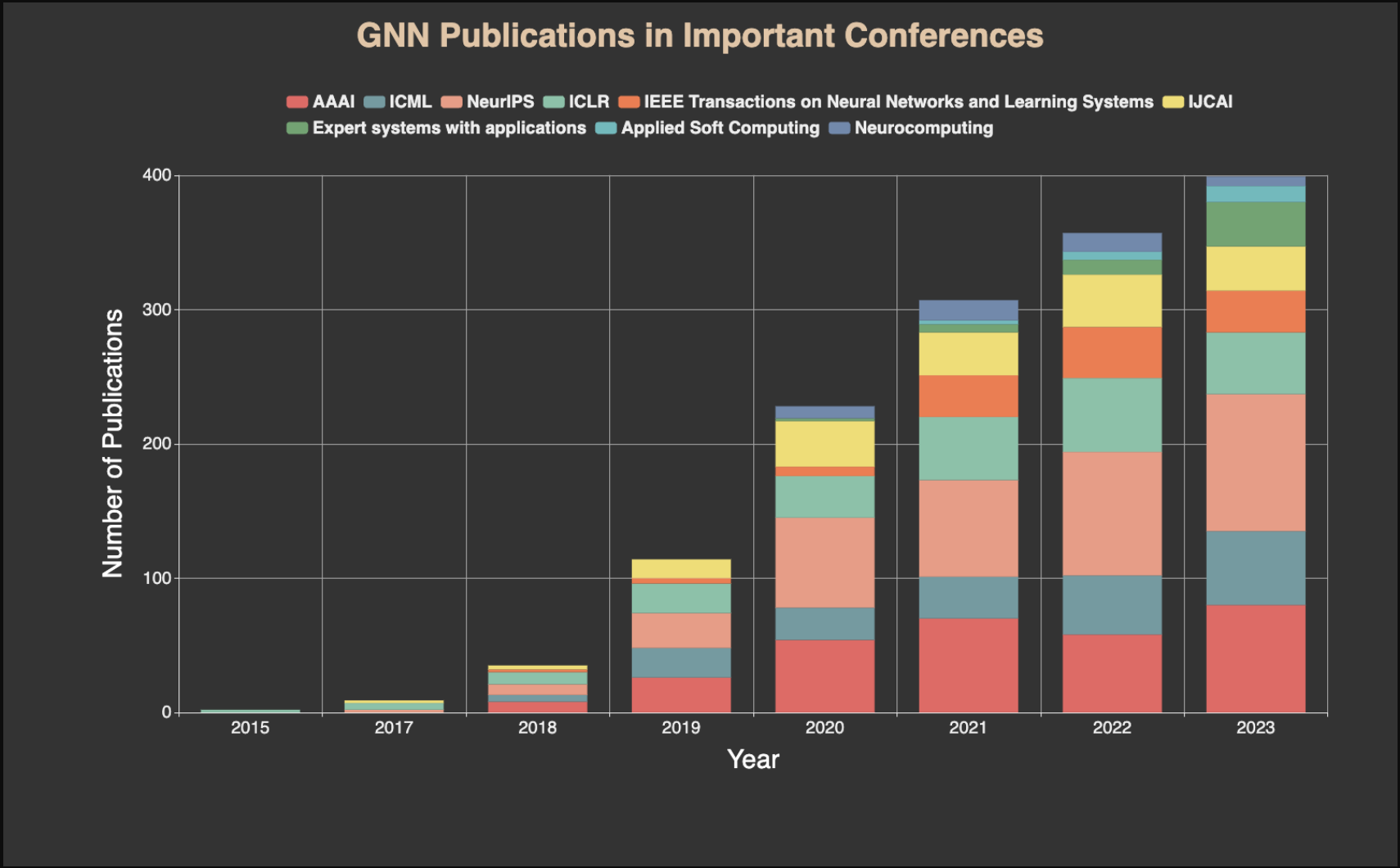
Milestones in GNN Evolution



Milestones in GNN Evolution



Milestones in GNN Evolution



What is a DDoS Attack?

A Distributed Denial of Service (DDoS) attack involves overwhelming a target—such as a server, website, or network—with a flood of internet traffic.

What is a DDoS Attack?

DDoS attacks can be categorized into three main types:

- ❑ Volume-based Attacks
- ❑ Protocol Attacks
- ❑ Application Layer Attacks

Traditional Approaches for DDoS Detection

- Filtering techniques
  - block traffic based on IP addresses, ports
- Statistical analysis
  - detect anomalies in traffic patterns, e.g. entropy, diversity
- Machine learning
  - k-Nearest Neighbors, Hidden Markov Models, Neural Networks

Traditional Approaches for DDoS Detection

Advantages of using traditional approaches:

- ❑ Simplicity and Low computational overhead
- ❑ Effectiveness against known attacks
- ❑ Interpretability

Traditional Approaches for DDoS Detection

Disadvantages of using traditional approaches:

- ❑ Limited adaptability
- ❑ Inability to model complex relationships
- ❑ High false positive rates
- ❑ Difficulty detecting low-volume attacks

The GNN Approach

- Represents the network as a graph
- Node features
  - IP address, port, and traffic statistics
- Edge features
  - Bandwidth and latency
- Learn node and edge embeddings and detect malicious activity by classifying nodes or entire graphs.

The GNN Approach

Advantages of using GNN approach:

- ❑ Automated feature learning
- ❑ Modeling complex relationships
- ❑ Generalization to unseen data

The GNN Approach

Disadvantages of using GNN approach:

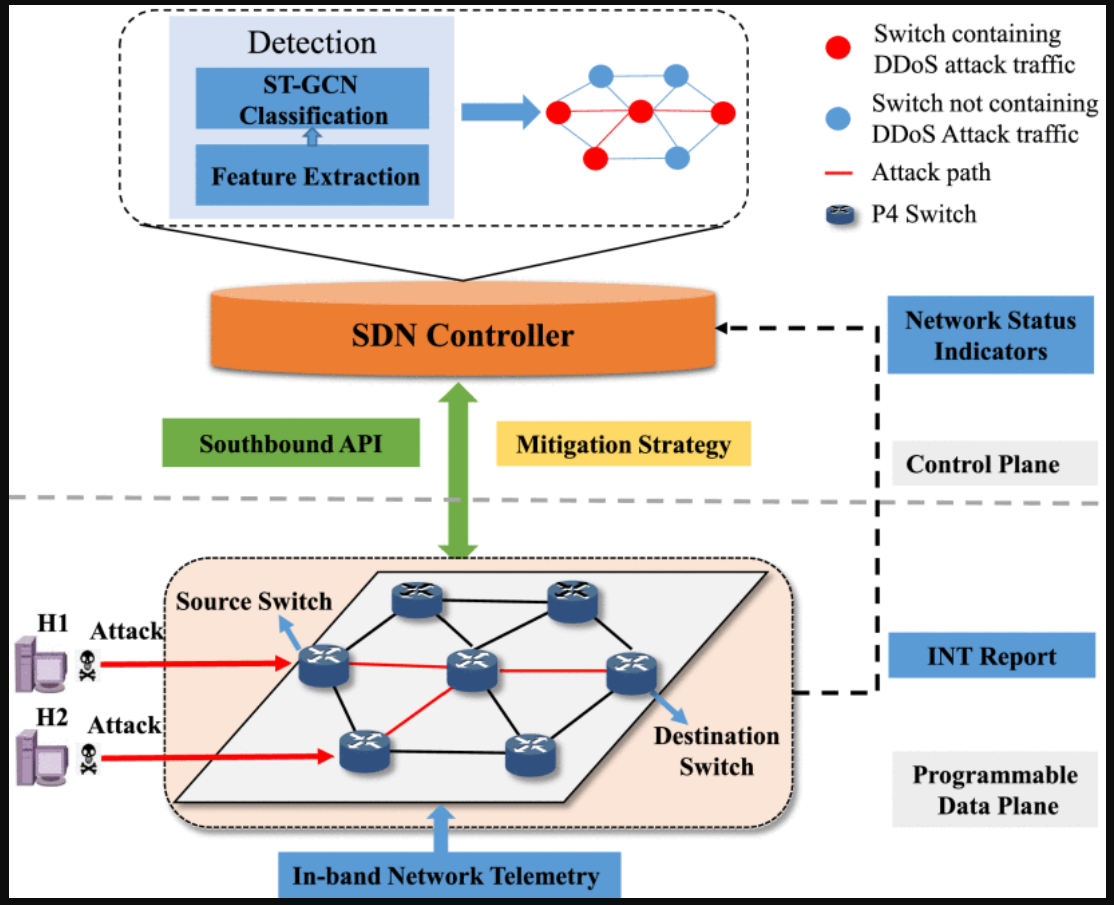
- ❑ Computational complexity
- ❑ Interpretability challenges

Detecting DDoS Attacks in SDN Using Spatial-Temporal GCN

How's the network is modeled?

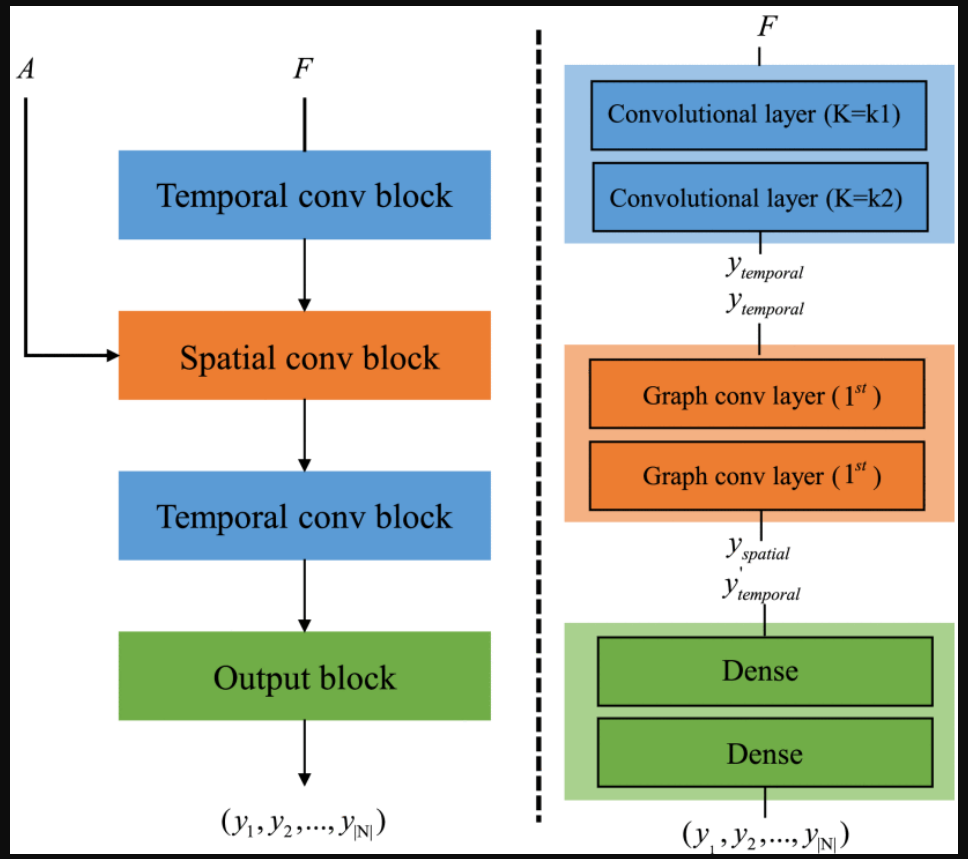
- ❑ The network is modeled as a graph, with **switches as nodes** and **links as edges**
- ❑ **Network state information** is used to create feature vectors for each switch
- ❑ The graph captures both the **network topology** and the temporal dynamics of network states

Detecting DDoS Attacks in SDN Using Spatial-Temporal GCN



System Design Overview

Detecting DDoS Attacks in SDN Using Spatial-Temporal GCN



ST-GCN Model Architecture

Detecting DDoS Attacks in SDN Using Spatial-Temporal GCN

How does it detect the DDoS?

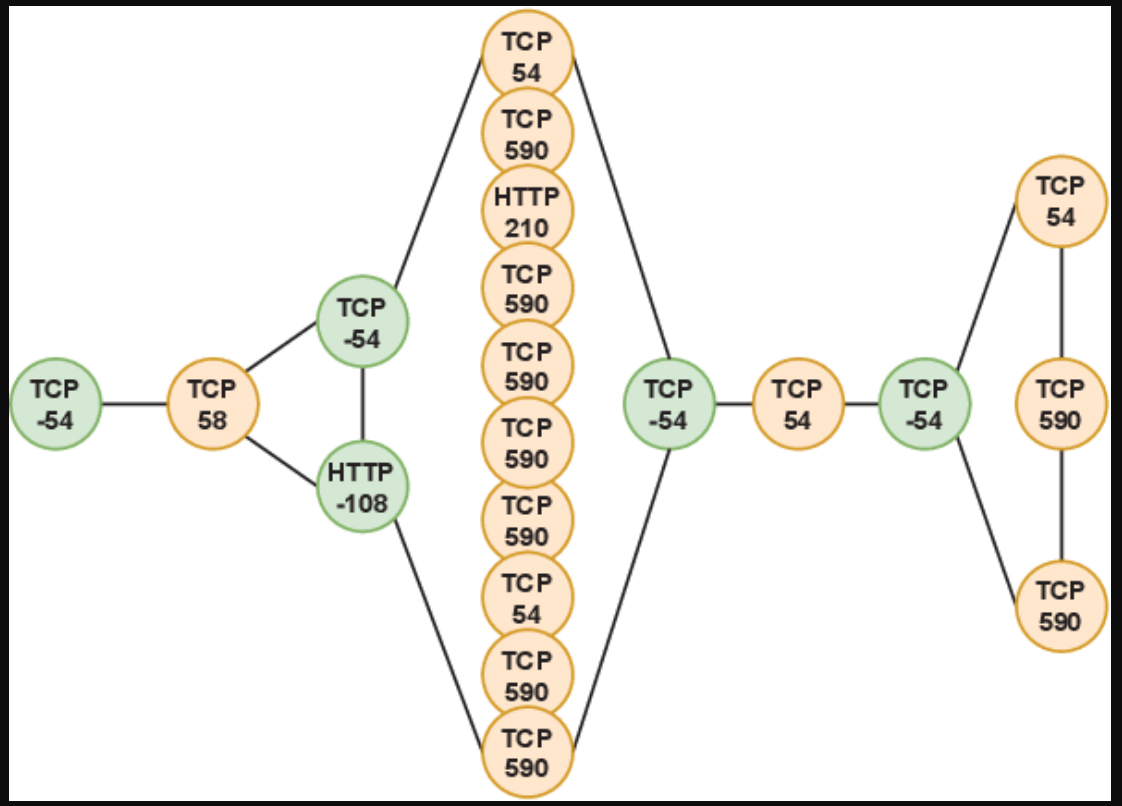
- When deployed, the ST-GCN continuously monitors the network state.
- It analyzes the graph-based representation of the network in real-time.
- If a DDoS attack is detected, the model identifies the specific switches and links involved.

GraphDDoS: Effective DDoS Attack Detection Using GNN

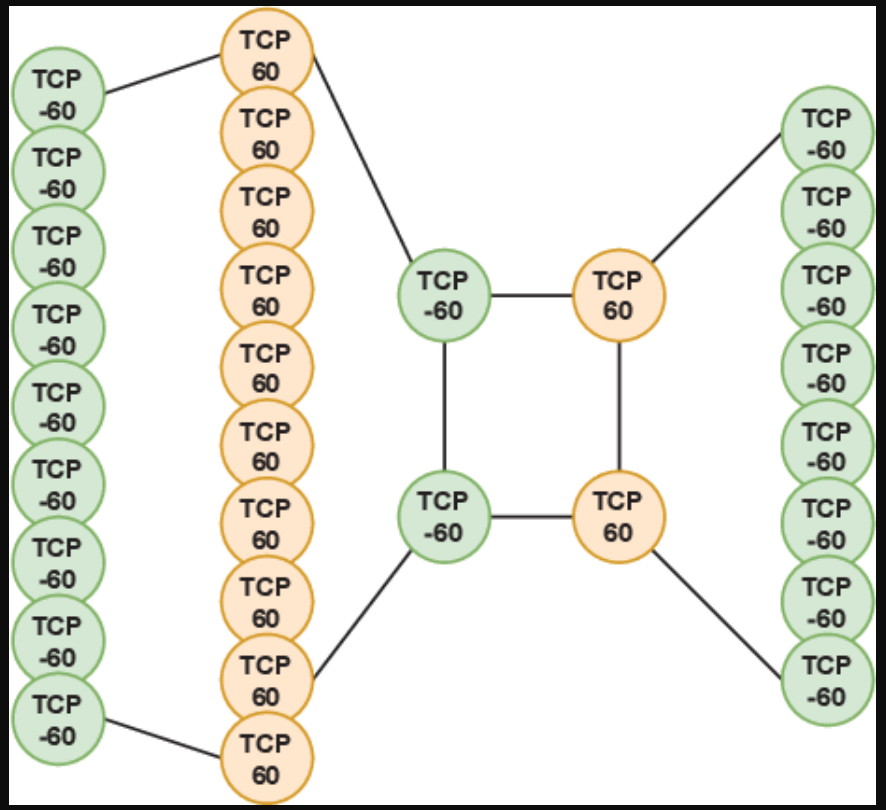
How's the network is modeled?

- Grouping Packets with the same source IP address and destination IP address.
- Sorting Packets based on their timestamp in ascending order.
- Packets are converted into nodes.
  - a pre-defined parameter determine the max number of nodes in a graph
  - node features are protocol type (e.g., TCP, UDP) of the packet.
- There are two types of edges:
  - Edges between consecutive packets in the same direction (client to server or server to client)
  - Edges between the last packet in one direction and the first packet in the opposite direction.

GraphDDoS: Effective DDoS Attack Detection Using GNN

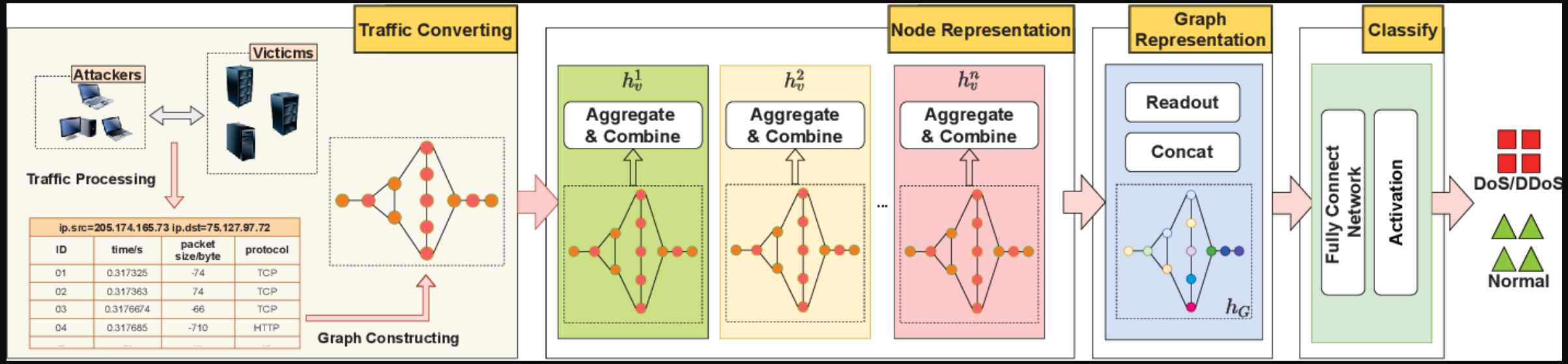


The endpoint traffic graph of HTTP GET attack.



The endpoint traffic graph of SYN flood attack.

GraphDDoS: Effective DDoS Attack Detection Using GNN



The architecture of GraphDDoS

References

[1] Cao, Yongyi, et al. "Detecting and mitigating DDoS attacks in SDN using spatial-temporal graph convolutional network." IEEE Transactions on Dependable and Secure Computing 19.6 (2021): 3855-3872.

[2] Li, Yuzhen, et al. "Graphddos: Effective ddos attack detection using graph neural networks." 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE, 2022.

Thank You