Graph Neural Network based Intrusion Detection and its Robustness against Adversarial Attacks

Romain Moreau[1] Thomas Winninger[1]

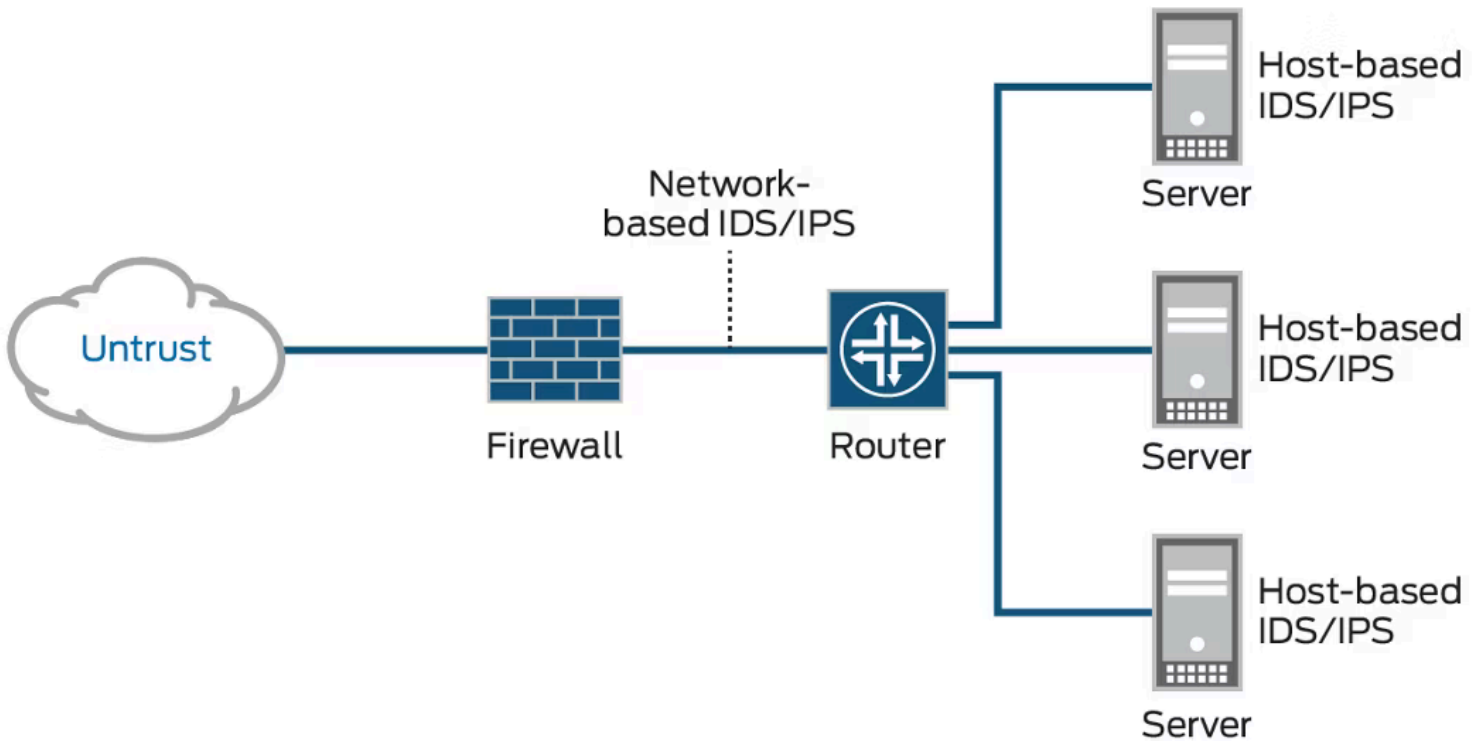
Gregory Blanc[2]

June 17, 2024

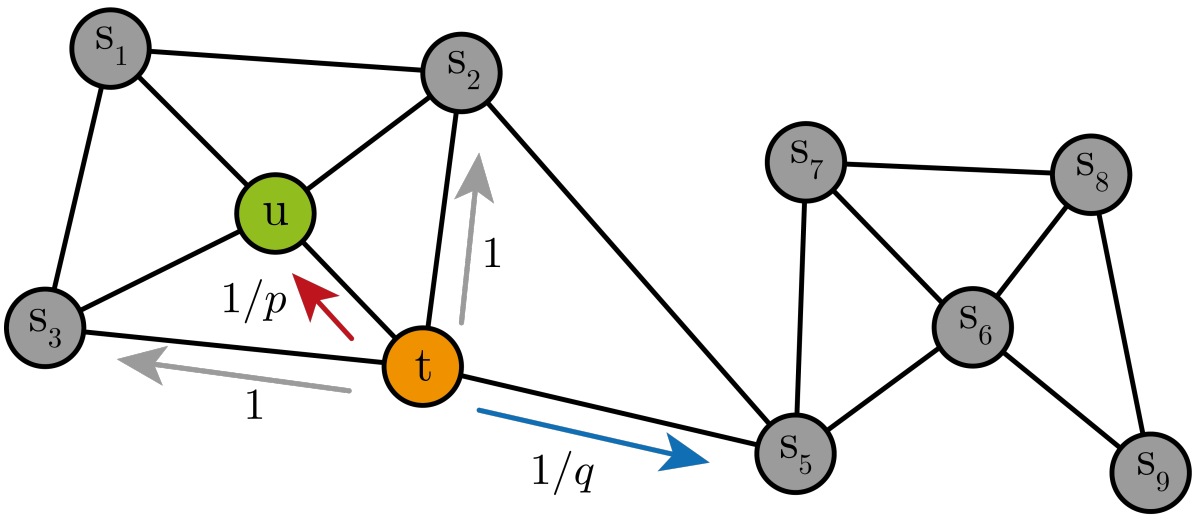
[1]Students - Télécom SudParis

[2]Supervisor - Télécom SudParis

Intrusion Detection System

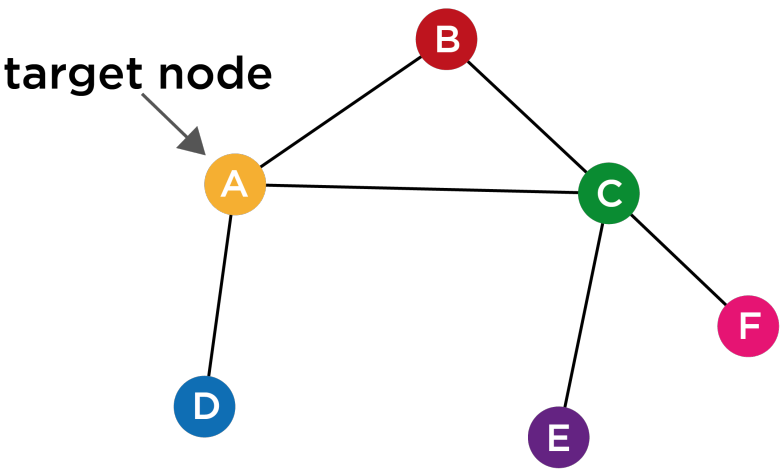


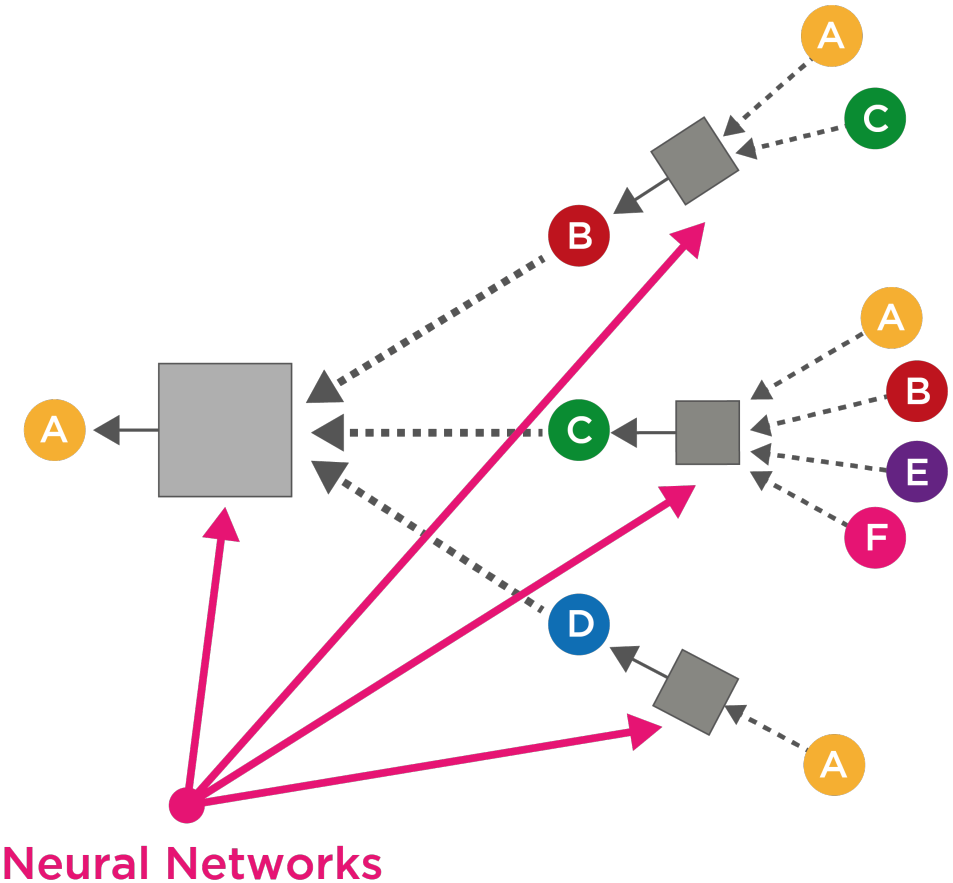
Graph Neural Network



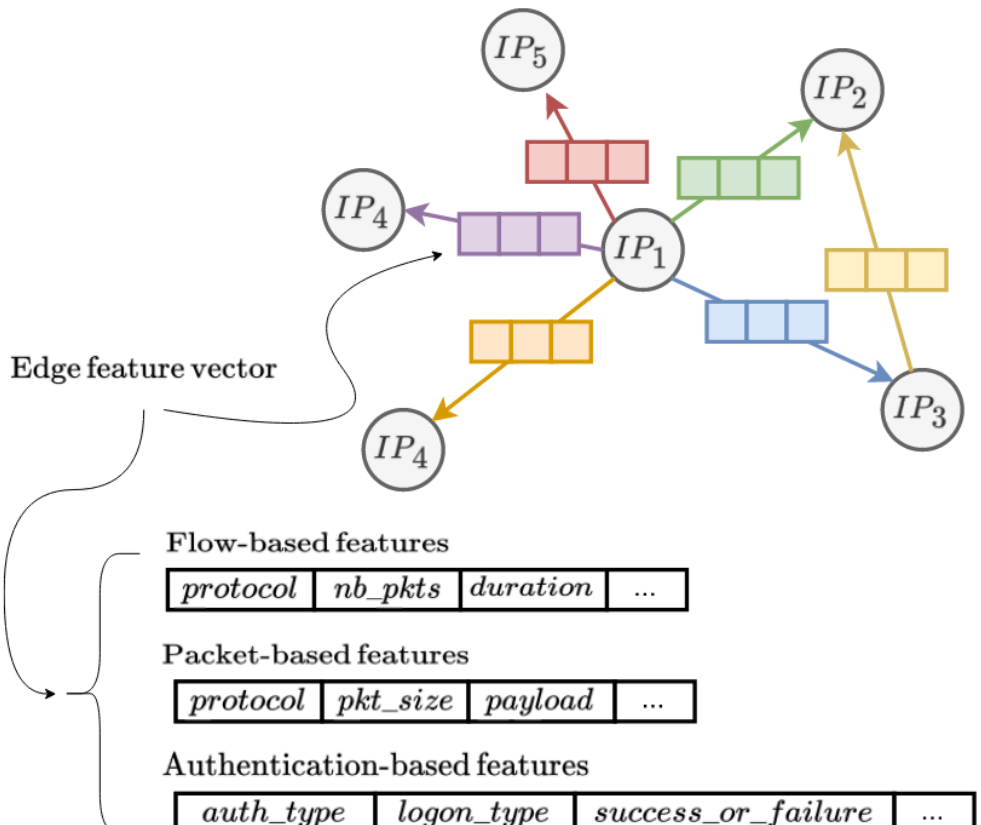
$$\alpha_{pq}(u,x) = \begin{cases} 1/p & \text{if } d(u,x) = 0 \\ 1 & \text{if } d(u,x) = 1 \\ 1/q & \text{if } d(u,x) = 2 \end{cases}$$

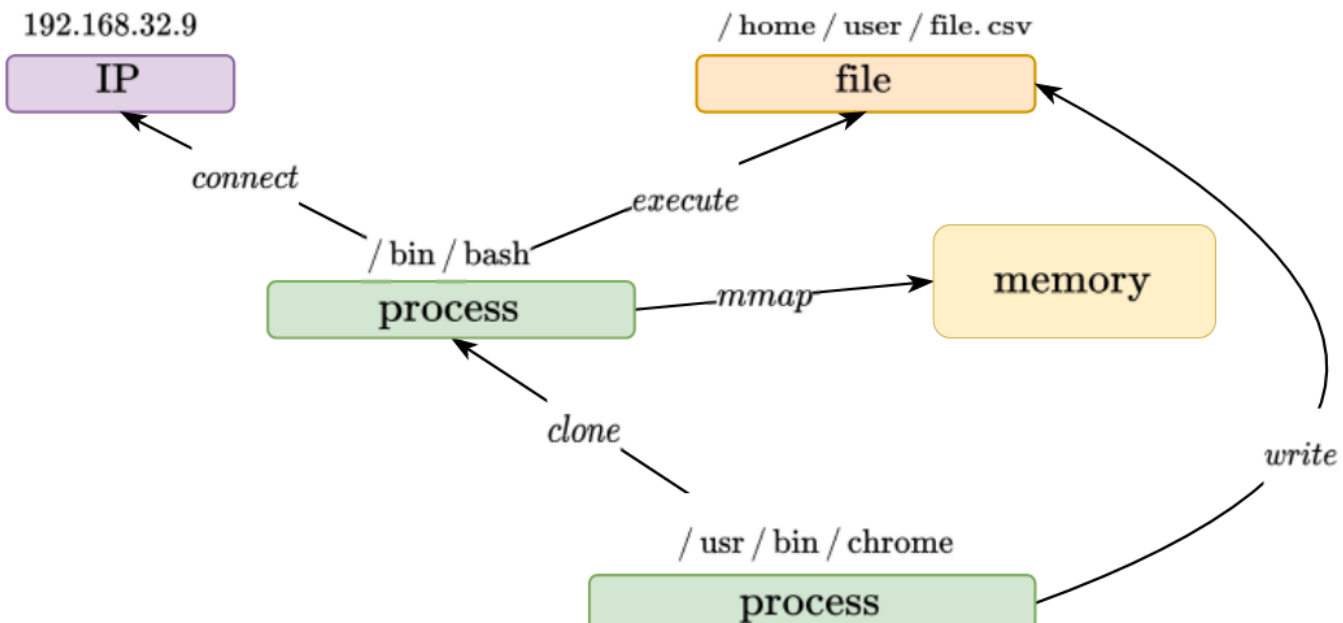
$d(u,x)$: shortest path length between node u to x

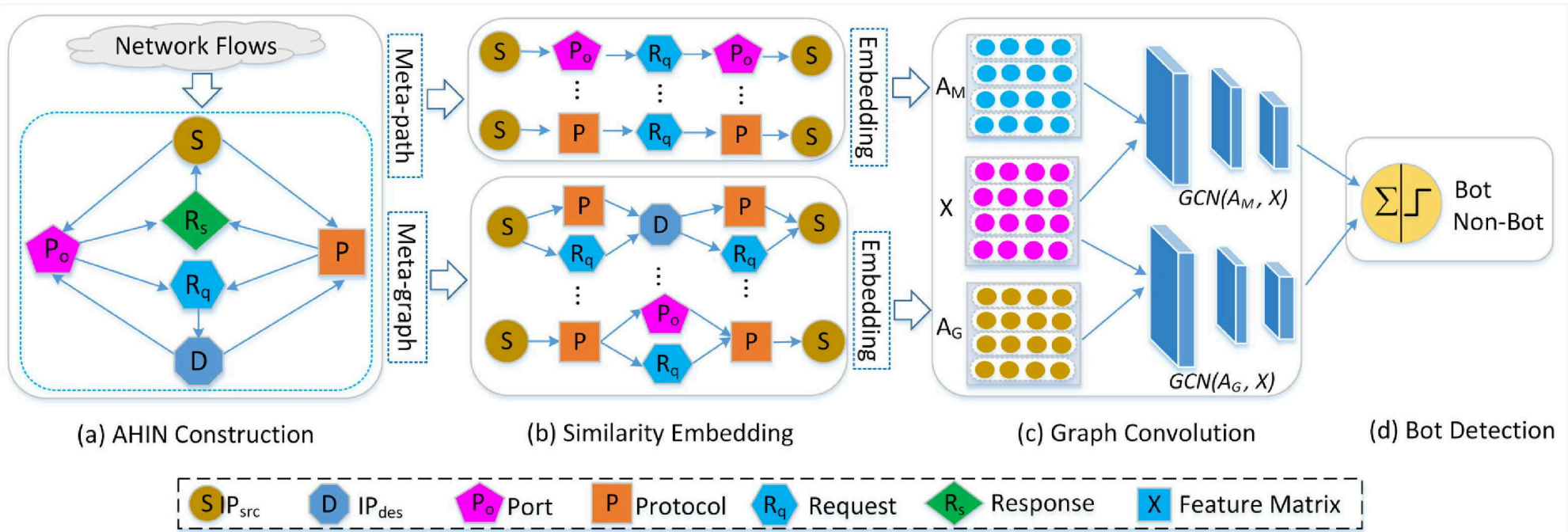

target node
A
B
C
D
E
F

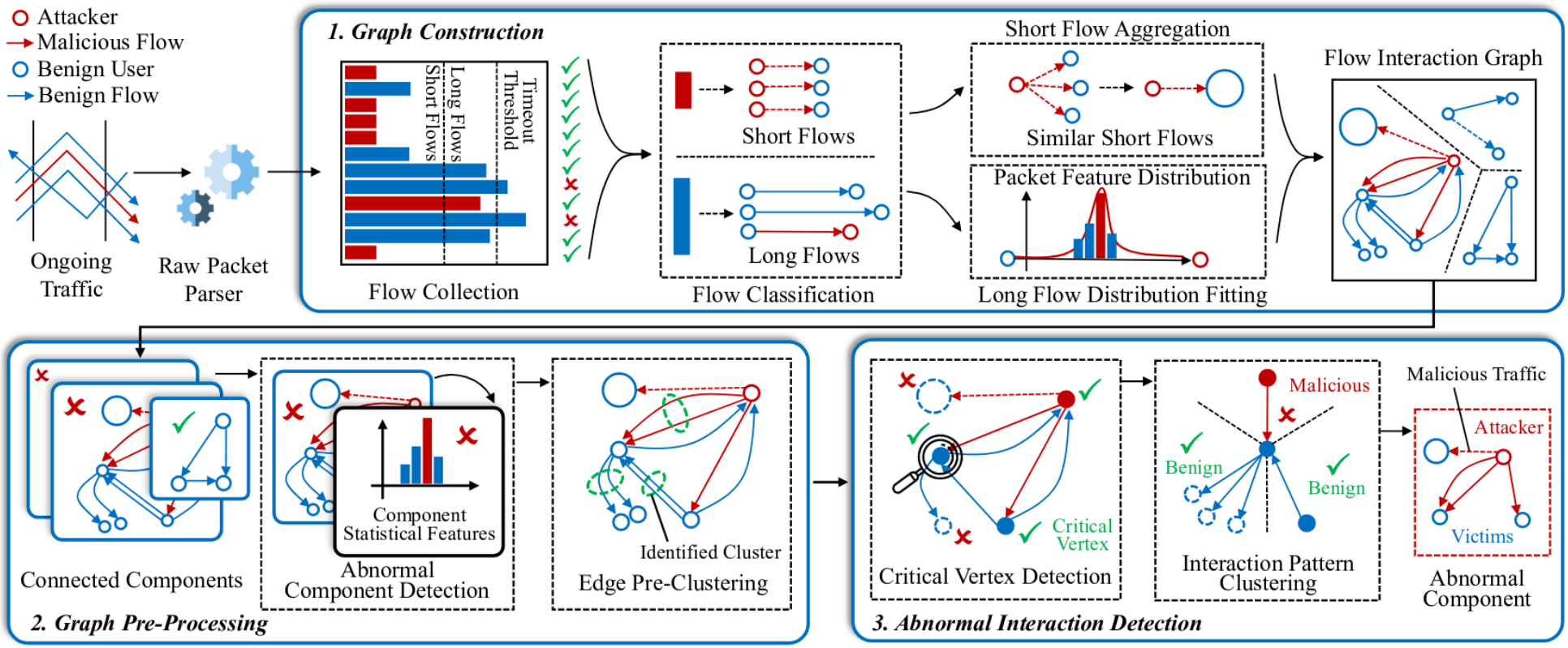

A
C
B
A
B
E
F
A
C
D
A
Neural Networks

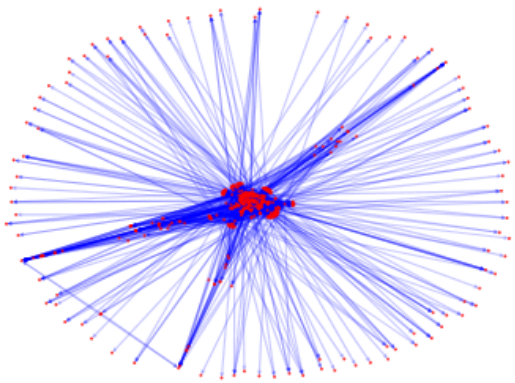
GNN-based IDS



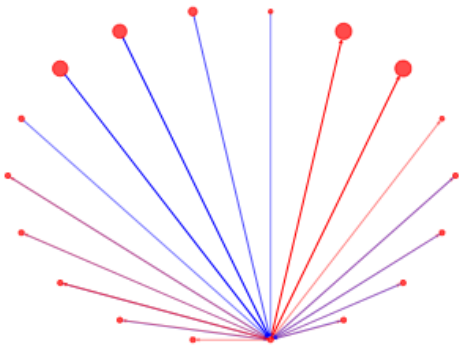

192.168.32.9
IP
/ home / user / file. csv
file
connect
execute
/ bin / bash
process
mmap
memory
clone
write
/ usr / bin / chrome
process


Network Flows
S
Po
Rs
Rq
P
D
Meta-path
Meta-graph
Embedding
Embedding
AM
X
AG
GCN(AM, X)
GCN(AG, X)
Bot
Non-Bot
(a) AHIN Construction
(b) Similarity Embedding
(c) Graph Convolution
(d) Bot Detection
S IPsrc
D IPdes
Po Port
P Protocol
Rq Request
Rs Response
X Feature Matrix

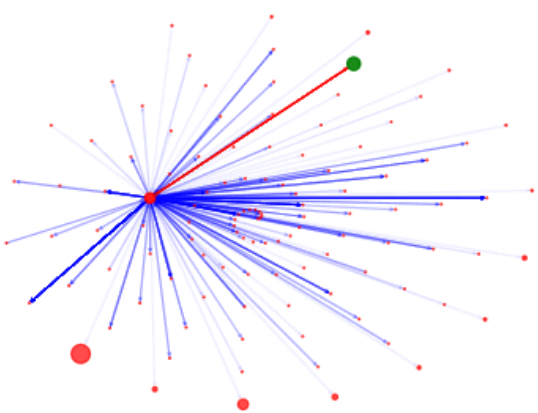

Attacker
Malicious Flow
Benign User
Benign Flow
Ongoing Traffic
Raw Packet Parser
1. Graph Construction
Timeout Threshold
Long Flows
Short Flows
Flow Collection
Short Flows
Long Flows
Flow Classification
Short Flow Aggregation
Similar Short Flows
Packet Feature Distribution
Long Flow Distribution Fitting
Flow Interaction Graph
Connected Components
Component Statistical Features
Abnormal Component Detection
Identified Cluster
Edge Pre-Clustering
2. Graph Pre-Processing
Critical Vertex
Critical Vertex Detection
Malicious
Benign
Benign
Interaction Pattern Clustering
Malicious Traffic
Attacker
Victims
Abnormal Component
3. Abnormal Interaction Detection



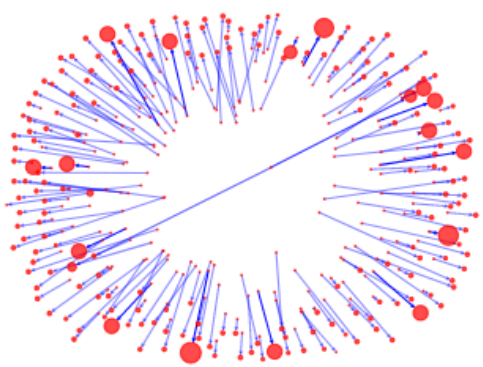
(a) Crossfire.



(b) SSH cracking.

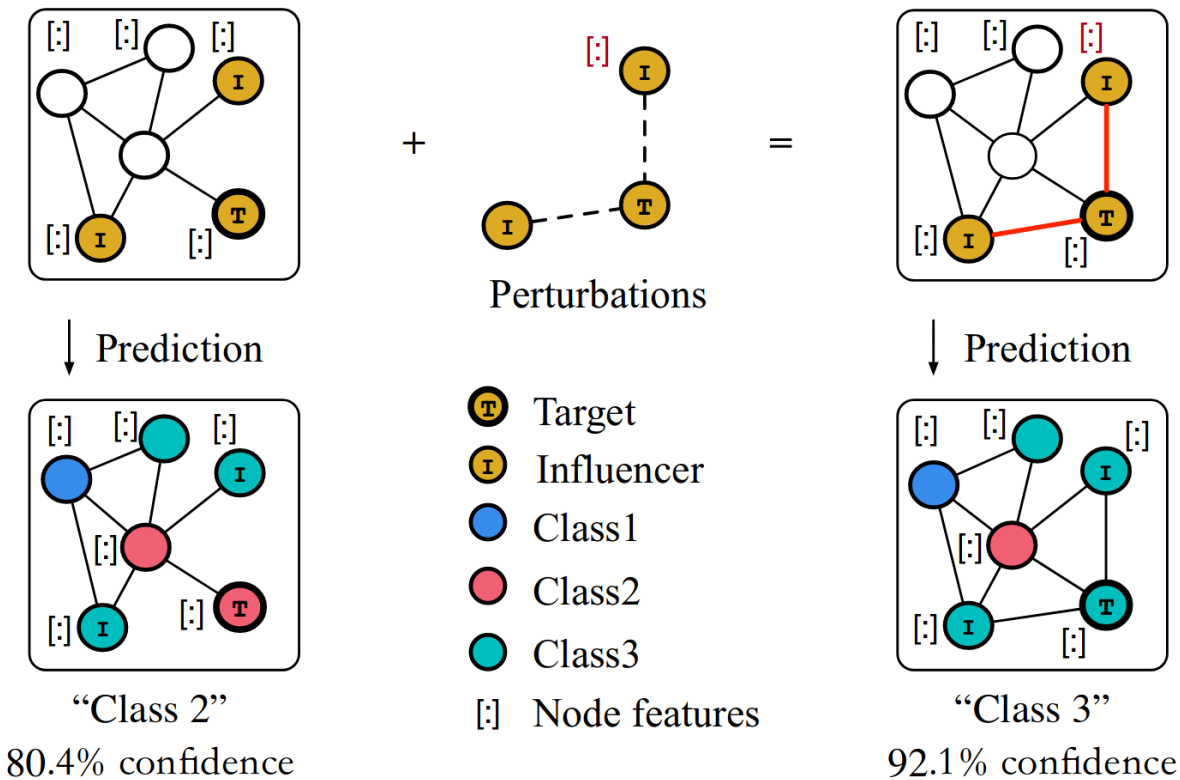


(c) XSS detection.



(d) P2P botnet.

GNN adversarial attacks



Conclusion