GNN based IDS and its robustness against adversarial attacks[1]

Le magicien quantique[2]

May 28, 2024

[1] Following a presentation with *le grand Racoon*

[2] Aka Sckathach, Caml Master, Fan2Thermo

IDS? IPS? *NANI??*

Intrusion Detection System

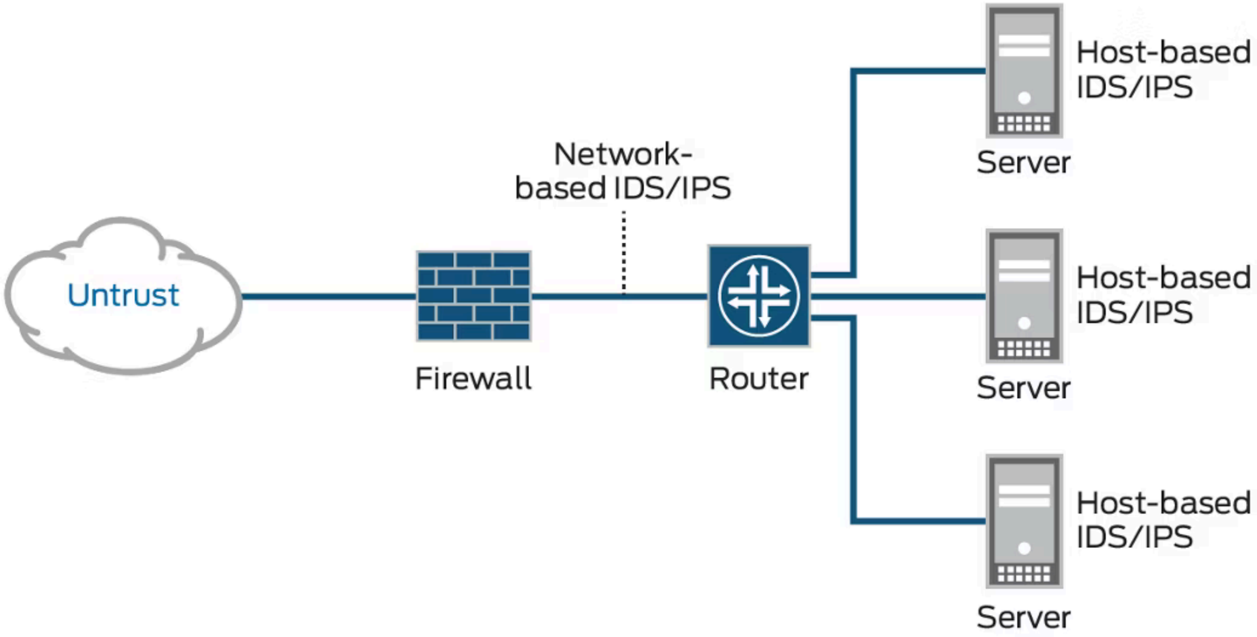
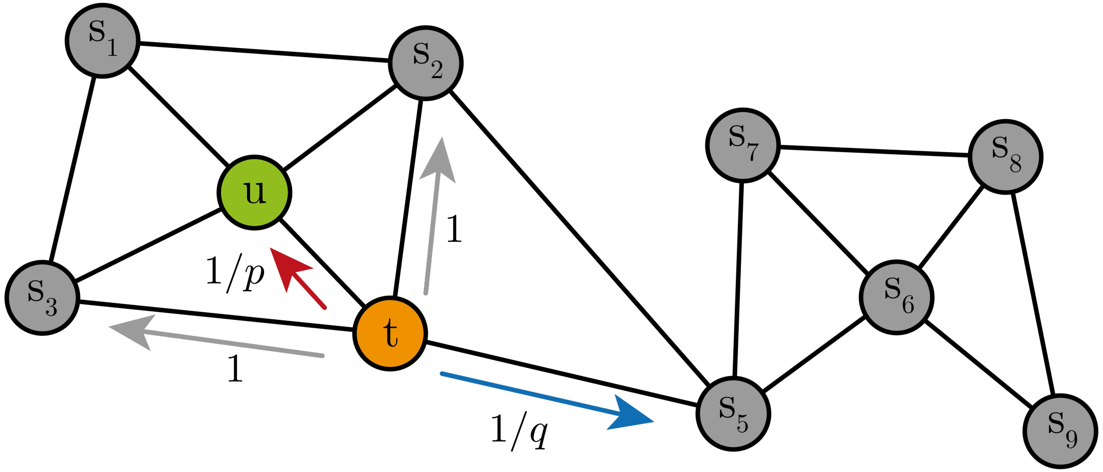


Figure 1: Juniper, What is IDS and IPS? [1]

GNN? *MO??*

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

Figure 2: A. Grover et al. “node2vec: Scalable Feature Learning for Networks”, 2016 [2]

GNN? *MO??*

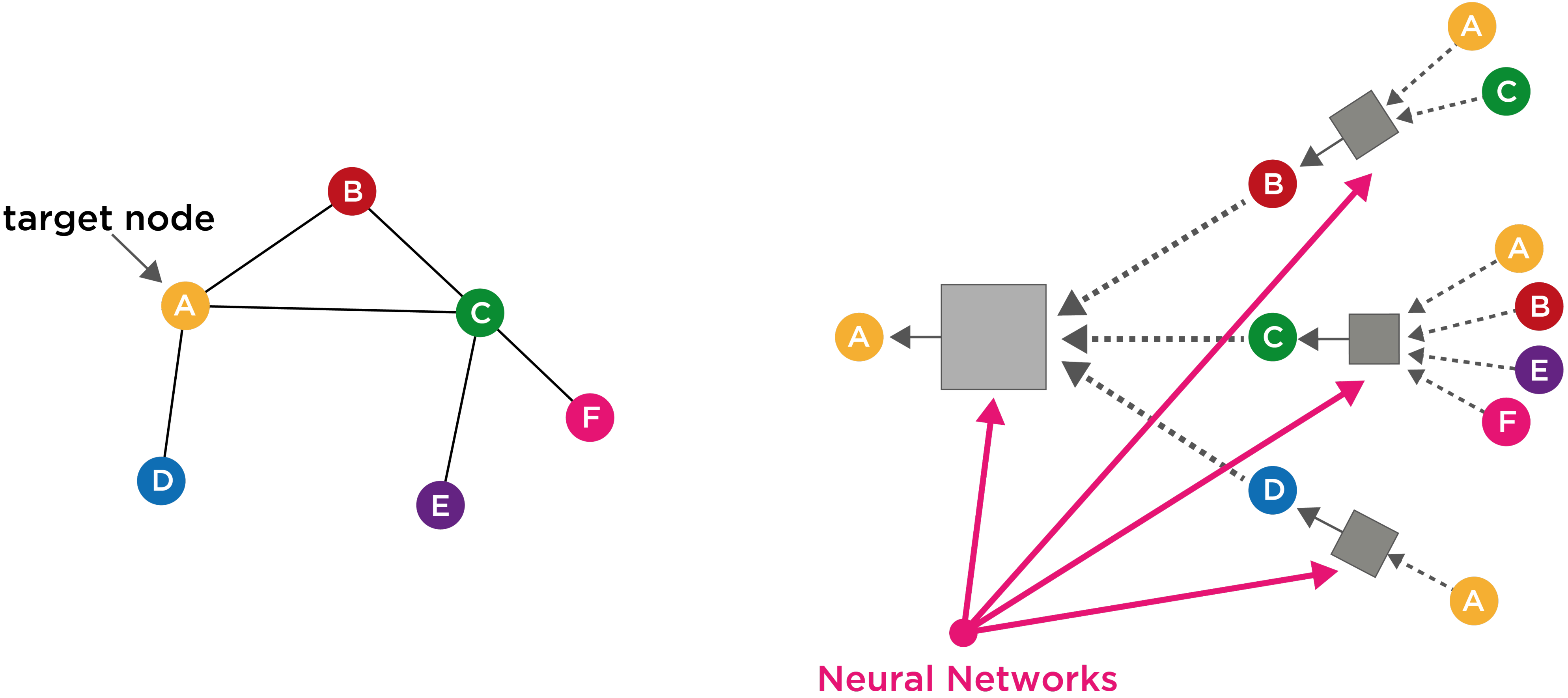
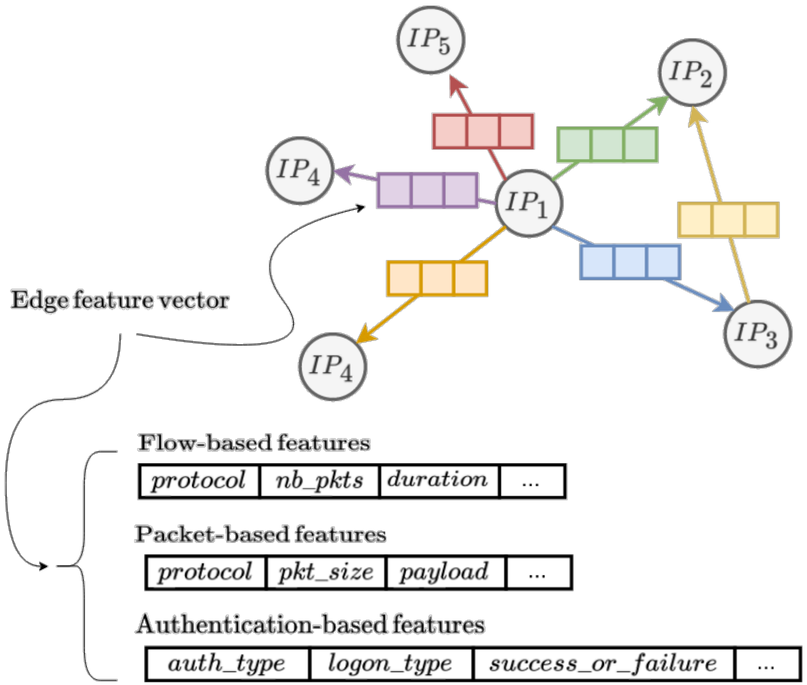


Figure 3: Z. Jin et al. “GNNVis: A Visual Analytics Approach for Prediction Error Diagnosis of Graph Neural Networks”, 2020 [3]

GNN + IDS = GNN based IDS :eyes:

GNN-based IDS



Flow-based features

protocol	nb_pkts	duration	...

Packet-based features

protocol	pkt_size	payload	...

Authentication-based features

auth_type	logon_type	success_or_failure	...

Figure 4: T. Bilot et al. “Graph Neural Networks for Intrusion Detection: A Survey”, 2023 [4]

GNN + IDS = GNN based IDS :eyes:

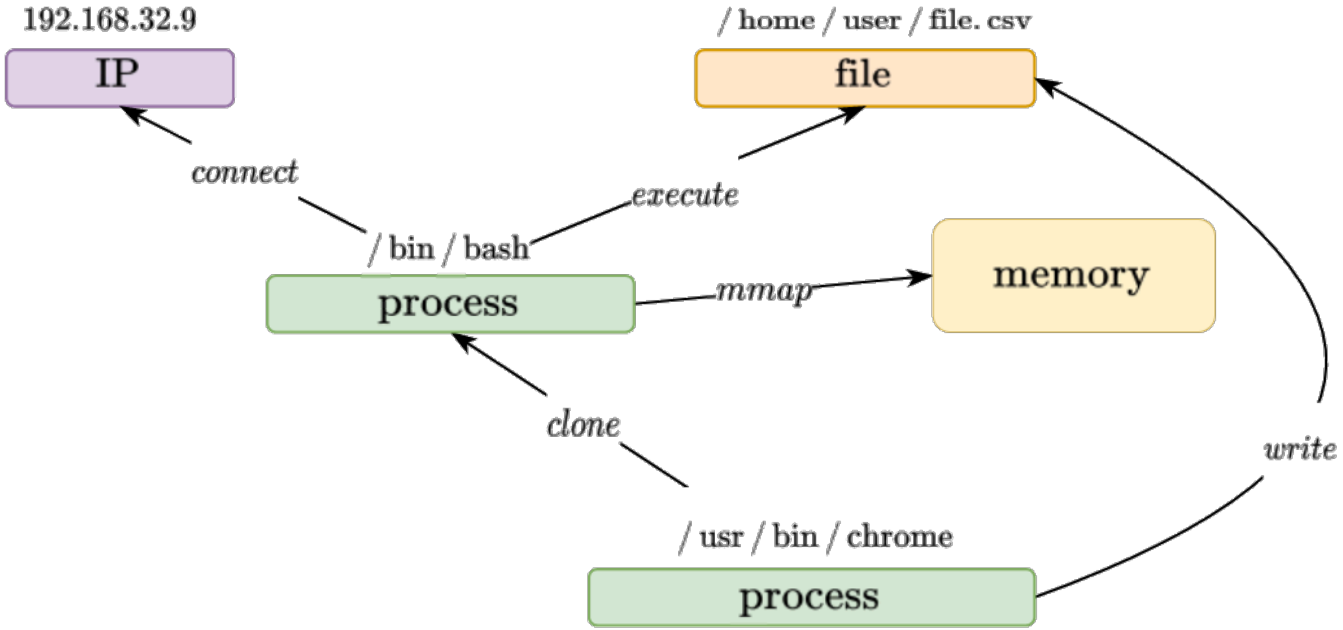


Figure 5: T. Bilot et al. “Graph Neural Networks for Intrusion Detection: A Survey”, 2023 [4]

GNN + IDS = GNN based IDS :eyes:

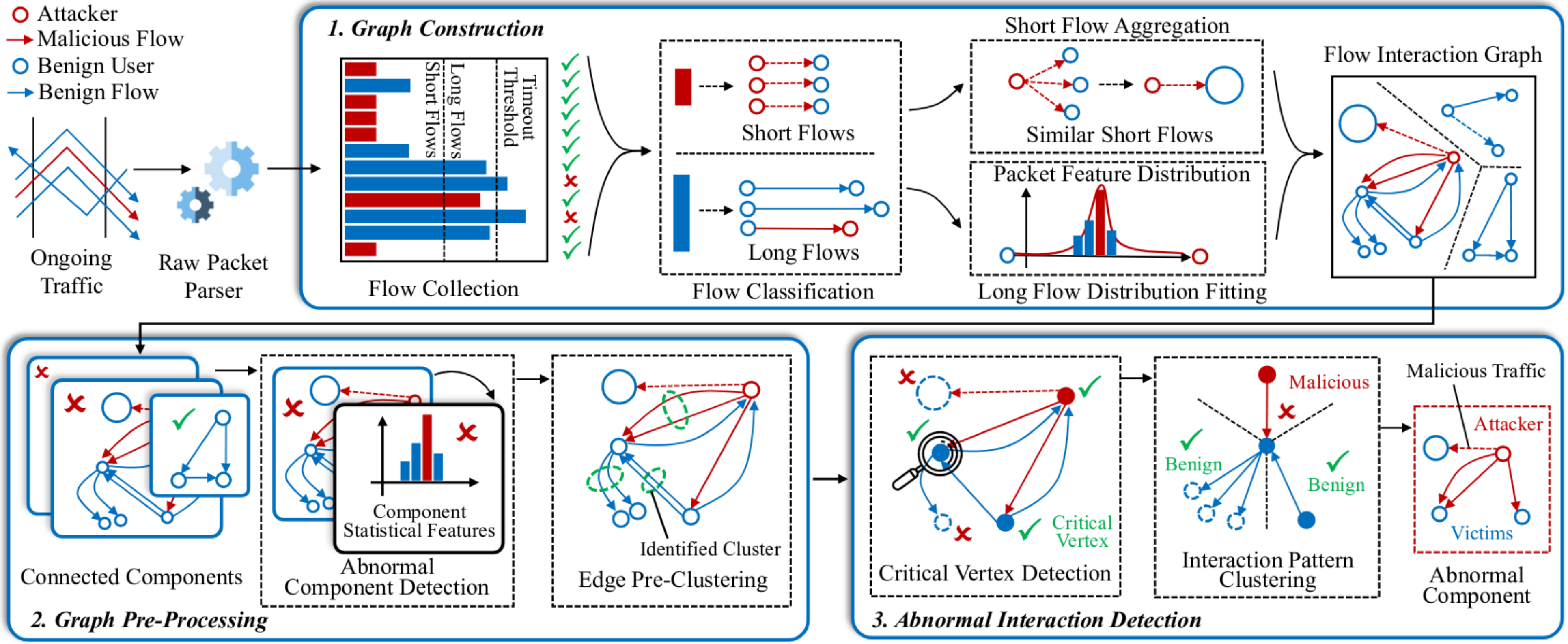
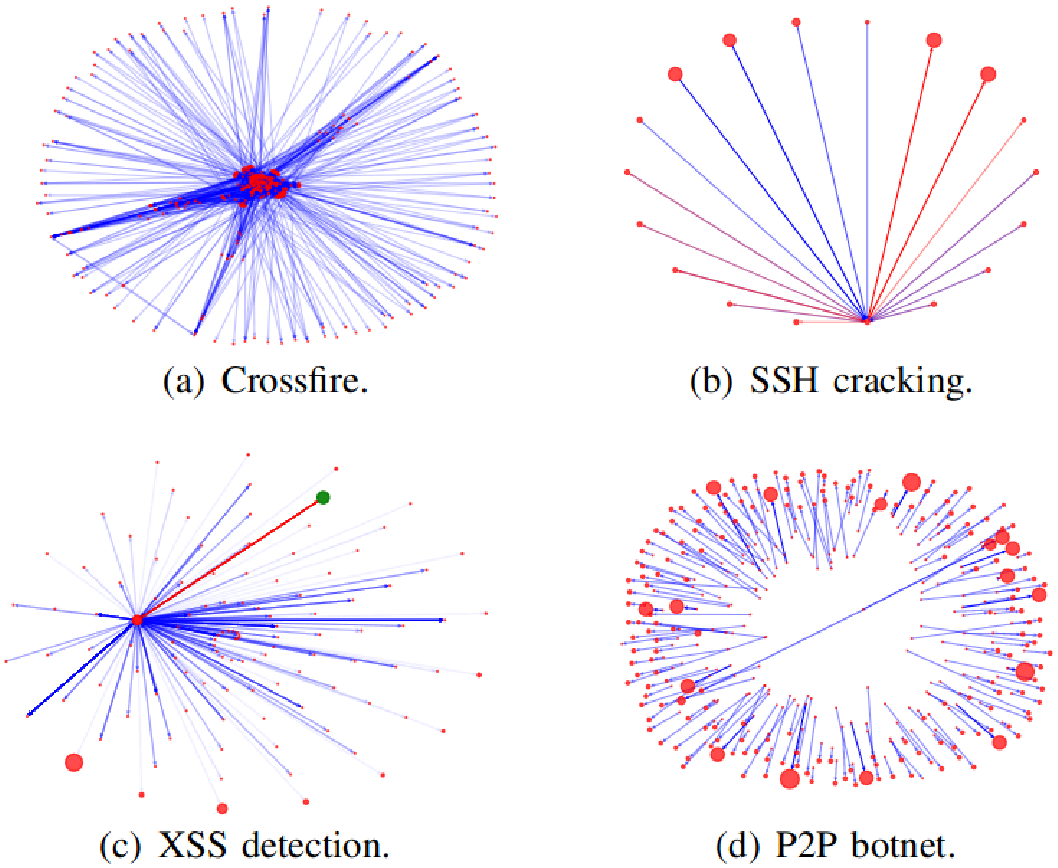


Figure 6: C. Fu et al. “Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis”, 2023 [5]

GNN + IDS = GNN based IDS :eyes:



(a) Crossfire.

(b) SSH cracking.

(c) XSS detection.

(d) P2P botnet.

Figure 7: C. Fu et al. “Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis”, 2023 [5]

AI to defend? → AI to attack the AI that defends

GNN adversarial attacks

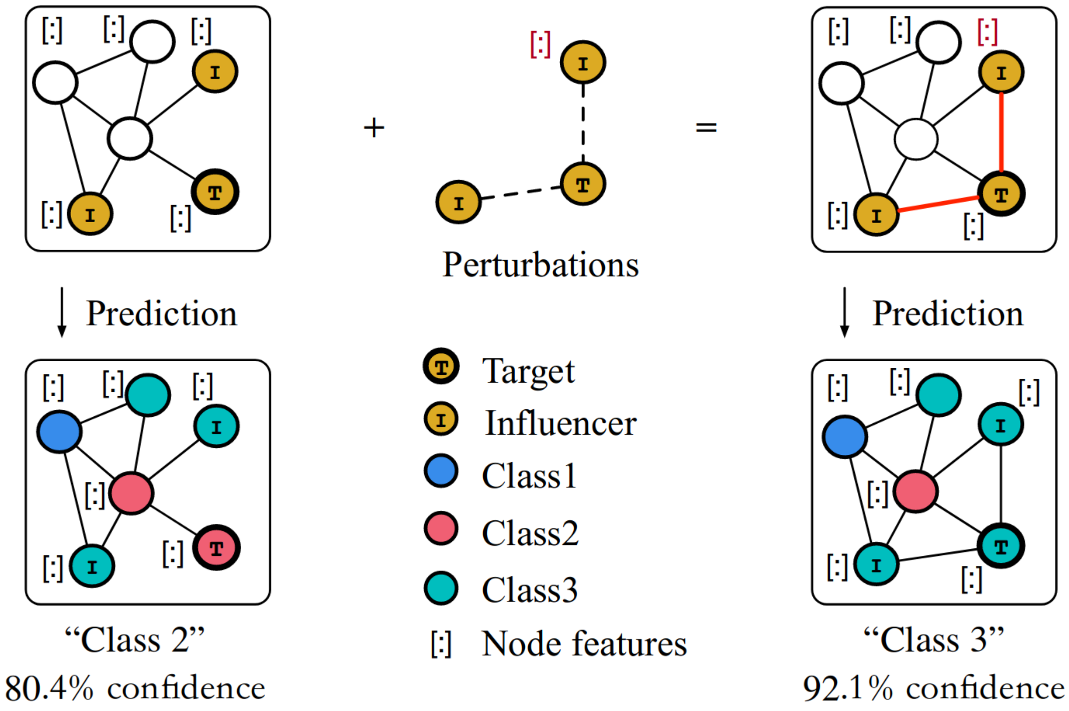


Figure 8: L. Chen et al. "A Survey of Adversarial Learning on Graphs", 2022 [6]

Genetic

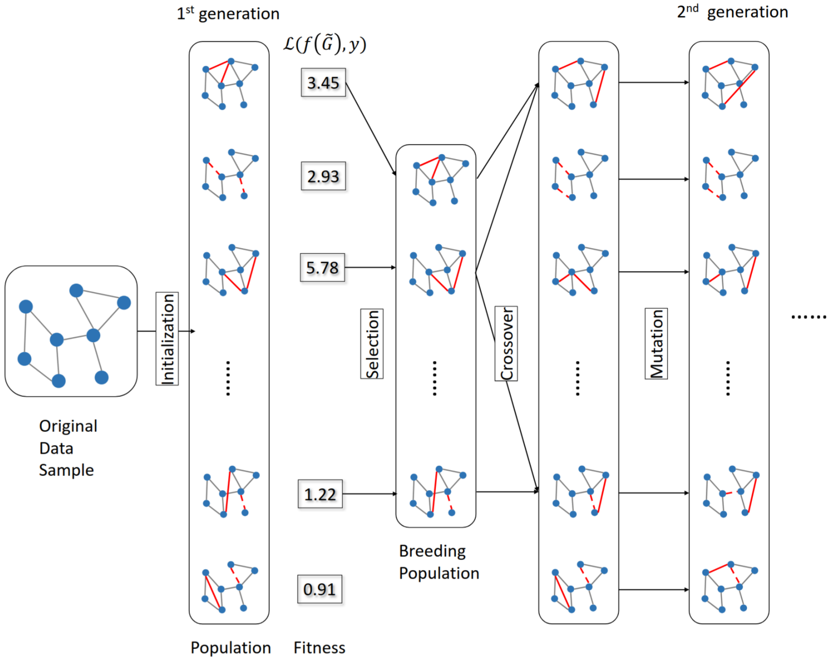


Figure 9: D. Hai, “Adversarial Attack on Graph Structured Data”, 2018 [7]

Black-box

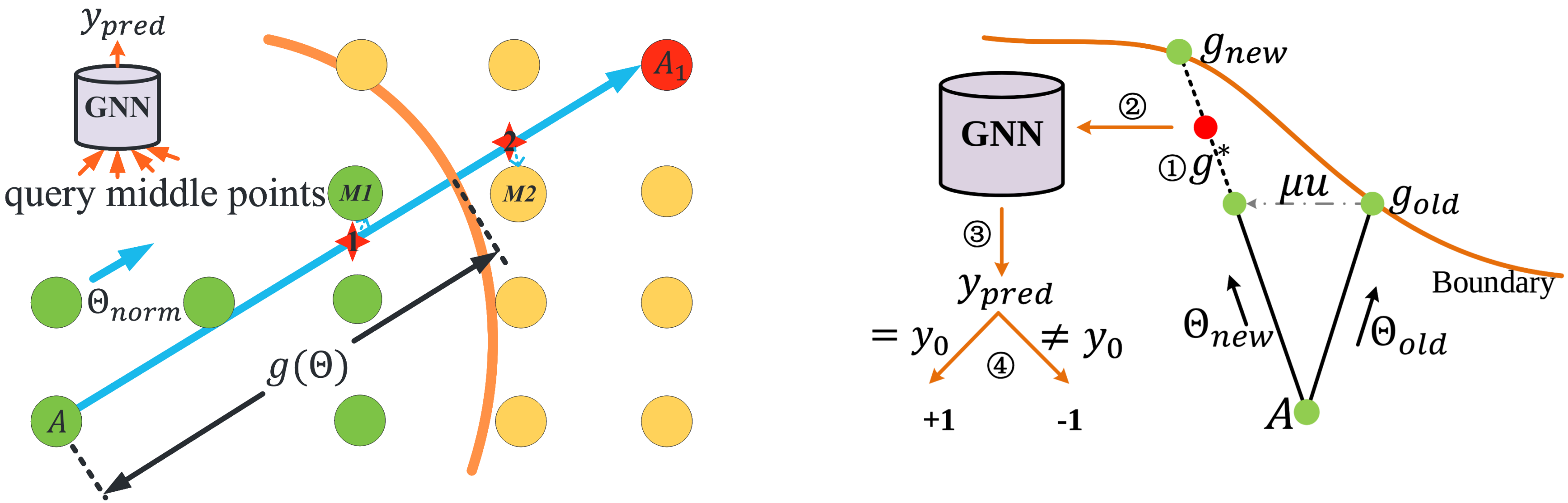


Figure 10: M. Jiaming et al. “A Hard Label Black-box Adversarial Attack Against Graph Neural Networks”, 2021 [8]

Conclusion

References

[1] Juniper, “What is IDS and IPS?.” [Online]. Available: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

[2] A. Grover and J. Leskovec, “node2vec: Scalable Feature Learning for Networks,” *CoRR*, 2016.

[3] Z. Jin, Y. Wang, Q. Wang, Y. Ming, T. Ma, and H. Qu, “GNNVis: A Visual Analytics Approach for Prediction Error Diagnosis of Graph Neural Networks,” p. , 2020.

[4] T. Bilot, N. E. Madhoun, K. A. Agha, and A. Zouaoui, “Graph Neural Networks for Intrusion Detection: A Survey,” *IEEE Access*, vol. 11, pp. 49114–49139, 2023, doi: 10.1109/ACCESS.2023.3275789.

[5] C. Fu, Q. Li, and K. Xu, “Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis.” arXiv, Jan. 2023.

[6] L. Chen *et al.*, “A Survey of Adversarial Learning on Graphs,” no. arXiv:2003.05730. arXiv, Apr. 05, 2022.

[7] H. Dai *et al.*, “Adversarial Attack on Graph Structured Data.” 2018.

[8] J. Mu, B. Wang, Q. Li, K. Sun, M. Xu, and Z. Liu, “A Hard Label Black-box Adversarial Attack Against Graph Neural Networks.” 2021.