GNN4IFA: Interest Flooding Attack Detection with Graph Neural Networks

Andrea Agiollo*
University of Bologna

Enkeleda Bardhi*
Sapienza University of Rome

Mauro Conti
University of Padua
Delft University of Technology

Riccardo Lazzeretti
Sapienza University of Rome

Eleonora Losiouk
University of Padua

Andrea Omicini
University of Bologna



Artifact

8-th IEEE European Symposium on Security and Privacy
Delft, July 6, 2023

Context: Information-Centric Networking

- The next generation Internet - TRIAD Project 2000 [1]
- Named-Data Networking [2] replacement of the IP layer with a information-centric layer
- Benefits:
  - reduction of network load/traffic
  - delay improvement
  - better support for distributed services
  - privacy-and-authenticity-by-design

Context: Information-Centric Networking

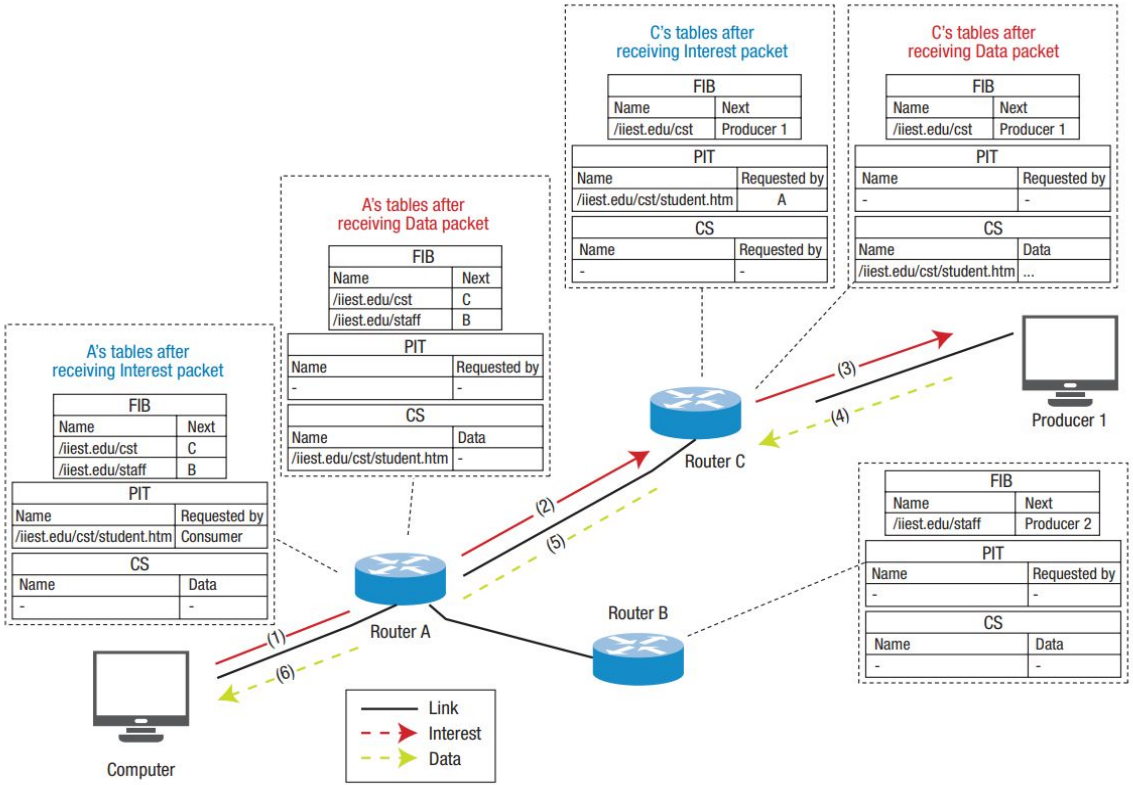


Image courtesy: Chatterjee, Tanusree, Sushmita Ruj, and Sipra Das Bit. "Security issues in named data networks." *Computer* 51.1 (2018)

Common NDN Attacks and Vulnerabilities

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Interest Flooding Attacks (IFA)

- PIT saturation
- congest the network
- deny/degrade the service for legitimate users

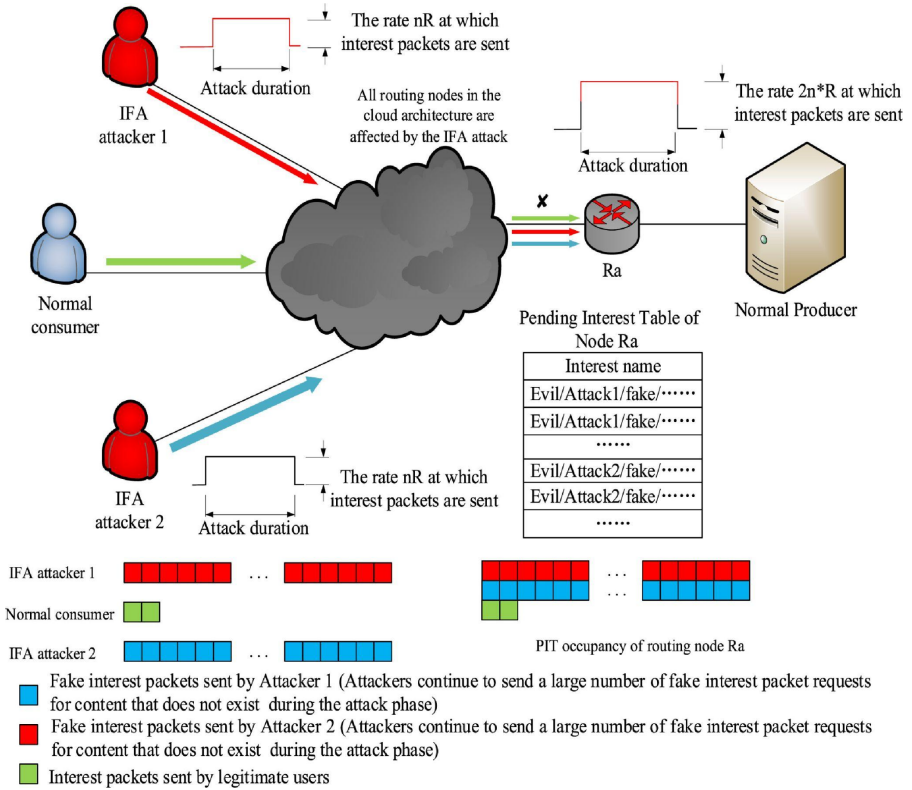


Image courtesy: Wu, Zhijun, et al. "I-CIFA: An improved collusive interest flooding attack in named data networking." *Journal of Information Security and Applications* 61 (2021)

SOTA for IFA Detection

- Two detection approaches:
  - Threshold-based
  - ML-based

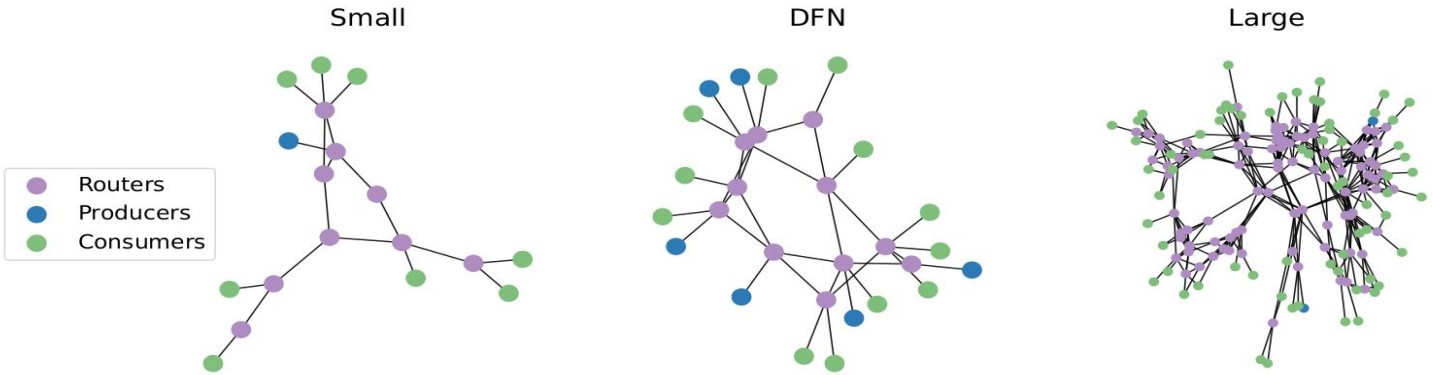
- Limitations of SOTA approaches:
  - locality issue
  - solutions are designed and implemented in small network topologies
  - missing datasets for designing data-driven solutions

GNN4IFA: Criteria to meet

C1: Global IFA Detection Mechanism	**GNNs** enable information extraction from the whole NDN network graph
C2: Adaptable to heterogeneous topologies	**GNNs** are proven to generalize well between different graph structures
C3: Large and representative network traffic	**SPOTIFAI** is the first comprehensive IFA's dataset
C4: Robust and efficient detection	**GNNs** reach reasonably time efficient results even in huge-scale graphs

SPOTIFAI: SPOTting IFA Intruders

- Generic NDN network: routers, consumers and producers
  - Three widely used topologies in SOTA
- All producers handle requests for content from a specific namespace



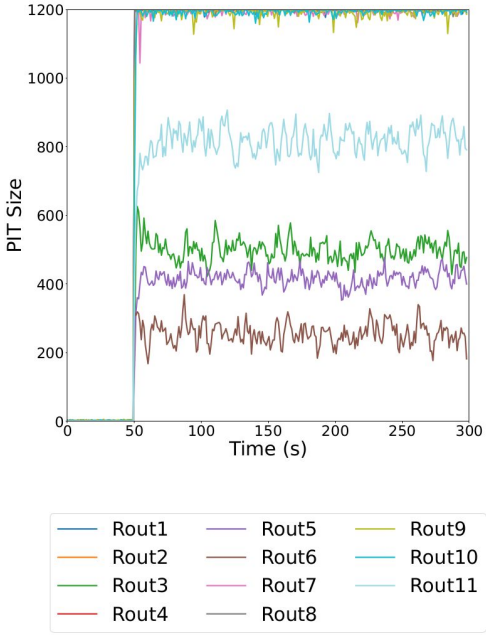
SPOTIFAI: SPOTting IFA Intruders

- ➢ Attacker targets an existing valid content namespace to deny access to it
- ➢ SPOTIFAI is collected using ndnSIM and encompasses 12 features collected in different simulation scenarios

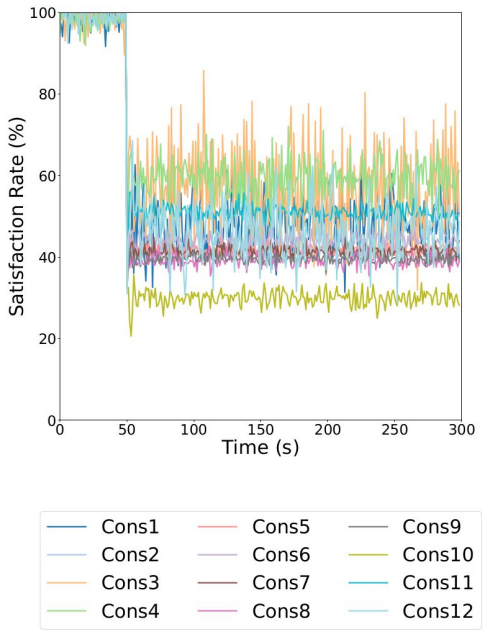
Feature Symbol	Description
f_1^l	# of received interests in an interface l
f_2^l	# of sent interests through an interface l
f_3^l	# of arrived data in an interface l
f_4^l	# of sent data through an interface l
f_5^l	# of satisfied interests per an incoming interface l
f_6^l	# of satisfied interests per an outgoing interface l
f_7^l	# of timed out interests per an incoming interface l
f_8^l	# of timed out interests per an outgoing interface l
f_9^l	# of NACKs per an incoming interface l
f_{10}^l	# of NACKs per an outgoing interface l
f_{11}	cumulative measurements of dropped packets per node
f_{12}	# of PIT entries per node

Simulation Parameter	Value
Simulation duration	300s
Statistics collection time	1s
Maximum PIT size	1200
Legitimate users frequency	U∼[50-150] interests/s
Attackers frequency coefficient	[4x, 8x, 16x, 32x, 64x]
Attackers number	Small-scale: 4, 5, 6, 7
	DFN: 4, 8, 11
	Large: 15, 36, 64
Legitimate users runtime	0-300s
Attackers runtime	50-300s

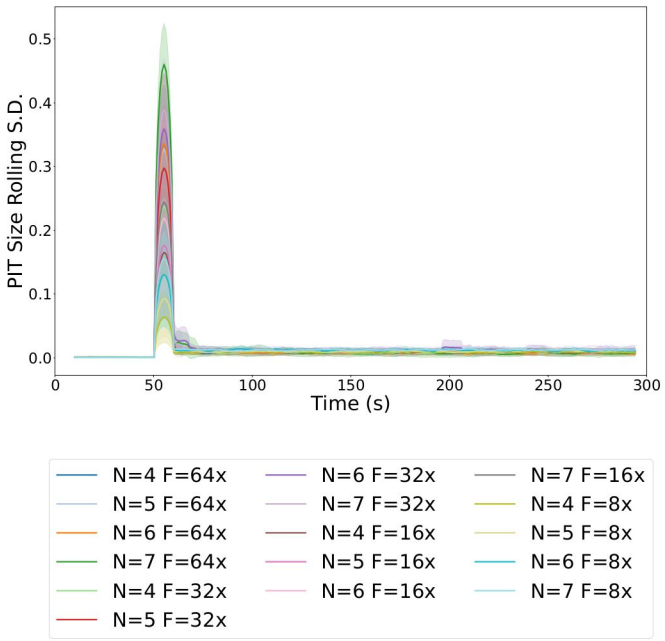
SPOTIFAI: SPOTting IFA Intruders



DFN Topology: F=32x, N=8



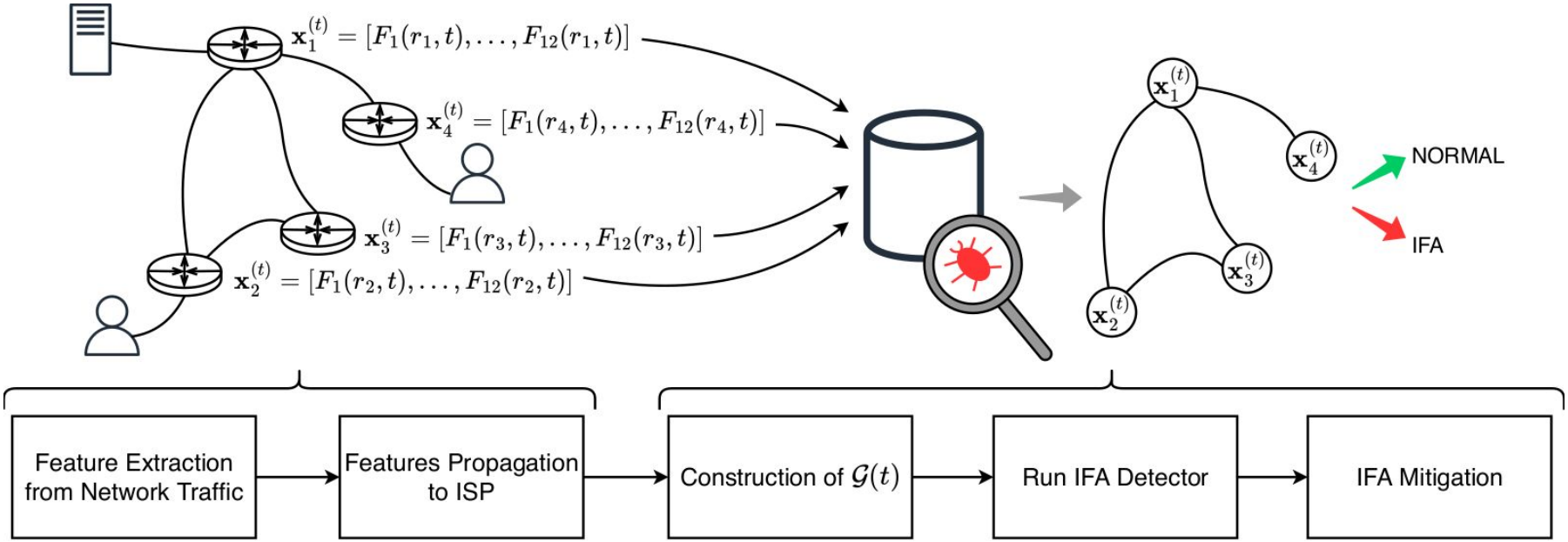
DFN Topology: F=32x, N=8



DFN Topology, all setups

Effect of IFA – i.e., PIT consumption, consumer satisfaction rate, and PIT size rolling standard deviation on the DFN topology

GNN4IFA: Overview



The routers of the NDN network collect features that characterise the traffic. These features are propagated to the ISP which is in charge of running the detection mechanism – SAD or UAD – and the attack mitigation.

GNN4IFA: NDN Network as a Graph

G(t) = {X(t), A(t)} represents the graph for NDN network at time *t*

- $\mathbf{A}^{NxN}$ represents the binary adjacency matrix for routers interconnections, where:

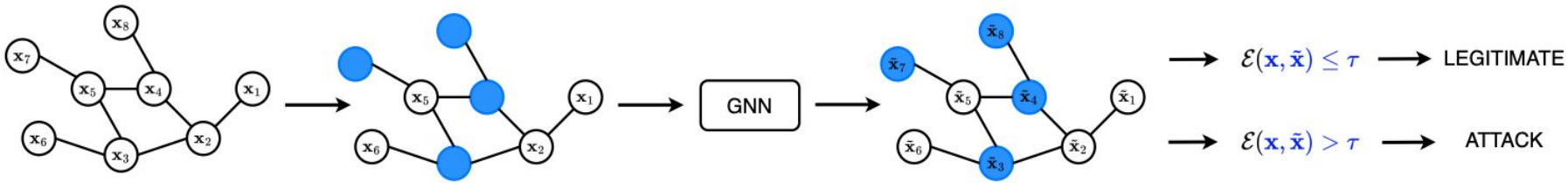
$$a_{i,j}(t) = \begin{cases} 1, & \text{if } link(r_i, r_j, t) = 1 \\ 0, & \text{otherwise} \end{cases}$$

- ***X(t)*** represents routers states, where:

$$\mathbf{X}(t) = \begin{bmatrix} \mathbf{x}_1(t) \\ \vdots \\ \mathbf{x}_N(t) \end{bmatrix} = \begin{bmatrix} F_1(r_1,t) & \cdots & F_{12}(r_1,t) \\ F_1(r_2,t) & \cdots & F_{12}(r_2,t) \\ \vdots & \ddots & \vdots \\ F_1(r_N,t) & \cdots & F_{12}(r_N,t) \end{bmatrix} \quad \text{and} \quad F_k = \sum_{l=1}^{L} f_k^l \quad \text{with } k = [1, 10]$$

GNN4IFA: SAD & UAD

- Supervised Attack Detection (SAD) graph classification task
  - GNN outputs a single label for the whole graph (attack or legitimate)
  - GNN training requires both legitimate and attack samples
- Unsupervised Attack Detection (UAD) self-supervised graph classification
  - Mask nodes status and train GNN to reconstruct them
  - Compare reconstructed (predicted) states with ground truth to check network state
  - Anomalous status (IFA attacks) deviate from reconstructed values
  - UAD training requires only legitimate traffic samples



GNN4IFA: SAD and UAD Performance

N \ F	8×	16×	32×	64×	Avg.
4	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
5	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
6	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
7	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
Avg.	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	**100.0%** **100.0%**

N \ F	8×	16×	32×	64×	Avg.
4	92.1% 95.5%	95.6% 97.5%	97.0% 98.2%	95.0% 97.1%	94.9% 97.0%
7	100.0% 100.0%	99.9% 99.9%	100.0% 100.00%	100.0% 100.0%	100.0% 100.0%
11	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
Avg.	97.4% 98.5%	98.5% 99.1%	99.0% 99.4%	98.3% 99.0%	**98.3%** **99.0%**

N \ F	8×	16×	32×	64×	Avg.
15	93.1% 95.2%	100.0% 100%	99.5% 99.7%	100.0% 100.0%	98.4% 98.7%
16	100.0% 100.0%	100.0% 100.0%	100.0% 100.00%	100.0% 100.0%	100.0% 100.0%
65	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
Avg.	97.9% 98.4%	100.0% 100.0%	99.8% 99.9%	100.0% 100.0%	**99.5%** **99.6%**

SAD accuracy and F1-score over the small, DFN and large topology, from left to right.

N \ F	8×	16×	32×	64×	Avg.
4	100.0% 2.0%	100.0% 0.8%	100.0% 1.2%	100.0% 0.8%	100.0% 1.2%
5	100.0% 0.8%	100.0% 2.0%	100.0% 3.6%	100.0% 0.8%	100.0% 1.8%
6	100.0% 1.6%	100.0% 4.8%	100.0% 2.4%	100.0% 2.4%	100.0% 2.8%
7	100.0% 2.4%	100.0% 2.8%	100.0% 2.8%	100.0% 2.0%	100.0% 2.5%
Avg.	100.0% 1.7%	100.0% 2.6%	100.0% 2.5%	100.0% 1.5%	**100.0%** **2.1%**

N \ F	8×	16×	32×	64×	Avg.
4	100.0% 2.4%	100.0% 3.2%	100.0% 2.0%	100.0% 2.0%	100.0% 2.4%
8	100.0% 0.8%	100.0% 2.0%	100.0% 2.0%	100.0% 1.6%	100.0% 1.6%
11	100.0% 1.6%	100.0% 1.2%	100.0% 1.6%	100.0% 1.2%	100.0% 1.4%
Avg.	100.0% 1.6%	100.0% 2.1%	100.0% 1.8%	100, 0% 1.6%	**100.0%** **1.8%**

N \ F	8×	16×	32×	64×	Avg.
15	100.0% 1.0%	100.0% 0.0%	100.0% 1.0%	100.0% 0.0%	100.0% 0.5%
36	100.0% 0.0%	100.0% 3.0%	100.0% 1.0%	100.0% 2.0%	100.0% 1.5%
65	100.0% 0.0%	100.0% 0.0%	100.0% 1.0%	100.0% 0.0%	100.0% 0.25%
Avg.	100.0% 0.3%	100.0% 1.0%	100.0% 1.0%	100, 0% 0.6%	**100.0%** **0.75%**

UAD TPR and FPR over the small, DFN and large topology, from left to right.

GNN4IFA: SAD vs SOTA

SAD vs non ML-based Baselines

Baseline	Features	Topologies		
		Small	DFN	Large
[7]	$[\frac{f_1^l}{f_4^l}, \frac{f_{12}^l}{f_1^l}]$	99.0% 99.4%	79.9% 86.1%	93.9% 95.3%
[26]	$[\frac{f_{12}^l}{1200}, \frac{f_7^l}{f_7^l+f_5^l}]$	75.9% 83.0%	60.7% 68.7%	94.4% 95.4%
[24]	$[\frac{f_{12}^l}{1200}, \frac{f_7^l}{f_7^l+f_5^l}]$	66.5% 74.8%	81.0% 87.0%	91.8% 93.5%
[27]	$[\frac{f_3^l}{f_1^l}, f_1^l, f_7^l, f_9^l]$	83.2% 90.8%	82.3% 90.2%	61.4% 76.1%
[6]	$[\frac{f_1^l}{f_4^l}, \frac{f_{12}^l}{f_1^l}]$	88.3% 92.4%	43.3% 47.5%	88.9% 90.1%
GNN4IFA	**All**	**100.0%** **100.0%**	**98.3%** **99.0%**	**99.5%** **99.6%**

SAD outperforms all the non-ML baselines over all topologies.

GNN4IFA: SAD vs SOTA

SAD achieves identical or comparable results for the small and DFN topology, while it outperforms all the baselines for the large topology, confirming the superiority of global approaches.

SAD vs ML-based Baselines

Baseline	Features	Topologies		
		Small	DFN	Large
[29] (MLP)	$[F_1{:}F_6,\ F_{12}]$	100.0% 100.0%	100.0% 100.0%	93.6% 94.4%
[29] (SVM)	$[F_1{:}F_6,\ F_{12}]$	100.0% 100.0%	100.0% 100.0%	93.5% 94.3%
[28] (SVM)	$[F_{13} = \frac{F_3}{F_2},$ $F_{14} = \frac{F_{12}}{1200}]$	100.0% 100.0%	95.2% 97.1%	93.5% 94.4%
[31] (RF)	$[F_2,\ F_3,$ $F_8,\ F_{12}]$	100.0% 100.0%	100.0% 100.0%	93.5% 94.4%
[30] (DT)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	100.0% 100.0%	99.9% 99.9%	78.6% 78.6%
[30] (NB)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	83.2% 90.8%	82.3% 90.3%	60.7% 75.6%
[30] (SVM)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	100.0% 100.0%	100.0% 100.0%	93.5% 94.4%
[30] (MLP)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	100.0% 100.0%	100.0% 100.0%	93.5% 94.4%
SAD (GIN)	**All**	**100.0%** **100.0%**	**98.3%** **99.0%**	**99.5%** **99.6%**

GNN4IFA: UAD vs SOTA

UAD vs non ML-based Baselines

Baseline	Features	Topologies		
		Small	DFN	Large
[7]	$[\frac{f_1^l}{f_4^l}, \frac{f_{12}^l}{f_1^l}]$	98.9% 0.0%	75.6% 0.0%	99.9% 15.5%
[26]	$[\frac{f_{12}^l}{1200}, \frac{f_7^l}{f_7^l+f_5^l}]$	71.0% 0.0%	52.3% 0.0%	94.8% 6.2%
[24]	$[\frac{f_{12}^l}{1200}, \frac{f_7^l}{f_7^l+f_5^l}]$	59.7% 0.0%	77.0% 0.0%	95.7% 14.2%
[27]	$[\frac{f_3^l}{f_1^l}, f_1^l, f_7^l, f_9^l]$	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
[6]	$[\frac{f_1^l}{f_4^l}, \frac{f_{12}^l}{f_1^l}]$	86.0% 0.0%	31.1% 0.0%	82.0% 0.0%
GNN4IFA	**All**	**100.0%** **2.1%**	**100.0%** **1.8%**	**100.0%** **0.75%**

UAD outperforms the baselines in the three topologies in terms of TPR. Instead, regarding the FPR, UAD outperforms all the baselines for the large topology, confirming the benefits of the global knowledge in such scenarios.

GNN4IFA: UAD vs SOTA

UAD vs ML-based Baselines

Baseline	Features	Topologies		
	Small	DFN	Large	
[29] (MLP)	$[F_1{:}F_6,\ F_{12}]$	100.0% 0.0%	100.0% 0.0%	89.4% 0.0%
[29] (SVM)	$[F_1{:}F_6,\ F_{12}]$	100.0% 0.0%	100.0% 0.0%	89.3% 0.0%
[28] (SVM)	$[F_{13}=\frac{F_3}{F_2},$ $F_{14}=\frac{F_{12}}{1200}]$	100.0% 0.0%	96.9% 12.4%	89.4% 0.0%
[31] (RF)	$[F_2,\ F_3,$ $F_8,\ F_{12}]$	100.0% 0.0%	100.0% 0.0%	89.4% 0.0%
[30] (DT)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	100.0% 0.0%	99.9% 0.0%	64.7% 0.0%
[30] (NB)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	99.9% 100.0%	100.0% 100.0%	100.0% 100.0%
[30] (SVM)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	100.0% 0.0%	100.0% 0.0%	89.3% 0.0%
[30] (MLP)	$[F_1{:}F_8,$ $F_{11},\ F_{12}]$	100.0% 0.0%	100.0% 0.0%	89.4% 0.0%
UAD (GIN)	**All**	**100.0%** **2.1%**	**100.0%** **1.8%**	**100.0%** **0.75%**

UAD obtains a TPR identical to the baselines for the small and DFN topology. Meanwhile, for the large topology, it outperforms the baselines achieving at least a 10% increase in TPR.

GNN4IFA: Generalisability study

Accuracy and F1-score of SAD over SPOTIFAI topologies, when trained on a different topology.

Topology transfer	Accuracy	F1-score
Small → Small	100.0%	100.0%
Small → DFN	72.8%	68.0%
Small → Large	72.8%	67.3%
DFN → Small	93.2%	96.1%
DFN → DFN	98.3%	99.0%
DFN → Large	54.9%	32.4%
Large → Small	100.0%	100.0%
Large → DFN	94.0%	94.2%
Large → Large	99.5%	99.6%

SAD generalises well from larger to smaller topologies.

TPR and FPR of UAD over SPOTIFAI topologies, when trained on a different topology.

Topology transfer	TPR	FPR
Small → Small	100.0%	2.1%
Small → DFN	98.3%	0.7%
Small → Large	91.7%*	0.0%*
DFN → Small	98.8%	2.2%
DFN → DFN	100.0%	1.8%
DFN → Large	100.0%†	2.9%†
Large → Small	100%	35.4%
Large → DFN	100%	26.9%
Large → Large	100.0%	0.75%

UAD generalises well from smaller to larger topologies.

GNN4IFA: Data requirements study

Accuracy (top) and F1-score (bottom) of SAD over SPOTIFAI topologies, when trained on a different percentage of samples.

Topology	60%	40%	20%	10%	5%
Small	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%	100.0% 100.0%
DFN	98.5% 99.1%	98.6% 99.2%	98.5% 99.1%	98.5% 99.2%	98.4% 99.0%
Large	99.5% 99.6%	99.4% 99.5%	98.3% 98.8%	98.0% 98.5%	94.8% 96.3%

TPR (top) and FPR (bottom) of UAD over SPOTIFAI topologies, when trained on a different percentage of samples.

Topology	90%	70%	50%	25%	10%
Small	100.0% 0.63%	100.0% 1.52%	98.75% 2.97%	98.75% 3.21%	97.5% 1.45%
DFN	100.0% 1.90%	100.0% 1.4%	100.0% 1.97%	100.0% 1.70%	100.0% 1.47%
Large	100.0% 0.73%	100.0% 0.68%	100.0% 0.66%	100.0% 0.51%	100.0% 1.16%

SAD and UAD perform well even when trained on small set of samples.

Conclusions and Future Works

In summary:

- SOTA for IFA detection lacks network-wide mechanisms and significant datasets
- We designed GNN4IFA, a global and novel GNN-based IFA detection mechanism, in two configurations: SAD and UAD
- We collected and released SPOTIFAI, the first IFA dataset
- We evaluated GNN4IFA performance and tested its generalizability over different topologies

In the future:

- Extend GNN4IFA with a proactive IFA mitigation scheme relying on xAI
- Model and implement GNN4IFA in a distributed fashion, with an ad-hoc communication protocol
- Extend SPOTIFAI by including more setups heterogeneity and other IFA types.

Thank You!
Questions?

Artifact







@enkeleda_bardhi
@and_agio

bardhi@diag.uniroma1.it
andrea.agiollo@unibo.it

SPOTIFAI



Acknowledgements:

- project “Secure ANd PrivatE Information sharing (SANPEI)”, Sapienza University of Rome
- the CHIST-ERA IV project “EXPECTATION” (CHIST-ERA-19-XAI-005), co-funded by EU and the Italian MUR
- project “SERICS” (PE00000014) under the NRRP MUR program funded by the EU - NGEU;
- the European Commission under the Horizon Europe Programme, as part of the project “LAZARUS”

References

[1] D. R. Cheriton and M. Gritter, “Triad: A New Next-Generation Internet Architecture,” 2000.

[2] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos et al., “Named Data Networking (NDN) Project,” Relatorio Tecnico NDN-0001, vol. 157, p. 158, 2010

[6] A. Benarfa, M. Hassan, A. Compagno, E. Losiouk, M. B. Yagoubi, and M. Conti, “Chokifa: A New Detection and Mitigation Approach Against Interest Flooding Attacks in NDN,” in *International Conference on Wired/Wireless Internet Communication*, 2019, pp. 53–65.

[7] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, “Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking,” in *IEEE Conference on Local Computer Networks*, 2013, pp. 630–638.

[24] H. Salah, J. Wulfheide, and T. Strufe, “Coordination supports security: A new defence mechanism against interest flooding in NDN,” in *40th IEEE Conference on Local Computer Networks, LCN 2015, Clearwater Beach, FL, USA, October 26-29, 2015*. IEEE Computer Society, 2015, pp. 73–81.

[26] K. Wang, H. Zhou, Y. Qin, and H. Zhang, “Cooperative-filter: countering interest flooding attacks in named data networking,” *Soft Computing*, vol. 18, no. 9, pp. 1803–1813, 2014.

[27] A. Benmoussa, A. E. K. Tahari, N. Lagraa, A. Lakas, F. Ahmad, R. Hussain, C. A. Kerrache, and F. Kurugollu, “A novel congestion- aware interest flooding attacks detection mechanism in named data networking,” in *28th International Conference on Computer Communication and Networks, ICCCN 2019, Valencia, Spain, July 29 - August 1, 2019*. IEEE, 2019, pp. 1–6.

[28] T. Zhi, Y. Liu, and Z. Yan, “An Entropy-SVM Based Interest Flooding Attack Detection Method in ICN,” in *IEEE Vehicular Technology Conference*, 2018, pp. 1–5.

[29] N. Kumar, A. K. Singh, and S. Srivastava, “Evaluating Machine Learning Algorithms for Detection of Interest Flooding Attack in Named Data Networking,” in *ACM International Conference Proceeding Series*, 2017, pp. 299–302.

[30] N. Kumar, A. K. Singh, and S. Srivastava, “Feature Selection for Interest Flooding Attack in Named Data Networking,” *International Journal of Computers and Applications*, vol. 43, no. 6, pp. 537–546, 2021.

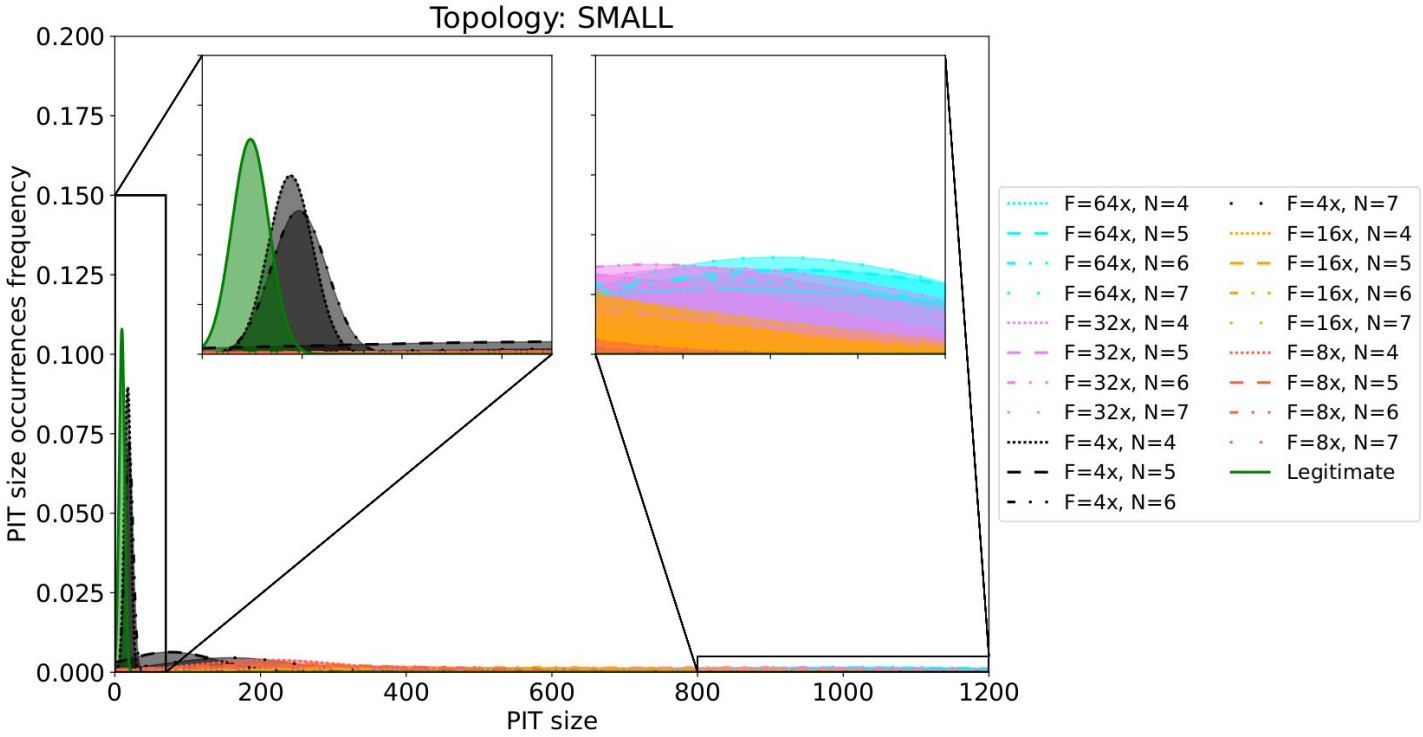
[31] J. Chen, G. Xing, M. Cui, H. Huo, and R. Hou, “Isolation forest based interest flooding attack detection mechanism in ndn,” in *2019 2nd International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 2019, pp. 58–62.

Backup Slides

What brings our paper?

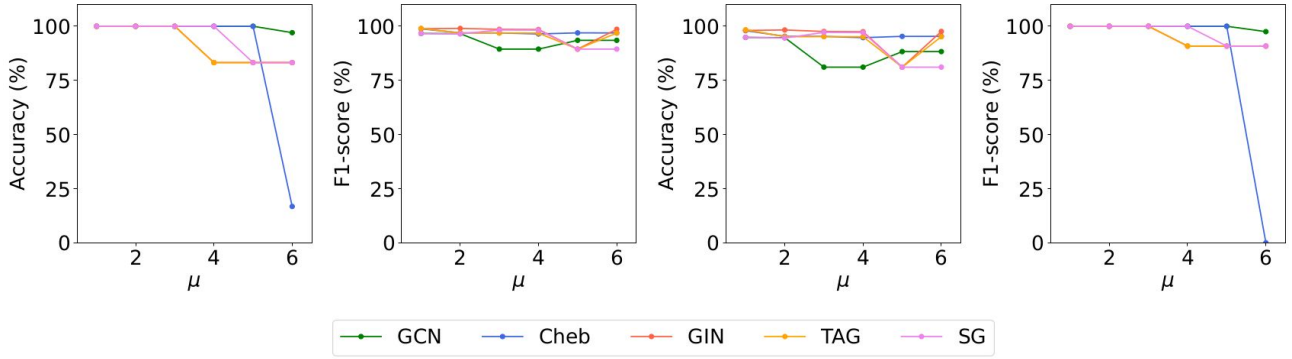
- Collection and release of SPOTIFAI: SPOTting IFA Intruders, the first IFA dataset
  - 40 IFA scenarios constructed over three network topologies, corresponding to 21 hours of traffic
- Design of GNN4IFA, a Graph Neural Network (GNN)-based IFA detection mechanism
  - Configurations: Supervised Attack Detection (SAD) and Unsupervised Attack Detection (UAD)
- Evaluation and comparison of GNN4IFA with SOTA
  - 300 SAD and UAD models trained
- Analysis of GNN4IFA generalizability
  - Train in one topology and test in the others

SPOTIFAI: SPOTting IFA Intruders



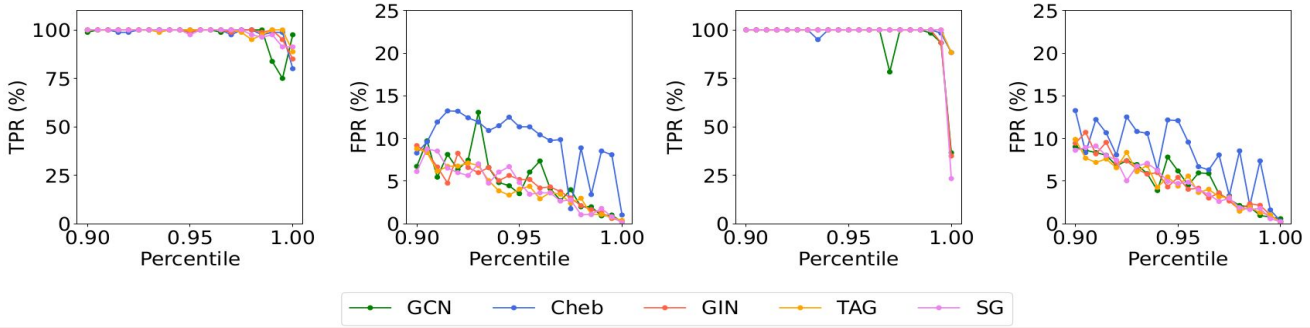
PIT size distribution for small-scale topology

GNN4IFA: SAD and UAD Ablation Study



Best setup:
τ = GIN
μ = 2

SAD ablation study. Accuracy and F1-score are shown concerning the μ and τ. Left side plots refer to the small topology, while the right side refers to DFN.



Best setup:
τ = GIN
p = 0.985

UAD ablation study. TPR and FPR are shown w.r.t the p-th percentile used to identify threshold τ. Left side small topology, while the right side to DFN.