Multi-domain Anomaly Detection in 5G Networks through Continuous Dynamic Graphs

HOGER Thomas
PhD Student, EDMITT, LAAS-CNRS
thomas.hoger@laas.fr

OWEZARSKI Philippe
Thesis Advisor, LAAS-CNRS
owe@laas.fr

AMDOUNI Mariam
Intern, LAAS-CNRS
mariamamdouni2001@gmail.com

LAAS-CNRS
/ Laboratoire d'analyse et d'architecture des systèmes du CNRS

PEPR HISEC : ANR-22-PEFT-0009

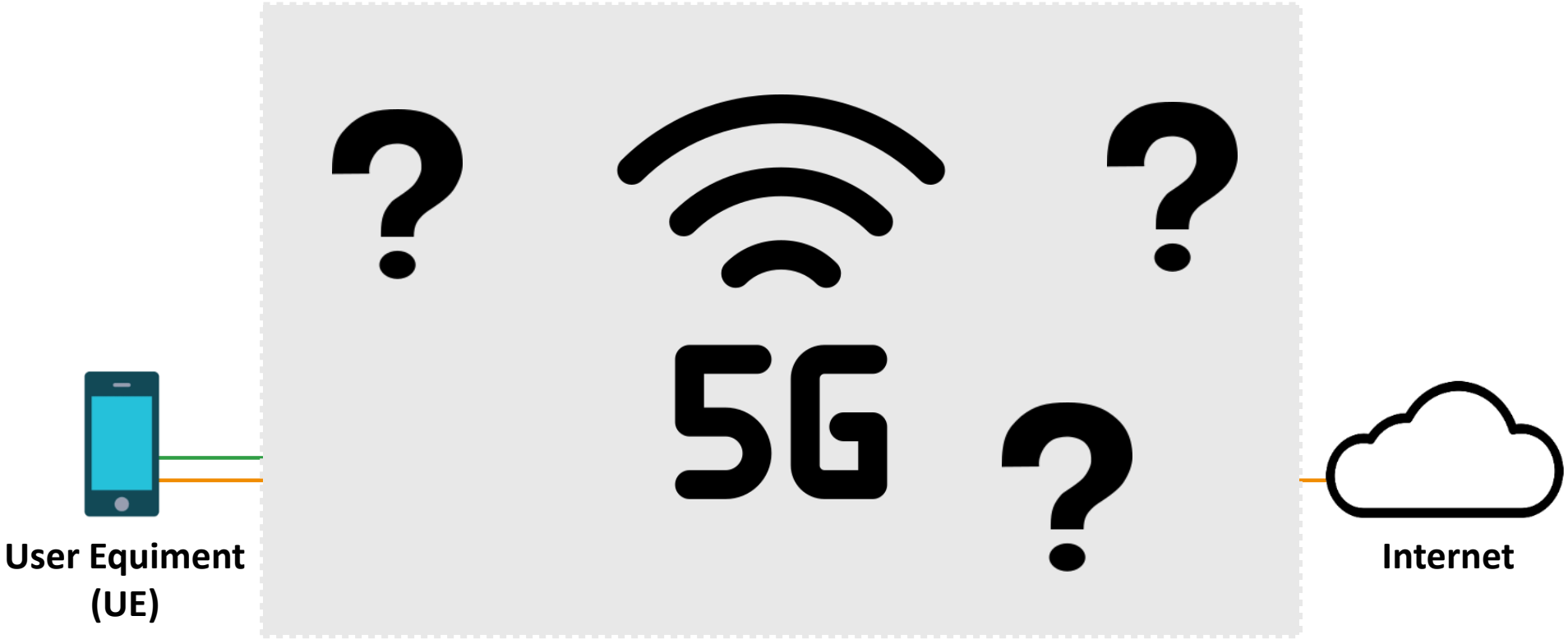
Laboratoire conventionné avec Université de Toulouse

Table of content

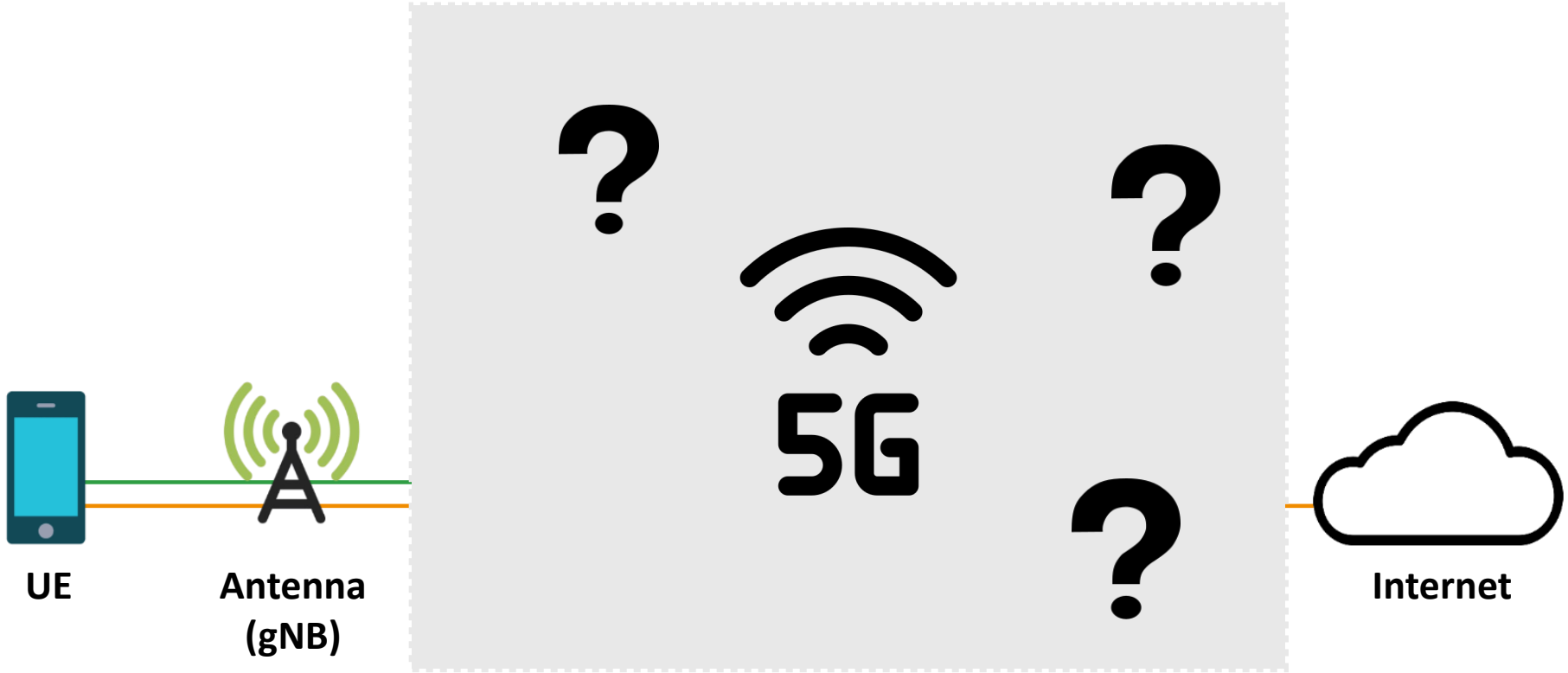
What is 5G?

A brief introduction

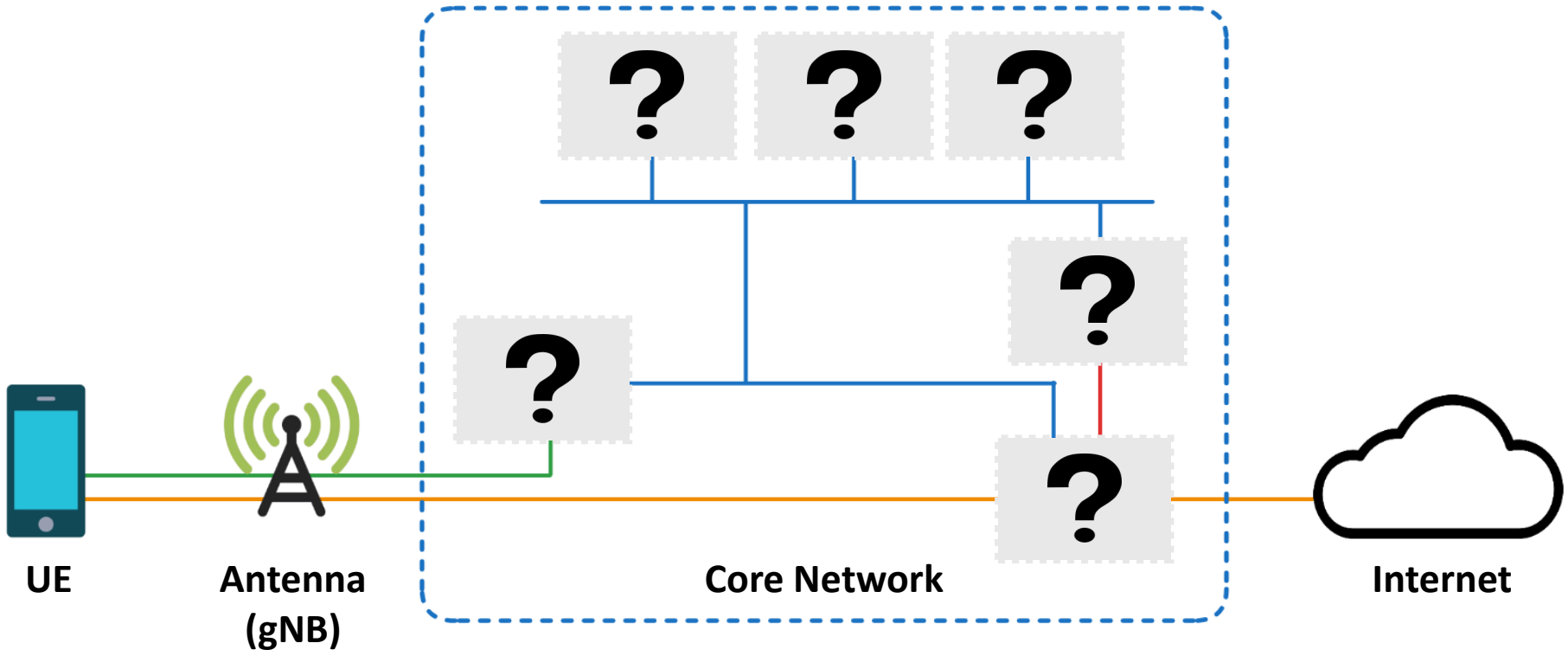
What is 5G ?



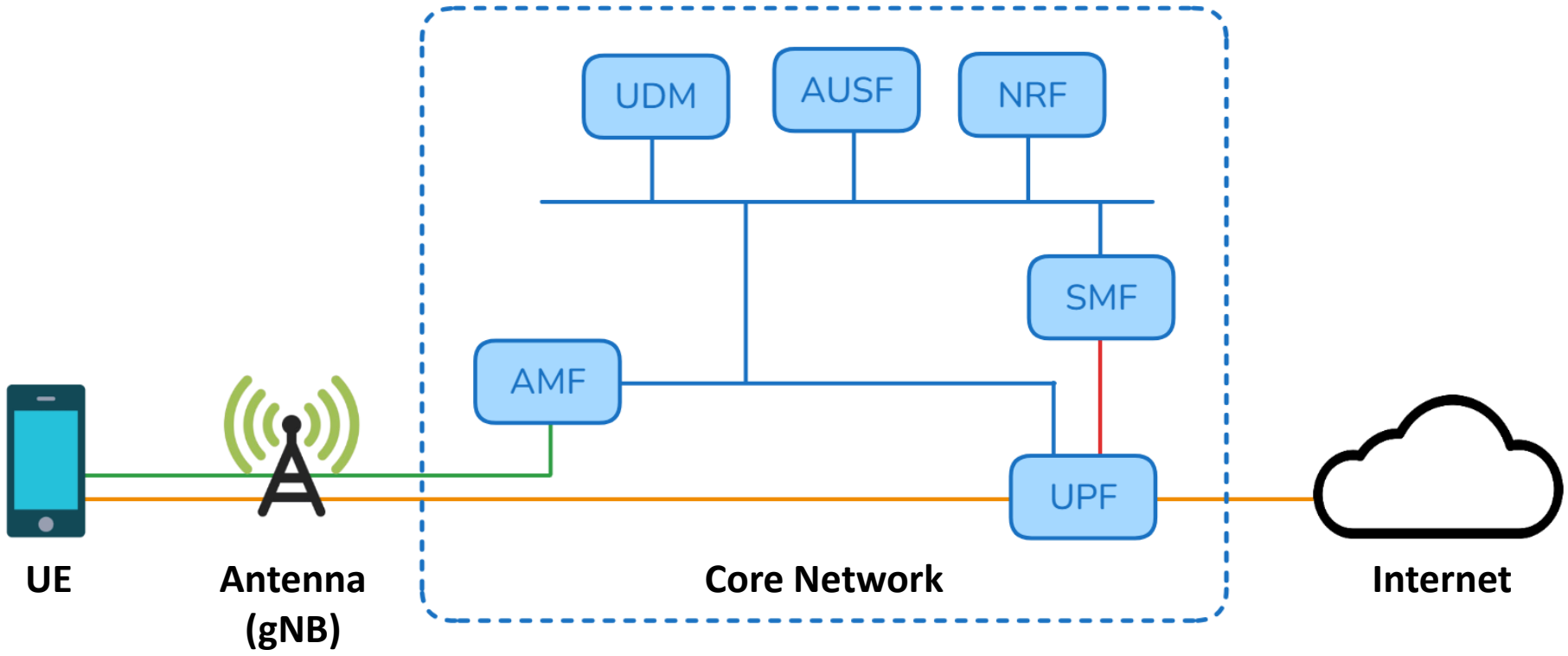
What is 5G ?



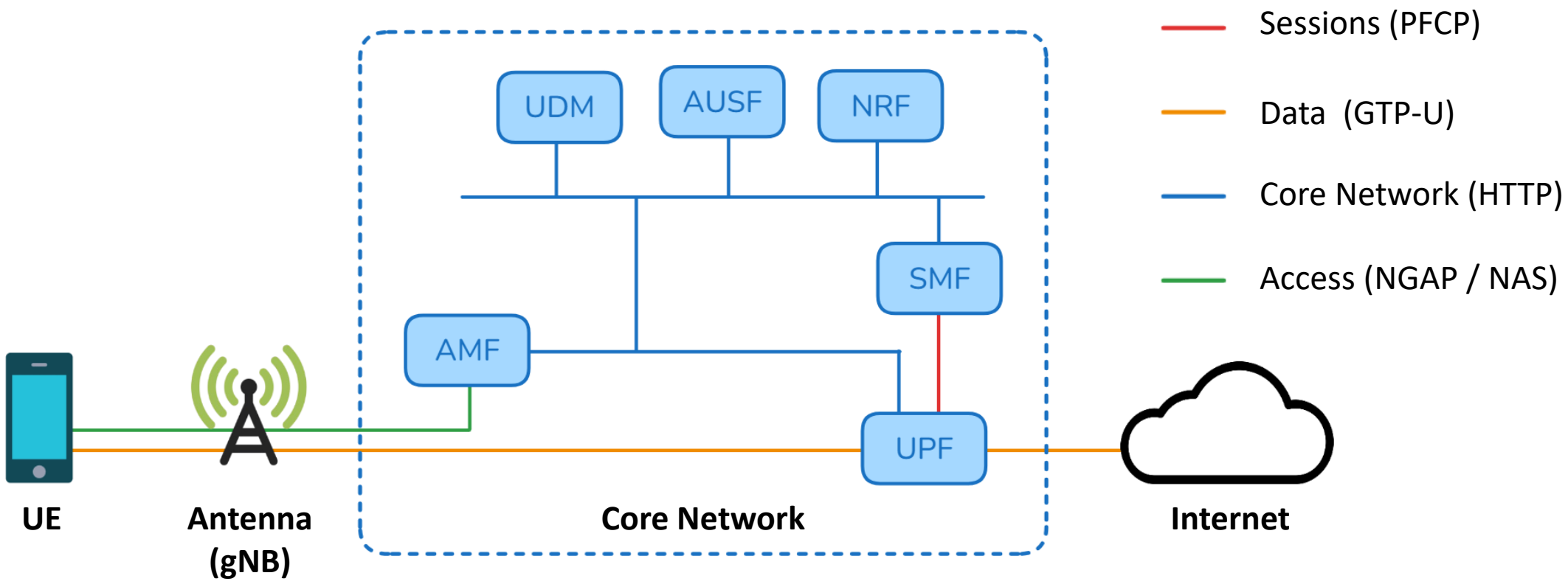
What is 5G ?



What is 5G ?


UDM
AUSF
NRF
SMF
AMF
UPF
UE
Antenna
(gNB)
Core Network
Internet

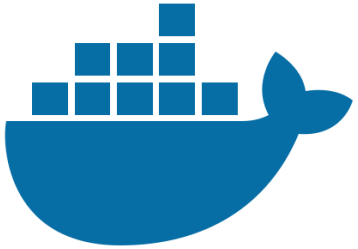
What is 5G ?



Channels with their own role and protocol stacks

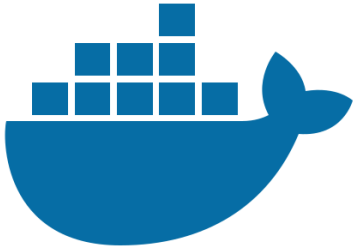
Major changes from 4G

Network Function Virtualization (NFV)



Major changes from 4G

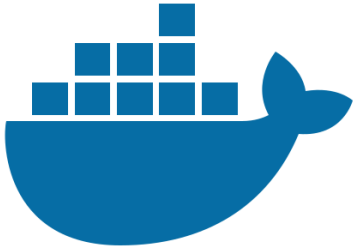
Network Function Virtualization (NFV)



Software Defined Network (SDN)

Major changes from 4G

Network Function Virtualization (NFV)

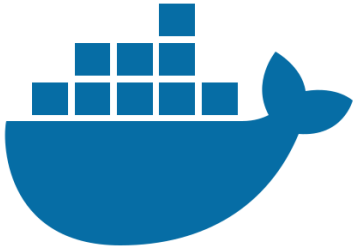


Software Defined Network (SDN)

Service-Based Interfaces (SBI)

Major changes from 4G

Network Function Virtualization (NFV)



Software Defined Network (SDN)

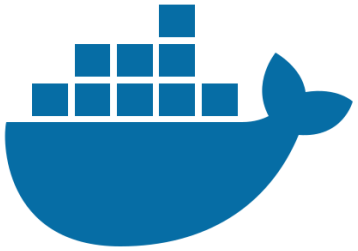
Service-Based Interfaces (SBI)

5G networks increasingly resemble distributed systems in their design

What about the attacks ?

Few examples of attacks now possible in 5G

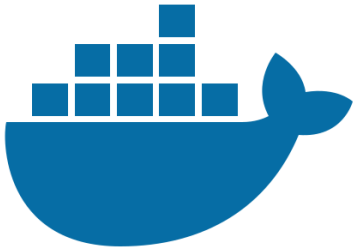
Broader attacking surface



VM/Docker escape [1]

[1] A. Tomar, D. Jeena, P. Mishra, et R. Bisht, « Docker Security: A Threat Model, Attack Taxonomy and Real-Time Attack Scenario of DoS », in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, janv. 2020, p. 150-155. doi: 10.1109/Confluence47617.2020.9058115.

Broader attacking surface

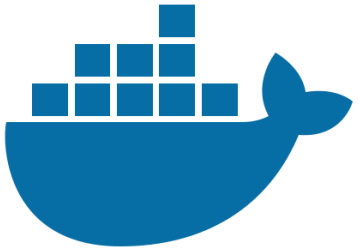


VM/Docker escape [1]

Man in the Middle [2]

[2] T. Hoger, P. Owezarski, et G. Durand-Nauze, « Control Traffic Dataset and Generation Framework for 5G Networks ». 27 février 2026. doi: 10.5281/zenodo.15853959.

Broader attacking surface



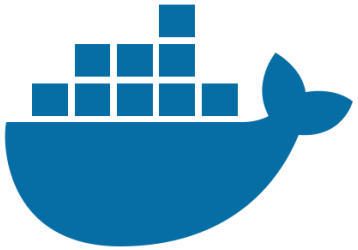
VM/Docker escape [1]

Man in the Middle [2]

Fuzzing [2]

[2] T. Hoger, P. Owezarski, et G. Durand-Nauze, « Control Traffic Dataset and Generation Framework for 5G Networks ». 27 février 2026. doi: 10.5281/zenodo.15853959.

Broader attacking surface



VM/Docker escape [1]

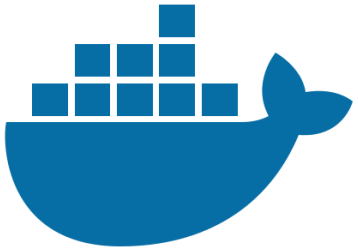
Man in the Middle [2]

Fuzzing [2]

Slice pivoting [3]

[3] A. Kumar et V. L. L. Thing, « Malicious Lateral Movement in 5G Core With Network Slicing And Its Detection », in *2023 33rd International Telecommunication Networks and Applications Conference*, nov. 2023, p. 110-117. doi: 10.1109/ITNAC59571.2023.10368559.

Broader attacking surface



VM/Docker escape [1]

Man in the Middle [2]

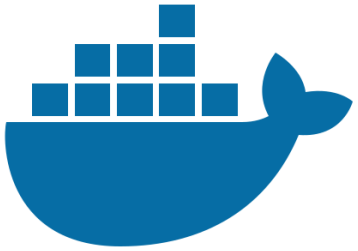
Fuzzing [2]

Slice pivoting [3]

Supply Chain Backdoor [4]

[4] R. G. Kula, D. M. German, A. Ouni, T. Ishio, et K. Inoue, « Do Developers Update Their Library Dependencies? An Empirical Study on the Impact of Security Advisories on Library Migration », *Empir Software Eng*, vol. 23, nº 1, p. 384-417, févr. 2018, doi: 10.1007/s10664-017-9521-5.

Broader attacking surface



VM/Docker escape [1]

Man in the Middle [2]

Fuzzing [2]

Slice pivoting [3]

Supply Chain Backdoor [4]

Features and flexibility at the cost of an increased attacking surface

Broader attacking surface

Control Plane Network Messages

VM/Docker escape [1]

Man in the Middle [2]

Fuzzing [2]

Slice pivoting [3]

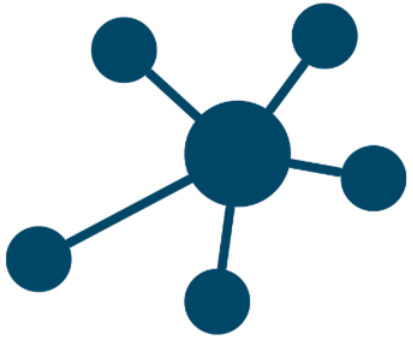
Supply Chain Backdoor [4]

Features and flexibility at the cost of an increased attacking surface

Anomaly Dimensions

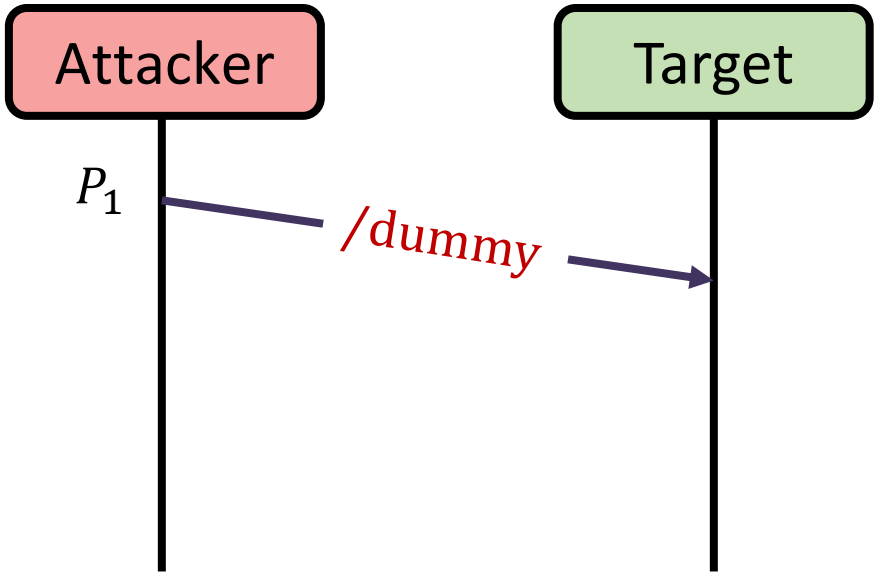
Semantic

Sequence



Topology

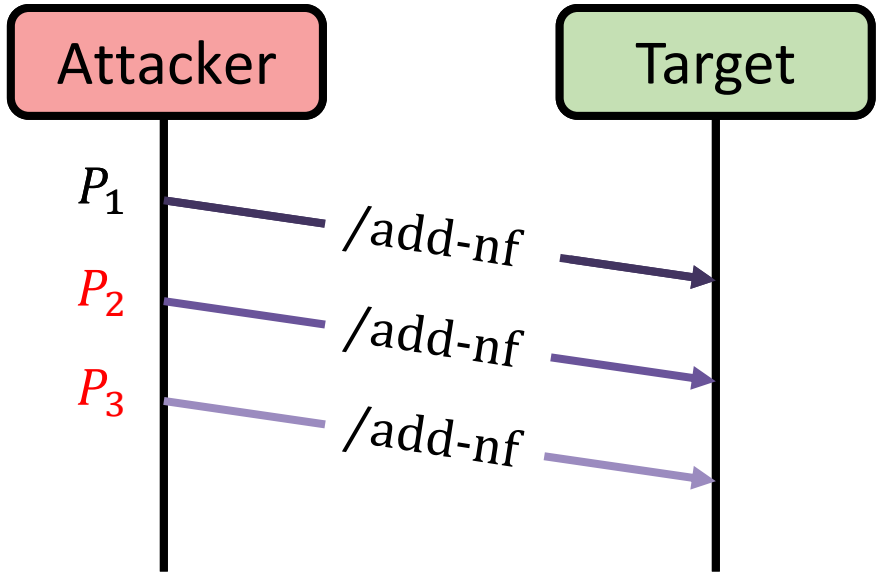
Anomaly 1 : Semantic



Example : API Fuzzing [2]

[2] T. Hoger, P. Owezarski, et G. Durand-Nauze, « Control Traffic Dataset and Generation Framework for 5G Networks ». 27 février 2026. doi: 10.5281/zenodo.15853959.

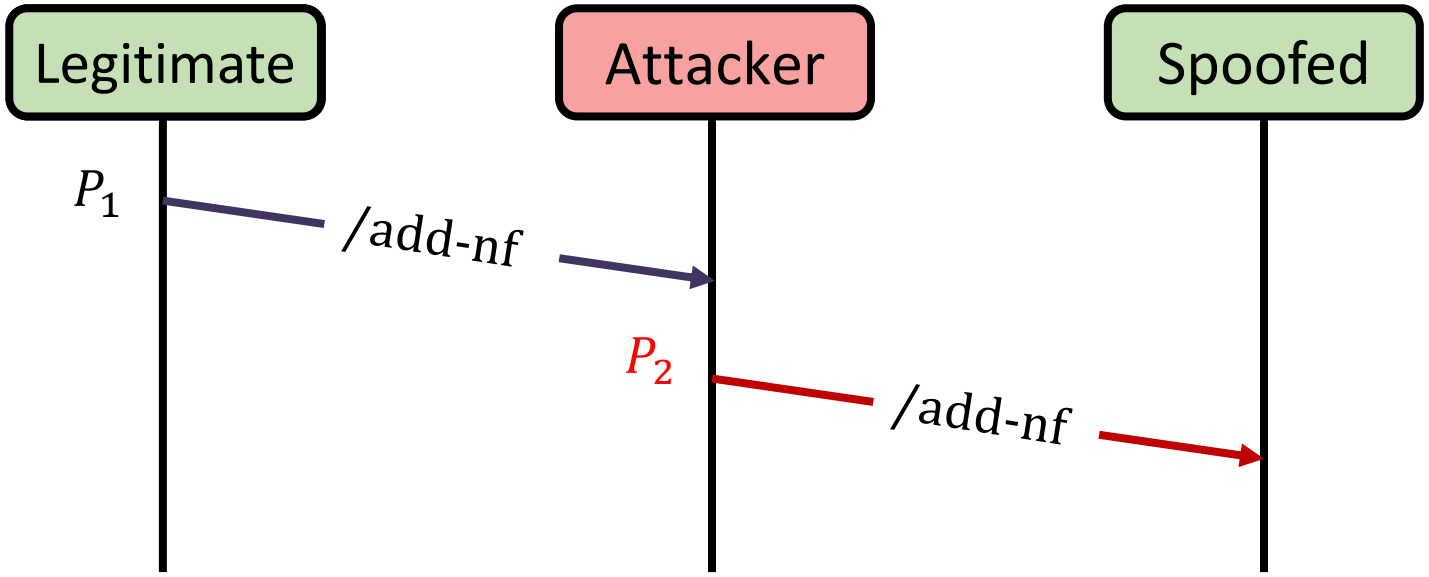
Anomaly 2 : Sequential



Example : Session Flooding [5]

[5] G. Amponis *et al.*, « Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications », *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, nº 1, p. 124, déc. 2022, doi: 10.1186/s13638-022-02204-5.

Anomaly 3 : Topologic



Example : Man in the Middle [2]

[2] T. Hoger, P. Owezarski, et G. Durand-Nauze, « Control Traffic Dataset and Generation Framework for 5G Networks ». 27 février 2026. doi: 10.5281/zenodo.15853959.

5G Anomaly Detection SoTA

What are they missing ?

State of the art for 5G anomaly detection

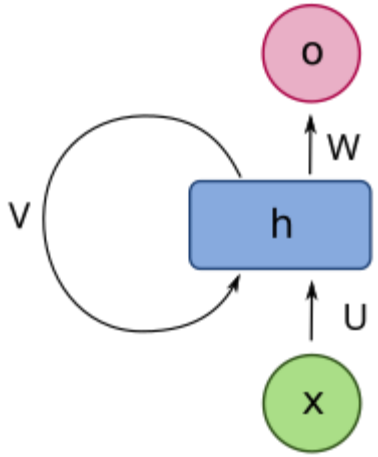
Sequences of Interactions

$F_{expected}$ = {gNB->AMF, AMF->AUSF, AUSF->AMF, AMF->AUSF, AUSF->AMF, AUSF->UDM, UDM->AUSF, UDM->UDR, UDR->UDM, ...}

F_{actual} = {gNB->AMF, AMF->AUSF, AUSF->AMF, AMF->AUSF, AUSF->AMF, SMF->AMF, SMF->AMF, SMF->AMF, AUSF->UDM,.....}

- S_1= [gNB->AMF, AMF->AUSF, AUSF->AMF, AMF->AUSF, AUSF->AMF] ➔ $E_{next-predict}$ match $E_{next-expected}$=[AUSF->UDM]
- S_2= [AMF->AUSF, AUSF->AMF, AMF->AUSF, AUSF->AMF, SMF->AMF] ➔ $E_{next-predict}$ mismatch $E_{next-expected}$=[UDM->AUSF]
- S_3= [AUSF->AMF, AMF->AUSF, AUSF->AMF, SMF->AMF, SMF->AMF] ➔ $E_{next-predict}$ mismatch $E_{next-expected}$=[UDM->UDR]
- S_4= [AMF->AUSF, AUSF->AMF, SMF->AMF, SMF->AMF, SMF->AMF] ➔ $E_{next-predict}$ mismatch $E_{next-expected}$=[UDR->UDM]

Recurrent Neural Network



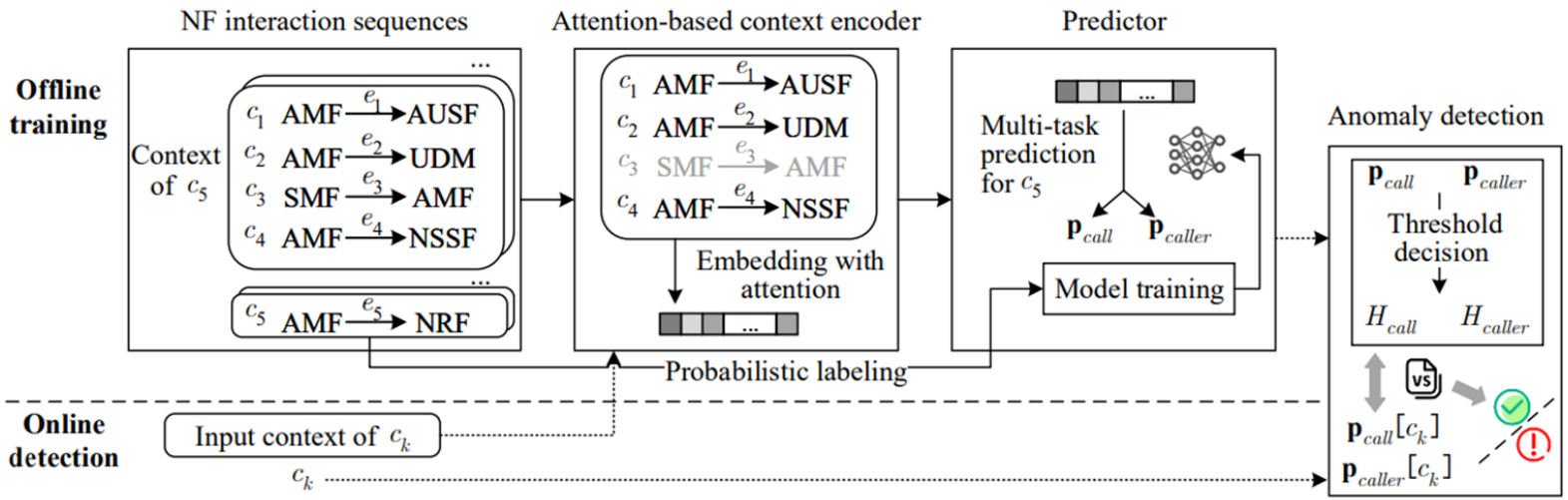
ADSeq-5GCN [6]

Semantic ✗ Sequential ☑ Topologic 😟

[6] Z. Tian, R. Patil, M. Gurusamy, et J. McCloud, « ADSeq-5GCN: Anomaly Detection from Network Traffic Sequences in 5G Core Network Control Plane », in *2023 IEEE 24th International Conference on High Performance Switching and Routing (HPSR)*, juin 2023, p. 75-82. doi: 10.1109/HPSR57248.2023.10147931.

State of the art for 5G anomaly detection

Sequences of Interactions (+ Endpoint)



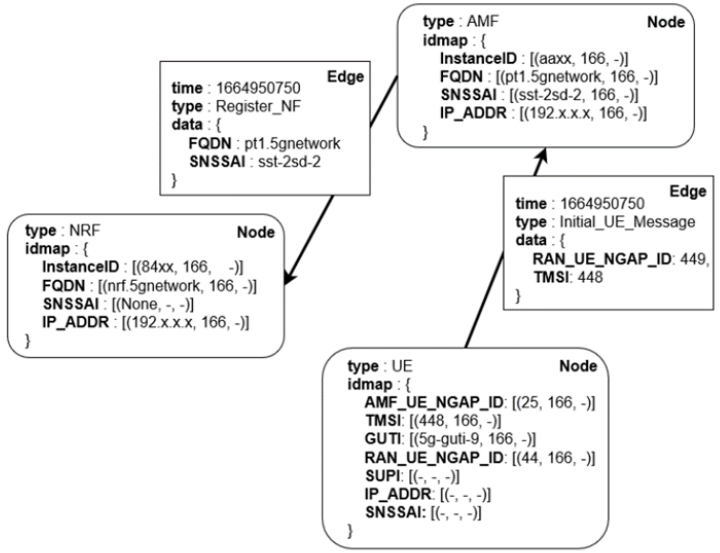
5GCGuard [7]

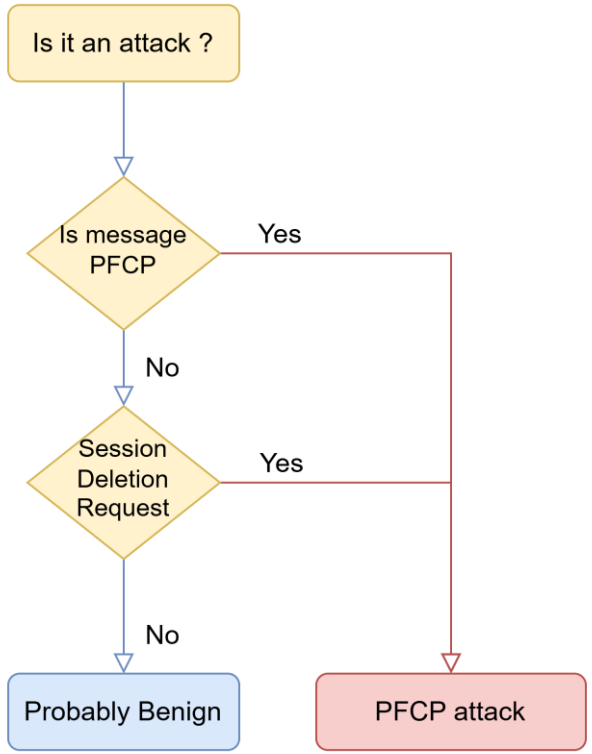
Semantic ✗ Sequential ☑ Topologic 😟

[7] Y. Tan, J. Liu, Y. Li, et J. Wang, « Deep Learning Based Proactive Anomaly Detection for 5G Core Control Plane Network Function Interactions », *IEEE Transactions on Cognitive Communications and Networking*, p. 1-1, 2025, doi: 10.1109/TCCN.2025.3539660.

State of the art for 5G anomaly detection

Provenance Graph



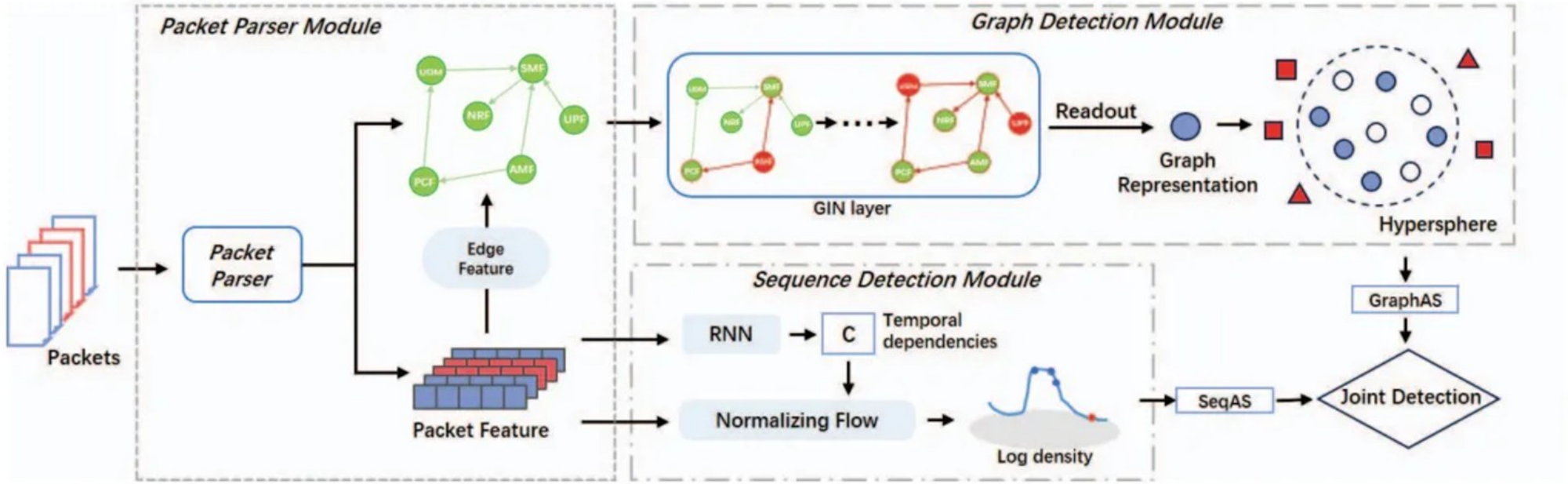


Prov5G [8]

Semantic 😟 Sequential ✗ Topologic ☑

[8] H. S. Pacherkar et G. Yan, « PROV5GC: Hardening 5G Core Network Security with Attack Detection and Attribution Based on Provenance Graphs », in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, in WiSec '24. New York, NY, USA: Association for Computing Machinery, mai 2024, p. 254-264. doi: 10.1145/3643833.3656129.

State of the art for 5G anomaly detection

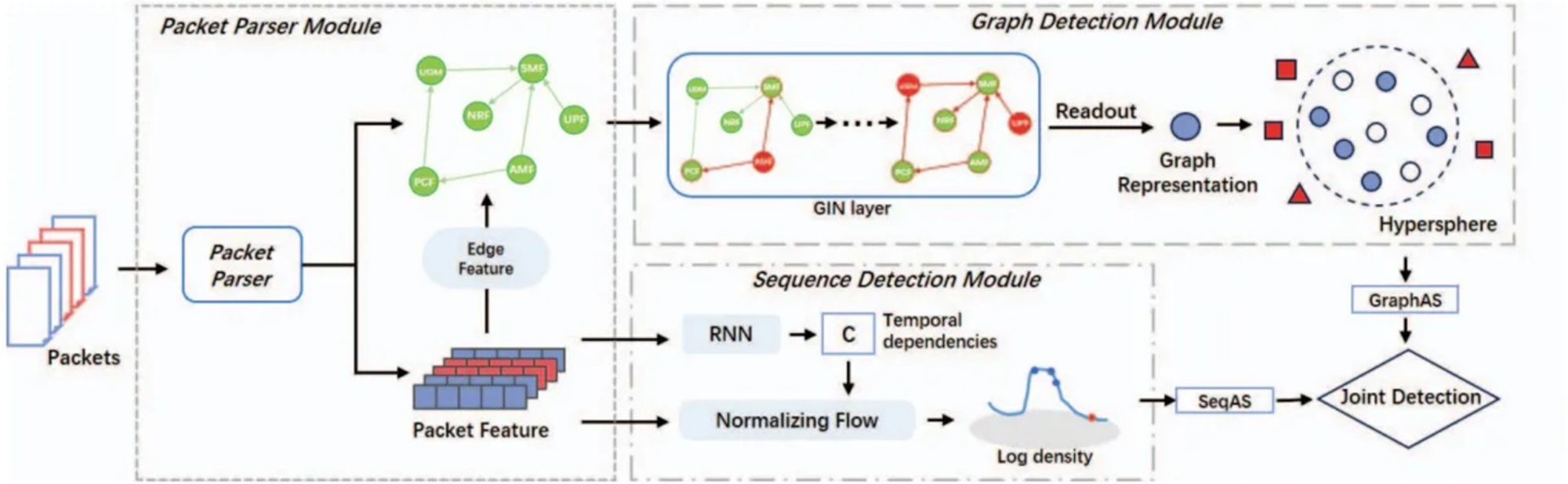


GSAD [9]

Semantic 😟 Sequential 😟 Topologic ☑

[9] M. Wang *et al.*, « Unsupervised Graph-Sequence Anomaly Detection for 5G Core Network Control Plane Traffic », in *2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS)*, déc. 2023, p. 1645-1652. doi: 10.1109/ICPADS60453.2023.00230.

State of the art for 5G anomaly detection



GSAD [9]

Semantic 😟 Sequential 😟 Topologic ☑

[9] M. Wang *et al.*, « Unsupervised Graph-Sequence Anomaly Detection for 5G Core Network Control Plane Traffic », in *2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS)*, déc. 2023, p. 1645-1652. doi: 10.1109/ICPADS60453.2023.00230.

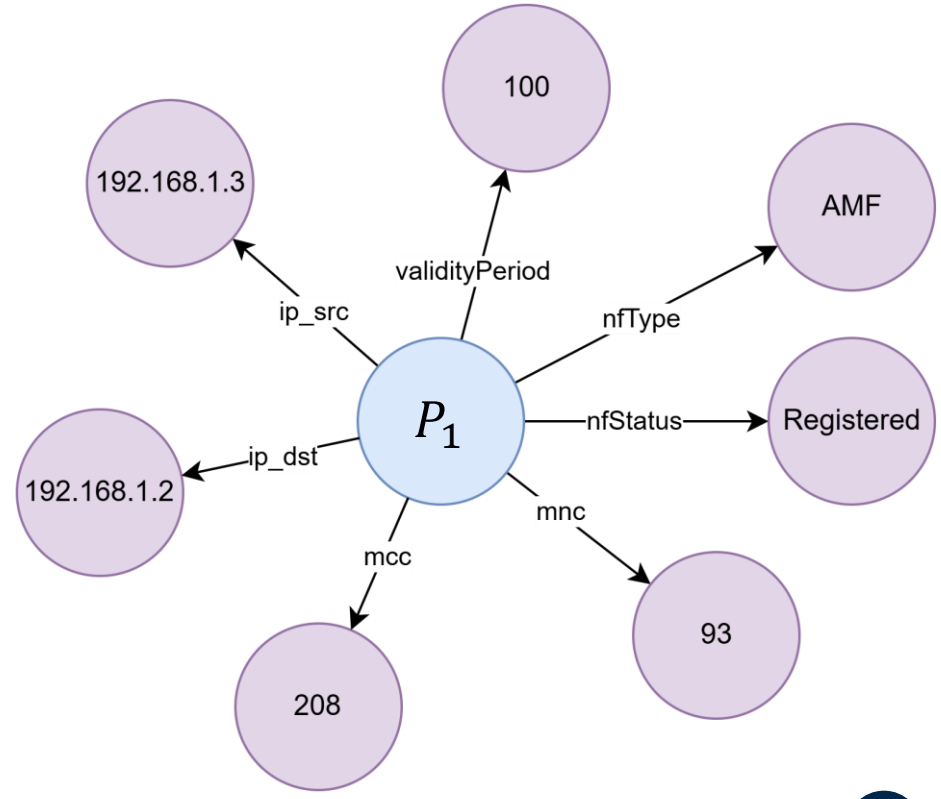
Graph Formalization

How do we represent the network messages

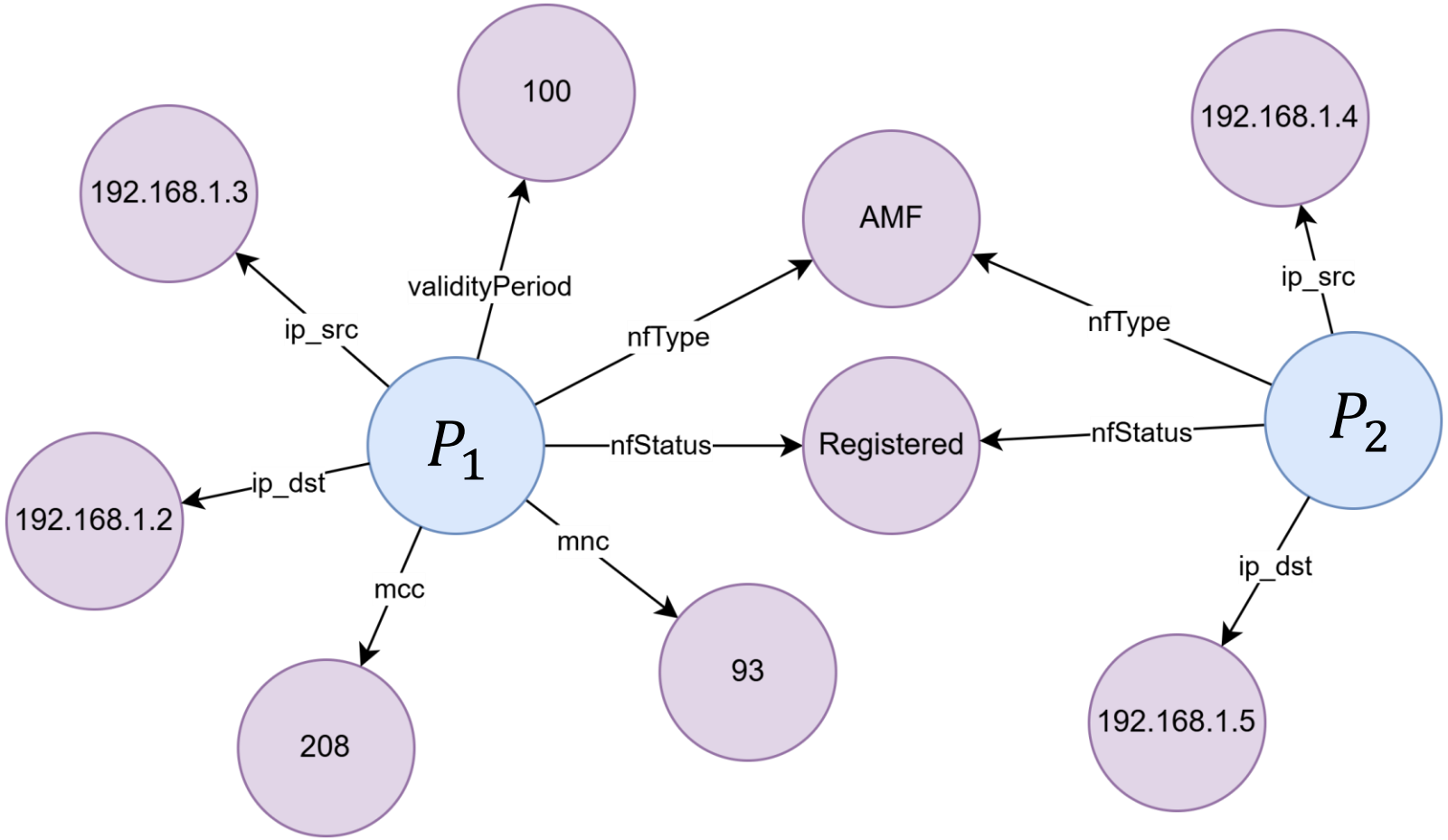
Graph formalization of network trafic

```
   4175 50.498176     localhost   NRF         HTTP2            639 HEADERS[5]: GET /nnrf-disc/v1/nf-instances?requester-nf-type=SMF&target-nf-instance-id=bb87e12b-e6fa-4
   4180 50.501378     NRF         localhost   HTTP2             89 HEADERS[5]: 200 OK
   4181 50.501455     NRF         localhost   HTTP2/JSON      2079 DATA[5], JSON (application/json)
```

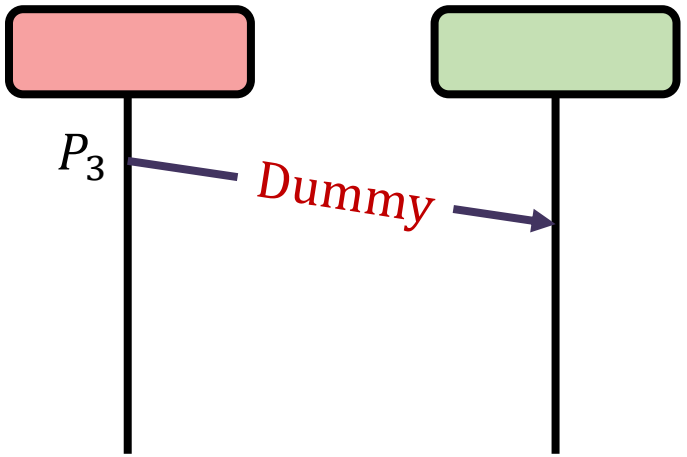
```
> Frame 4181: 2079 bytes on wire (16632 bits), 2079 bytes captured (16632 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: NRF (127.0.0.10), Dst: localhost (127.0.0.1)
> Transmission Control Protocol, Src Port: 80, Dst Port: 34738, Seq: 768, Ack: 875, Len: 200
v HyperText Transfer Protocol 2
  > Stream: DATA, Stream ID: 5, Length 1998
  v JavaScript Object Notation: application/json
    v Object
      > Member: validityPeriod
      v Member: nfInstances
        v Array
          v Object
            > Member: nfInstanceId
            > Member: nfType
            > Member: nfStatus
            > Member: plmnList
            > Member: sNssais
            > Member: ipv4Addresses
            > Member: amfInfo
            > Member: customInfo
            > Member: nfServices
            > Member: defaultNotificationSubscriptions
          Key: nfInstances
          [Path: /nfInstances]
```

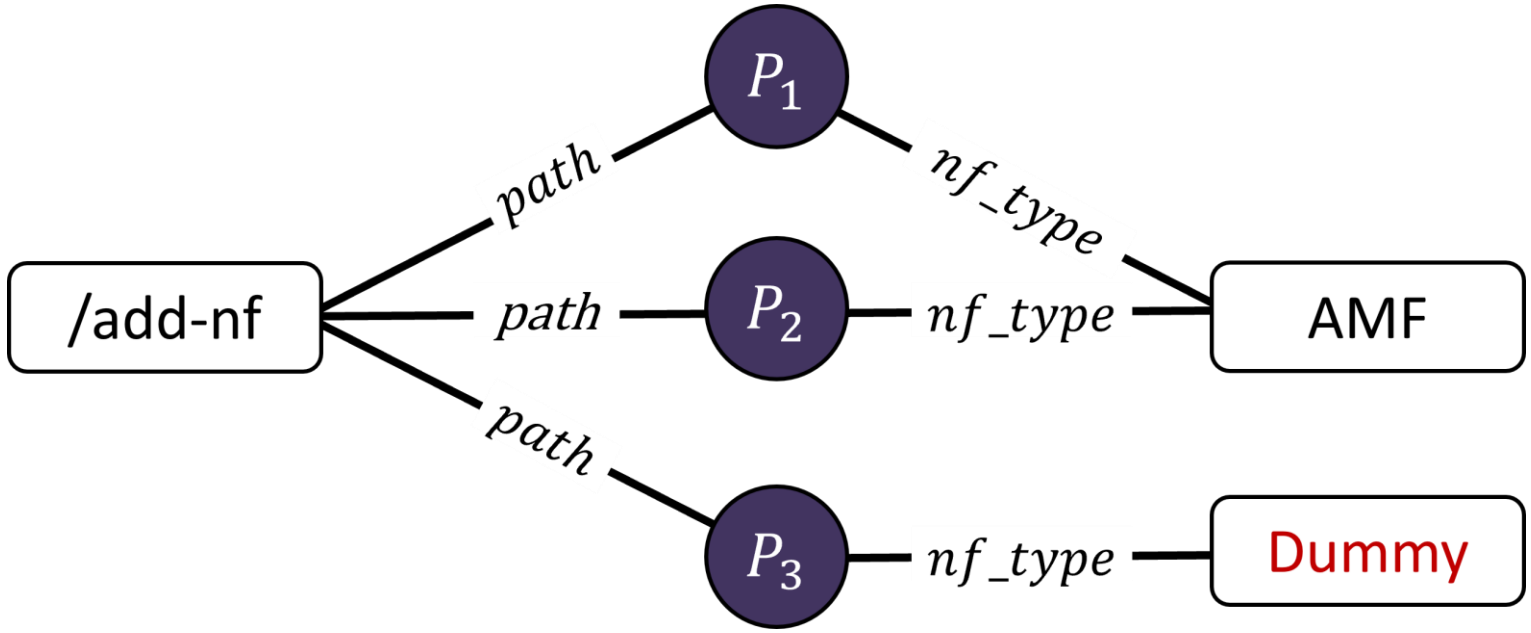


Graph formalization of network trafic

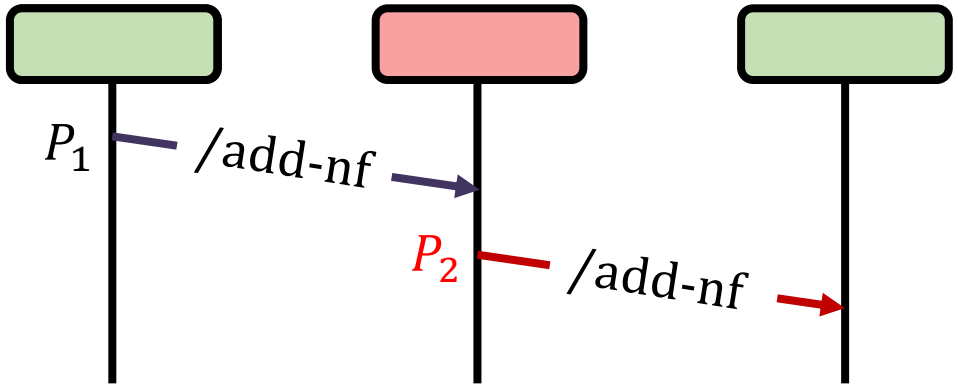


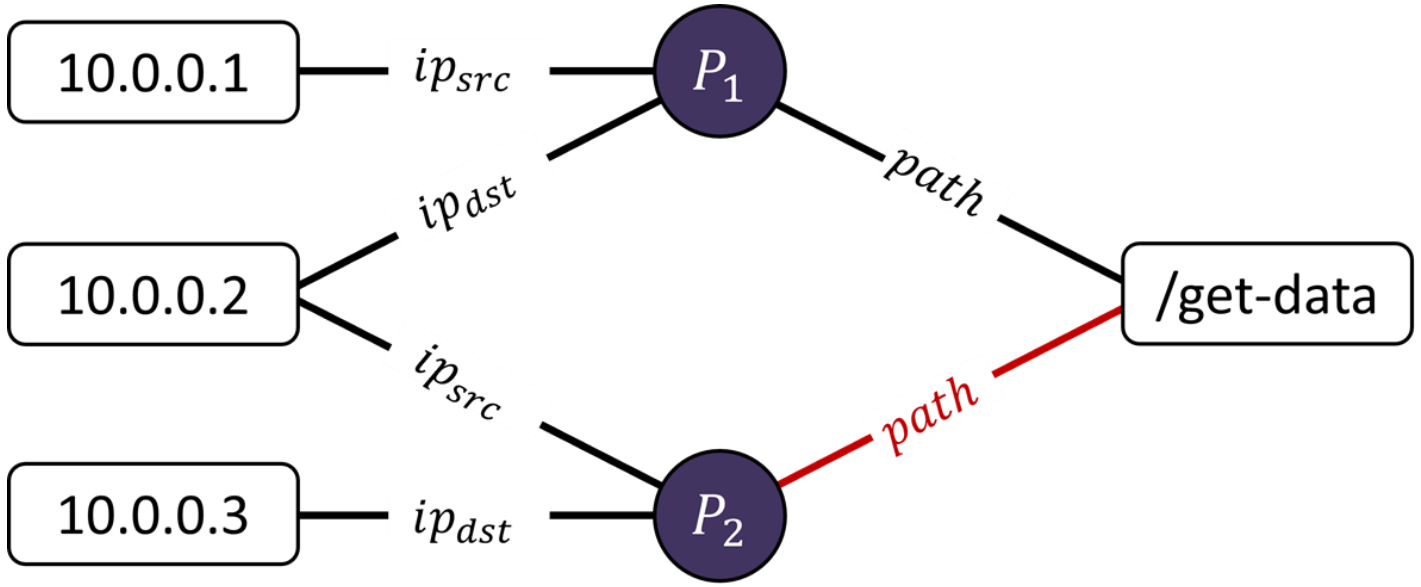
Anomaly 1 : Semantic



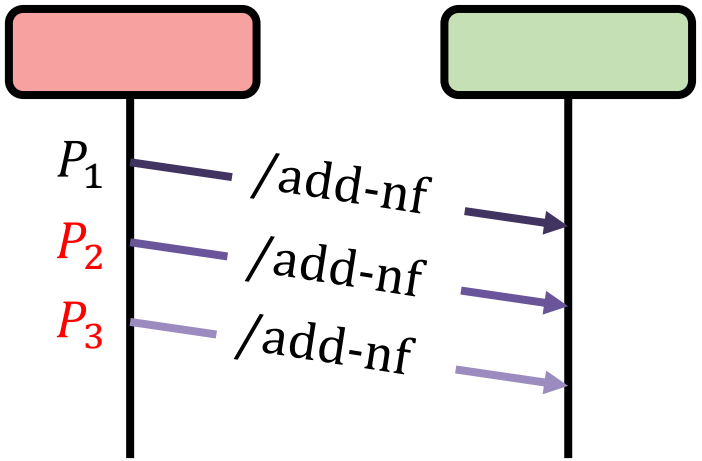


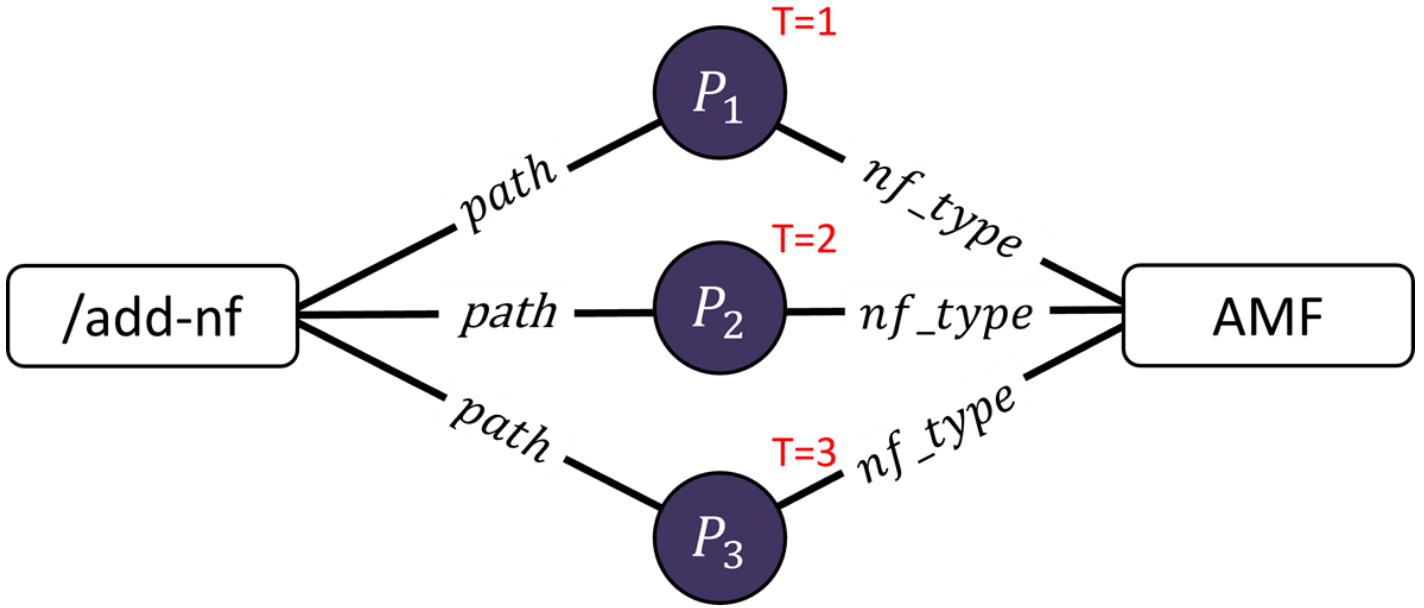
Anomaly 2 : Topologic





Anomaly 3 : Sequential

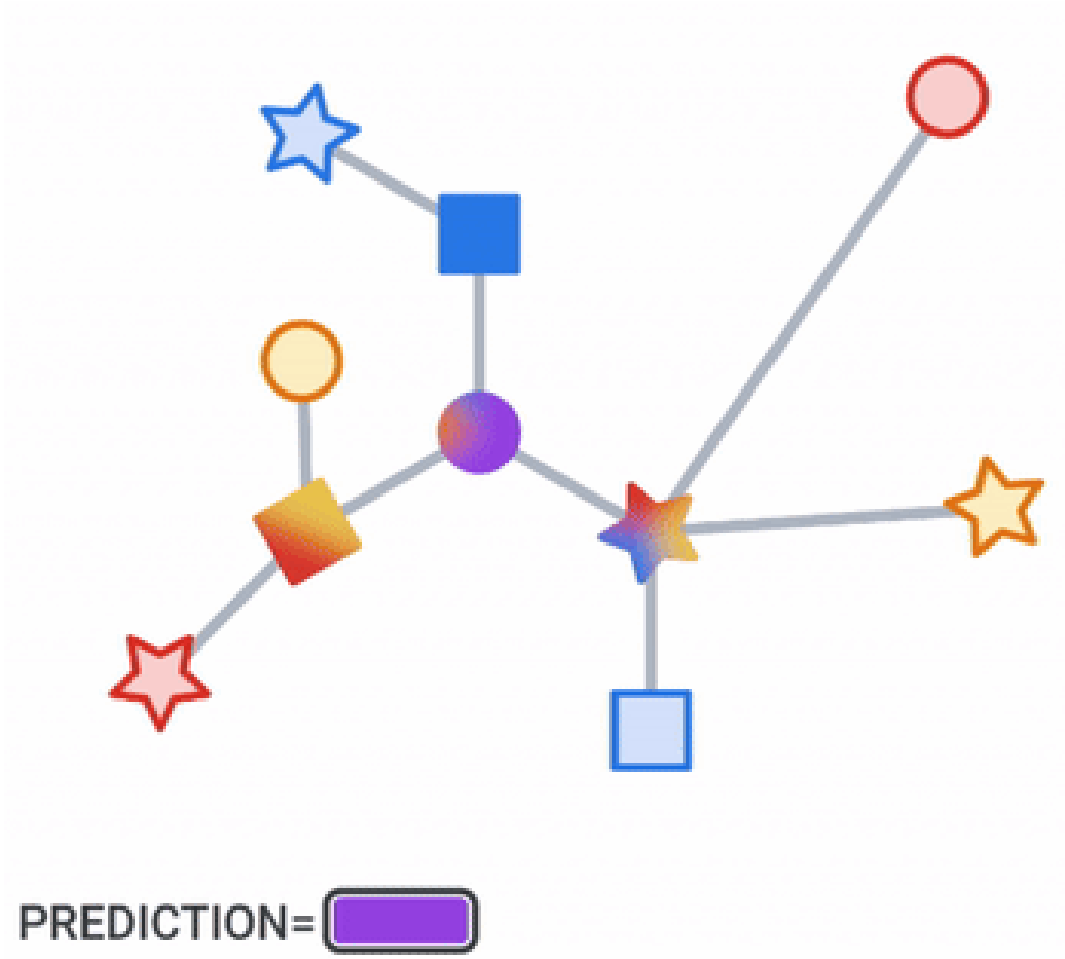




Graph Neural Network

How does it work and how to add the time aspect

Simple explanation of GNN operation



State of the art for GNN

Recent Domain

First paper [10] - 2008
Formalization [11] - 2017

[10] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, et G. Monfardini, « The Graph Neural Network Model », *IEEE Transactions on Neural Networks*, vol. 20, nº 1, p. 61-80, janv. 2009, doi: 10.1109/TNN.2008.2005605.

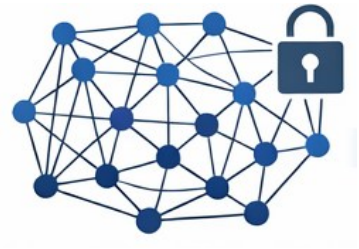
[11] J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals, et G. E. Dahl, « Neural Message Passing for Quantum Chemistry », 12 juin 2017, arXiv:1704.01212. doi: 10.48550/arXiv.1704.01212.

State of the art for GNN

Recent Domain

First paper [10] - 2008
Formalization [11] - 2017

Traditional GNN



Most GNN consider a single **Monolithic and Static** graph

[10] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, et G. Monfardini, « The Graph Neural Network Model », *IEEE Transactions on Neural Networks*, vol. 20, nº 1, p. 61-80, janv. 2009, doi: 10.1109/TNN.2008.2005605.

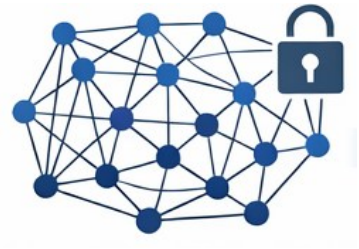
[11] J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals, et G. E. Dahl, « Neural Message Passing for Quantum Chemistry », 12 juin 2017, arXiv:1704.01212. doi: 10.48550/arXiv.1704.01212.

State of the art for GNN

Recent Domain

First paper [10] - 2008
Formalization [11] - 2017

Traditional GNN



Most GNN consider a single **Monolithic and Static** graph

Dynamic GNN

Specific GNN called
Dynamic **G**raph **N**eural **N**etwork
This domain is even more recent [12]

[12] E. Rossi, B. Chamberlain, F. Frasca, D. Eynard, F. Monti, et M. Bronstein, « Temporal Graph Networks for Deep Learning on Dynamic Graphs », 9 octobre 2020, *arXiv*: arXiv:2006.10637. doi: 10.48550/arXiv.2006.10637.

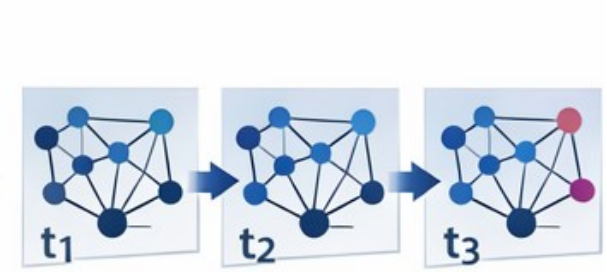
Dynamic GNN

Dynamic **G**raph **N**eural **N**etwork
(DGNN)

Dynamic GNN

Dynamic **G**raph **N**eural **N**etwork
(DGNN)

Discrete **T**ime **D**ynamic **G**raph
(DTDG)

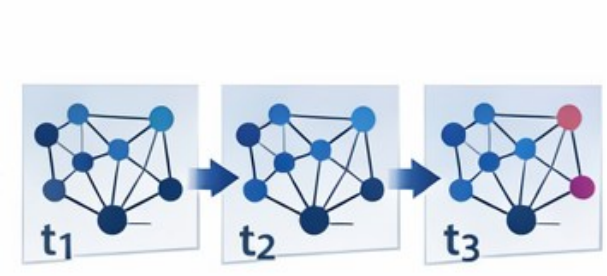


Graph snapshots at different time intervals
Each contain the entire graph state
Straightforward + Long time dependencies

Dynamic GNN

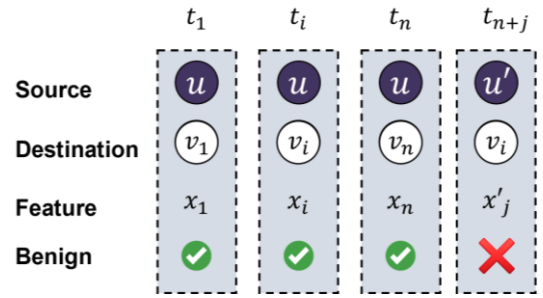
Dynamic **G**raph **N**eural **N**etwork
(DGNN)

Discrete **T**ime **D**ynamic **G**raph
(DTDG)



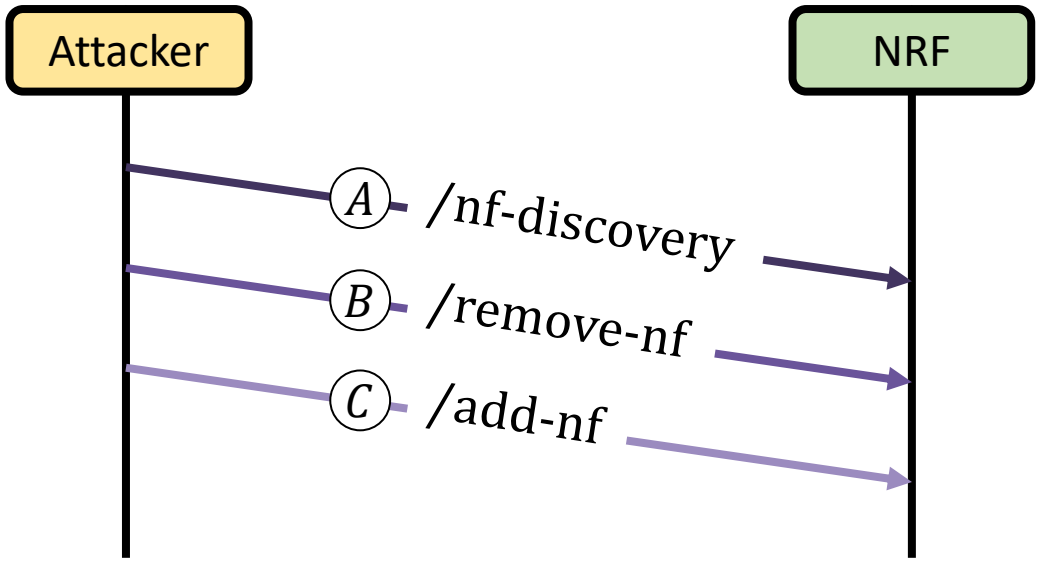
Graph snapshots at different time intervals
Each contain the entire graph state
Straightforward + Long time dependencies

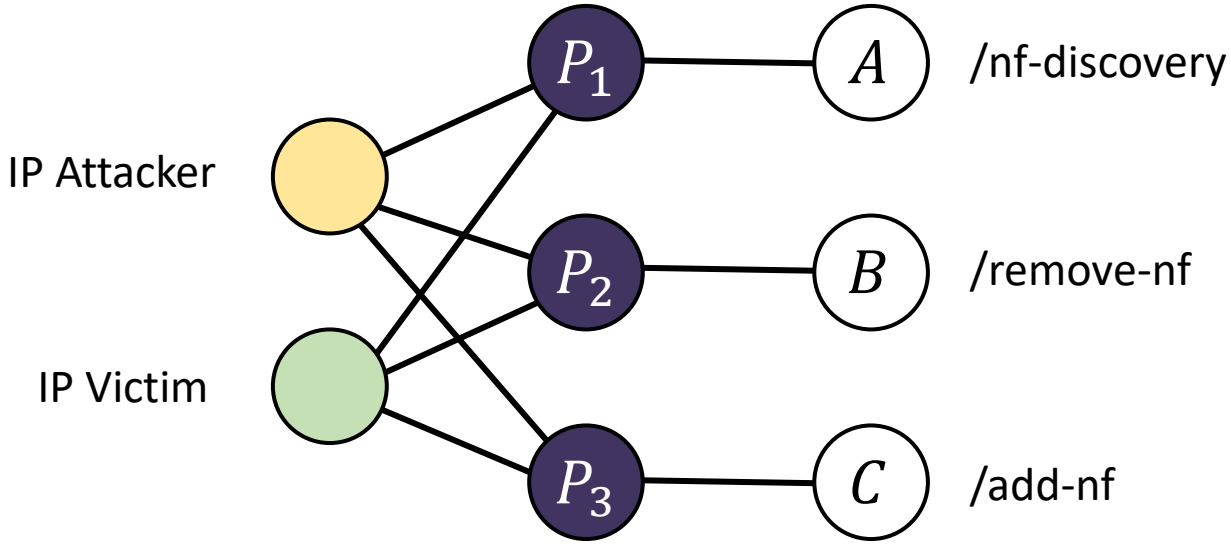
Continuous **T**ime **D**ynamic **G**raph
(CTDG)



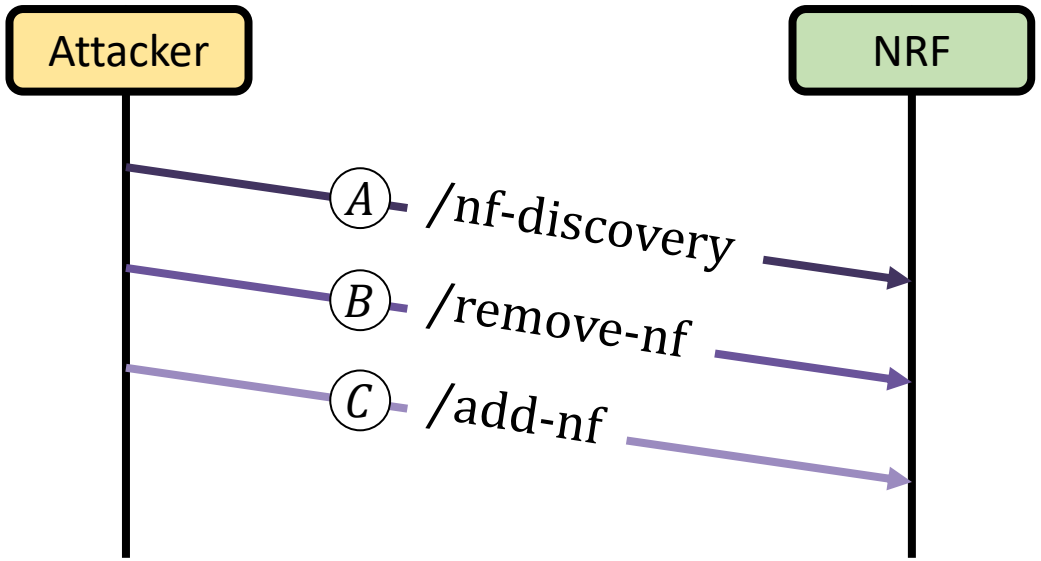
Event sequences (add, supp, modif..)
Represent the graph evolution at each step
No information loss + fine-grained

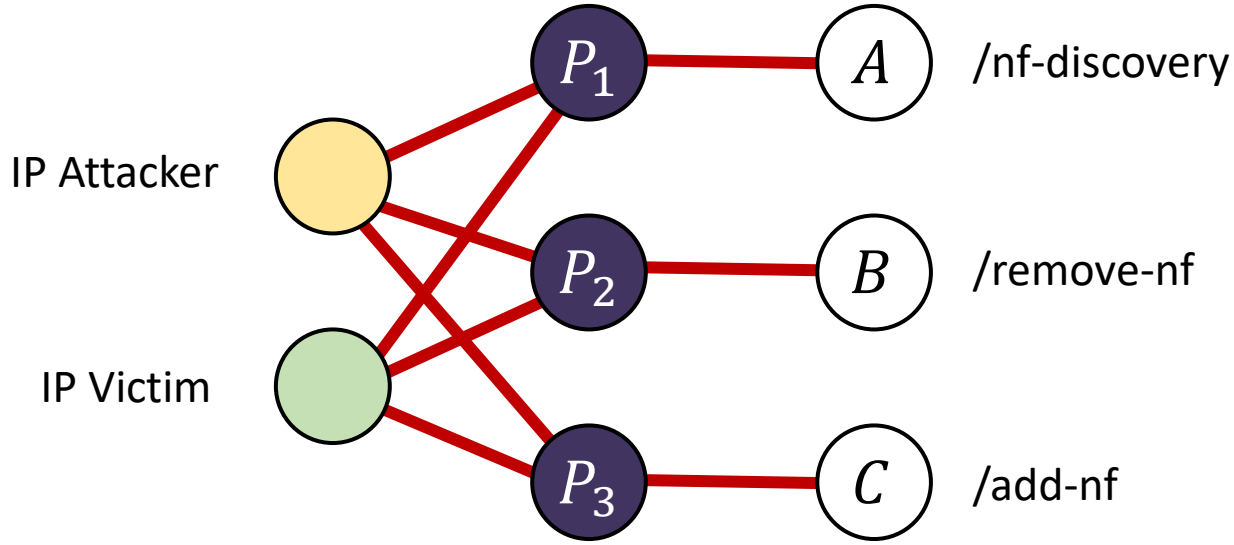
Example of CTDG transformation

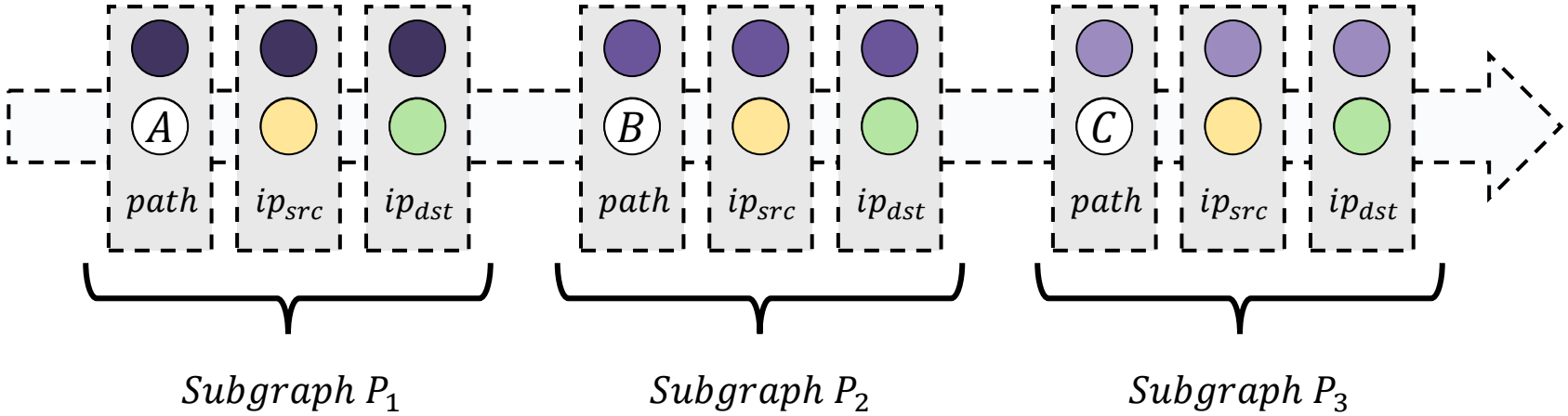




Example of CTDG transformation



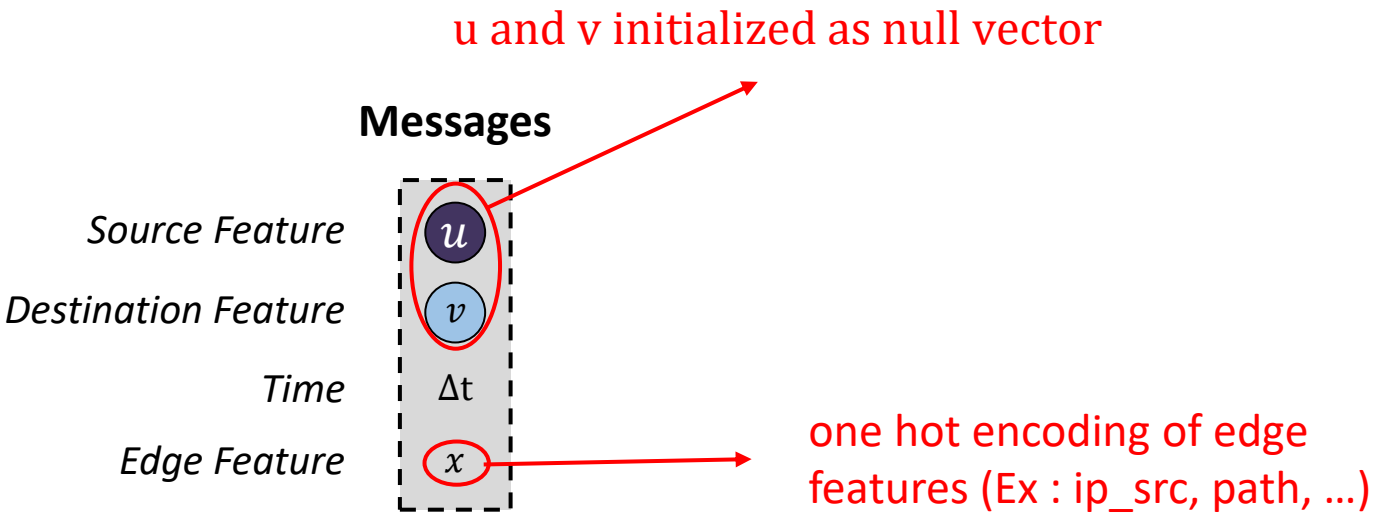




Model and Learning Process

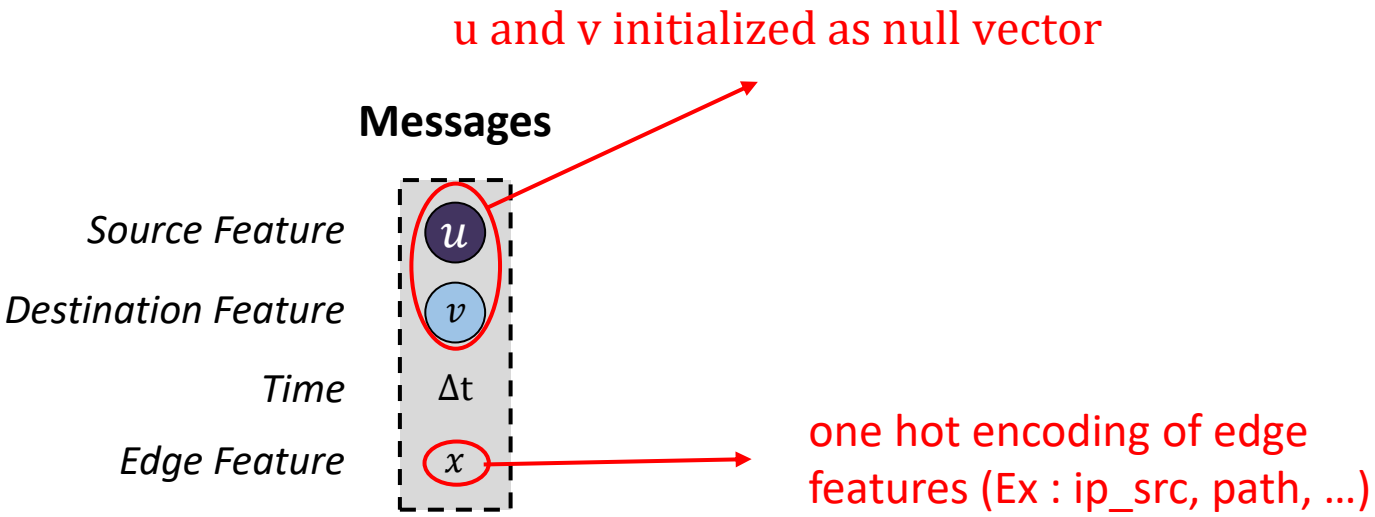
How does the machine learn

Deeper explanation of GNNs



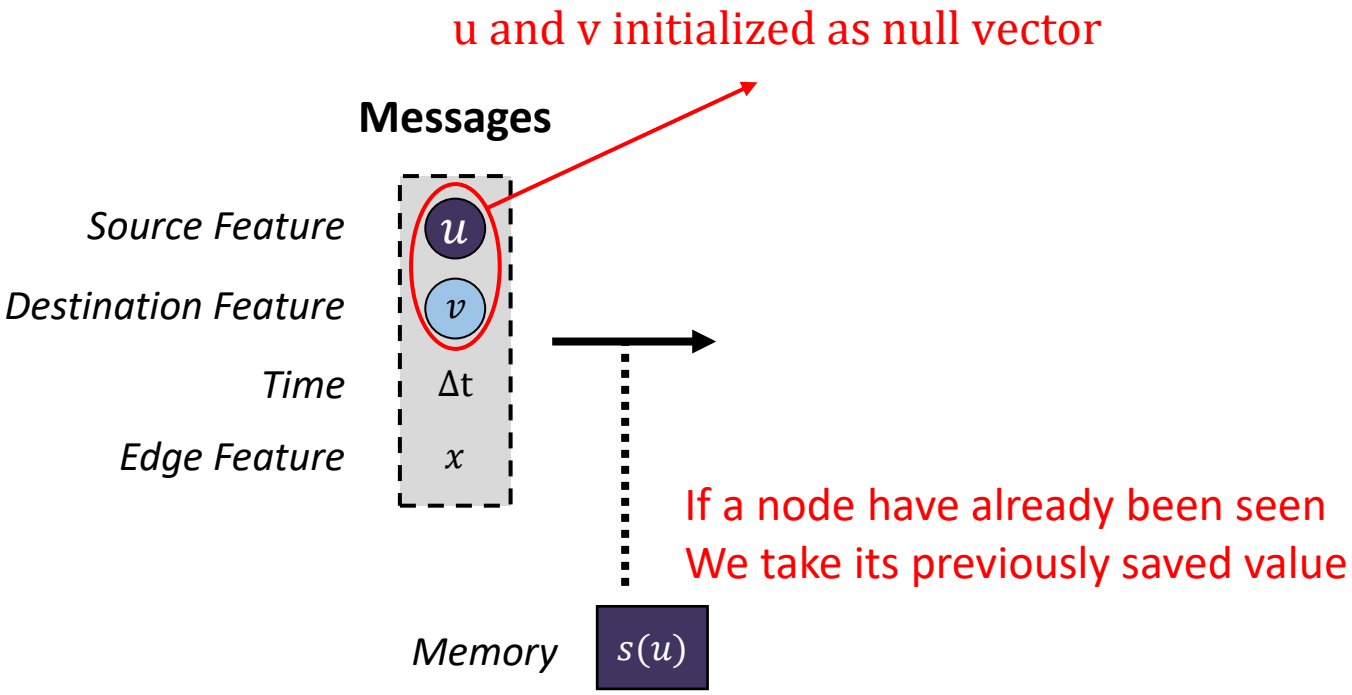
$$m(u) = \text{concat}(\text{u}, v, t, x)$$

Deeper explanation of GNNs

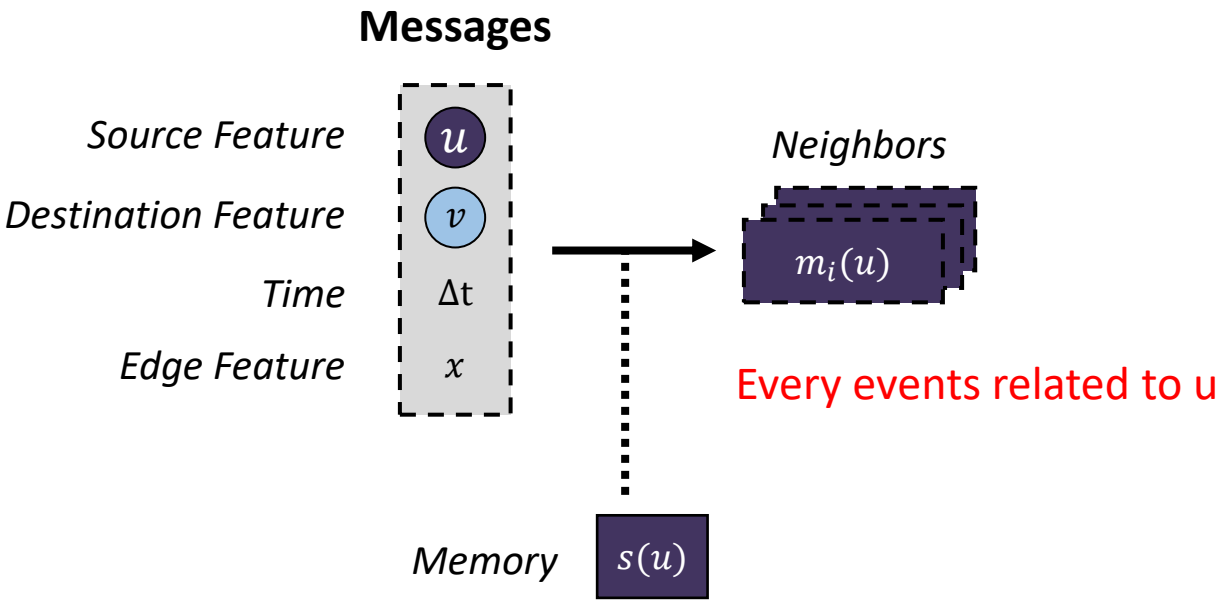


$$m(u) = \text{concat}(\text{u}, v, t, x)$$

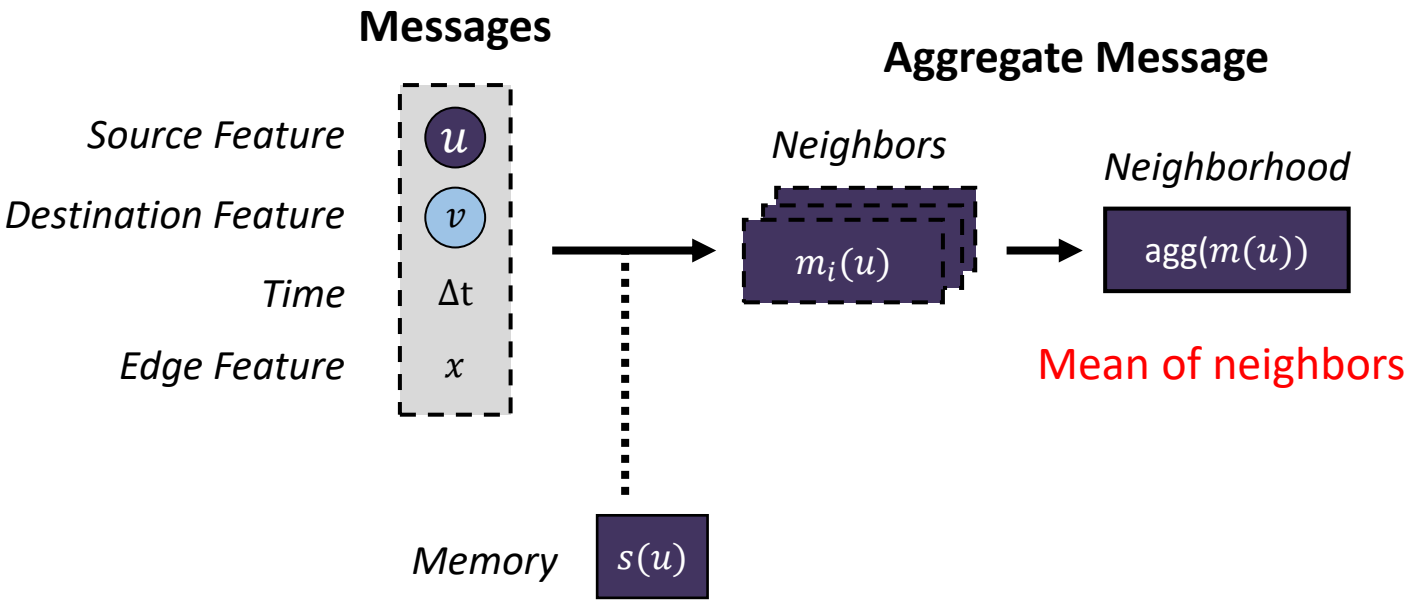
Deeper explanation of GNNs



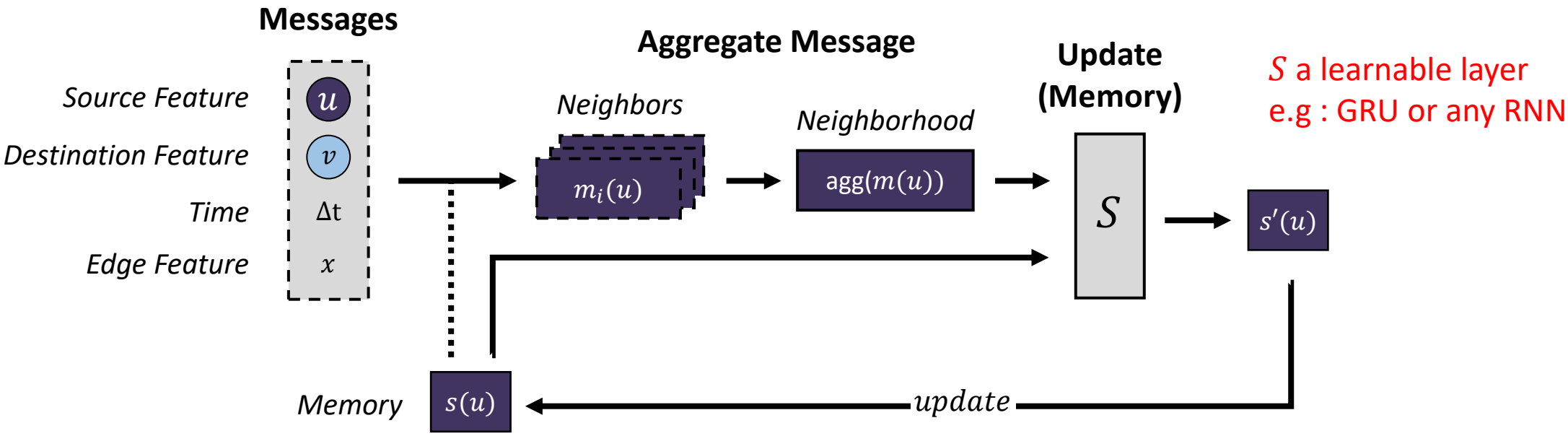
Deeper explanation of GNNs



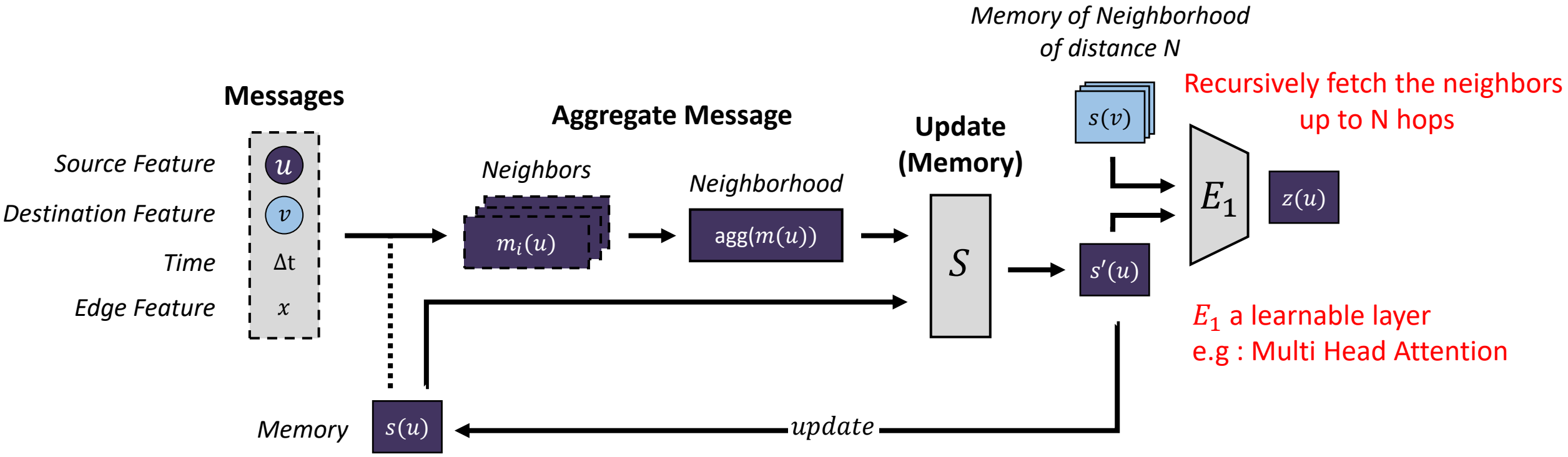
Deeper explanation of GNNs



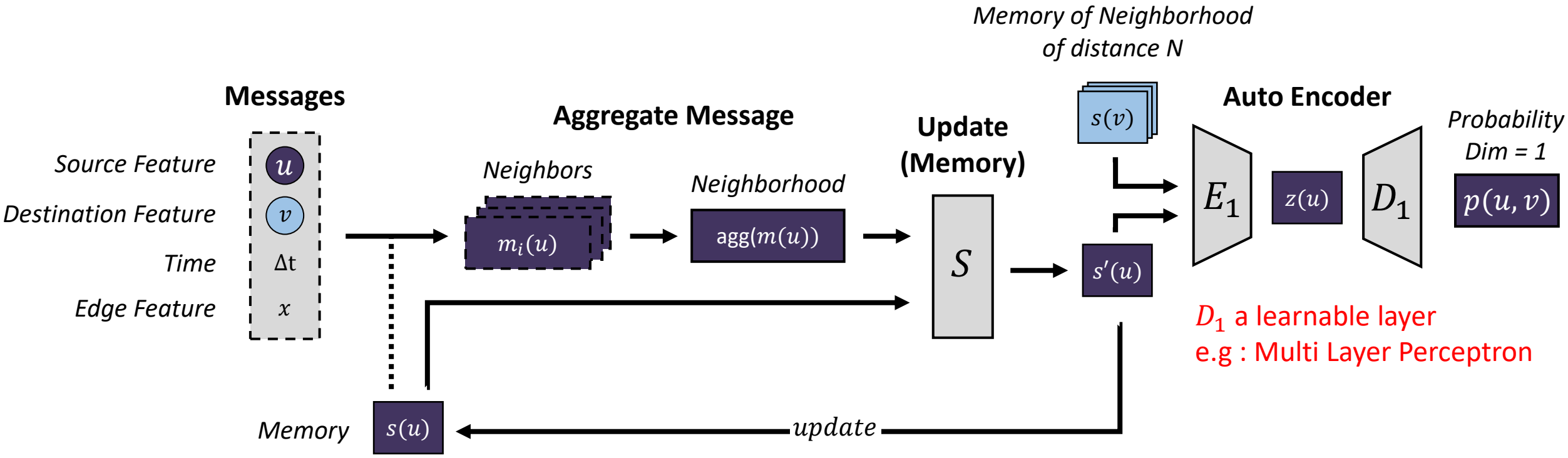
Deeper explanation of GNNs



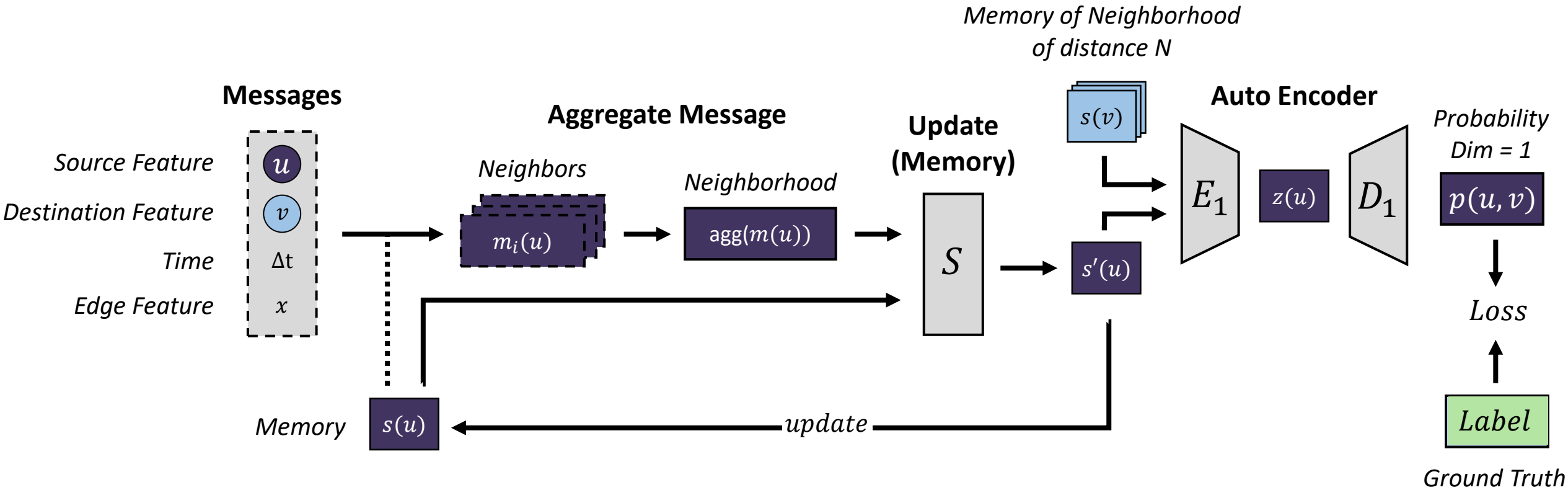
Deeper explanation of GNNs



Deeper explanation of GNNs



Deeper explanation of GNNs



Experimentation

Dataset content and process

Dataset State of the Art

Dataset	PCAP available	Code available	Benign procedures				
			(De)registration	Session management	State switching	NF management	UPF Forwarding
5GAD [13]	✓	✓					
PFCP IDD [14]	✓						
GSAD			✓				
AdSeq			✓	✓			
Prov5G			✓	✓	✓		
5GCguard		✓	✓	✓			
Our solution	✓	✓	✓	✓	✓	✓	✓

[13] C. Coldwell *et al.*, « Machine Learning 5G Attack Detection in Programmable Logic », in *2022 IEEE Globecom Workshops (GC Wkshps)*, déc. 2022, p. 1365-1370. doi: 10.1109/GCWkshps56602.2022.10008647.

[14] G. Amponis *et al.*, « 5G Core PFCP Intrusion Detection Dataset », in *2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, juin 2023, p. 1-4. doi: 10.1109/MOCAST57943.2023.10176693.

https://doi.org/10.5281/zenodo.15853959 | https://github.com/thomas-hoger/CTD-5G

Experiments with CTD5G Dataset

Benign			Attack		
Name	**Procedure Count**	**Packet Count**	**Name**	**Procedure Count**	**Packet Count**
Register UE	591	467,638	Fuzz	107	33,308
Restart Session	562	379,181	CN MiTM	123	22,587
User Traffic	317	159,228	SEID Fuzzing	116	23,858
Set UE Idle	288	67,124	Flood Establishment	113	23,949
Uplink Wake	137	55,599	Flood Deletion	98	20,446
Deregister UE	276	50,279	Applicative Scan	81	4,997
Downlink Wake	279	21,884	Modify Duplicate	119	345
Add NF	261	18,232	Modify Drop	100	292
Remove NF	253	16,336	Uplink Spoofing	102	102
			PFCP in GTP	101	101
Total	2,265	1,235,501	**Total**	1,060	129,985

Experiments with CTD5G Dataset

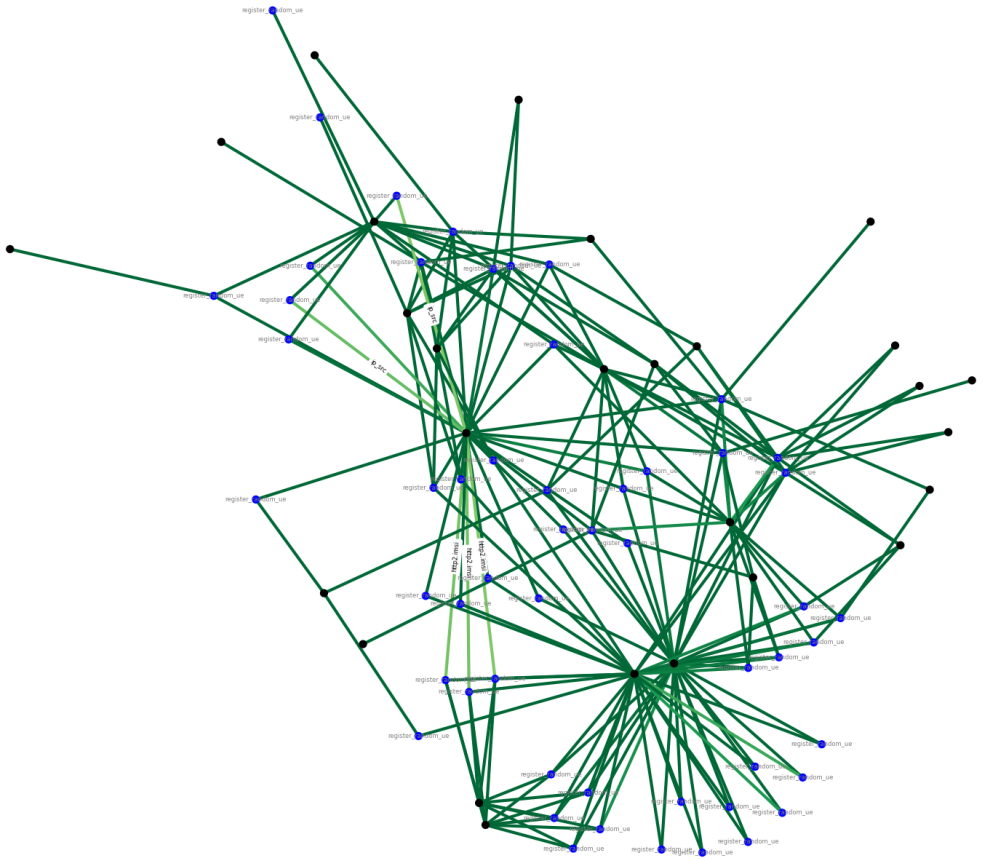
Attack name	Semantic	Sequential	Interaction
Applicative MiTM			✖
Applicative Scan		✖	✖
API Fuzzing	✖	✖	
Session Establishment Flood		✖	
Session Deletion Flood		✖	
SEID Fuzzing	✖	✖	
Session Modify Drop	✖	✖	
Session Modify Duplicate	✖	✖	
Uplink Spoofing	✖		✖
PFCP in GTP	✖		✖

Results : Metrics

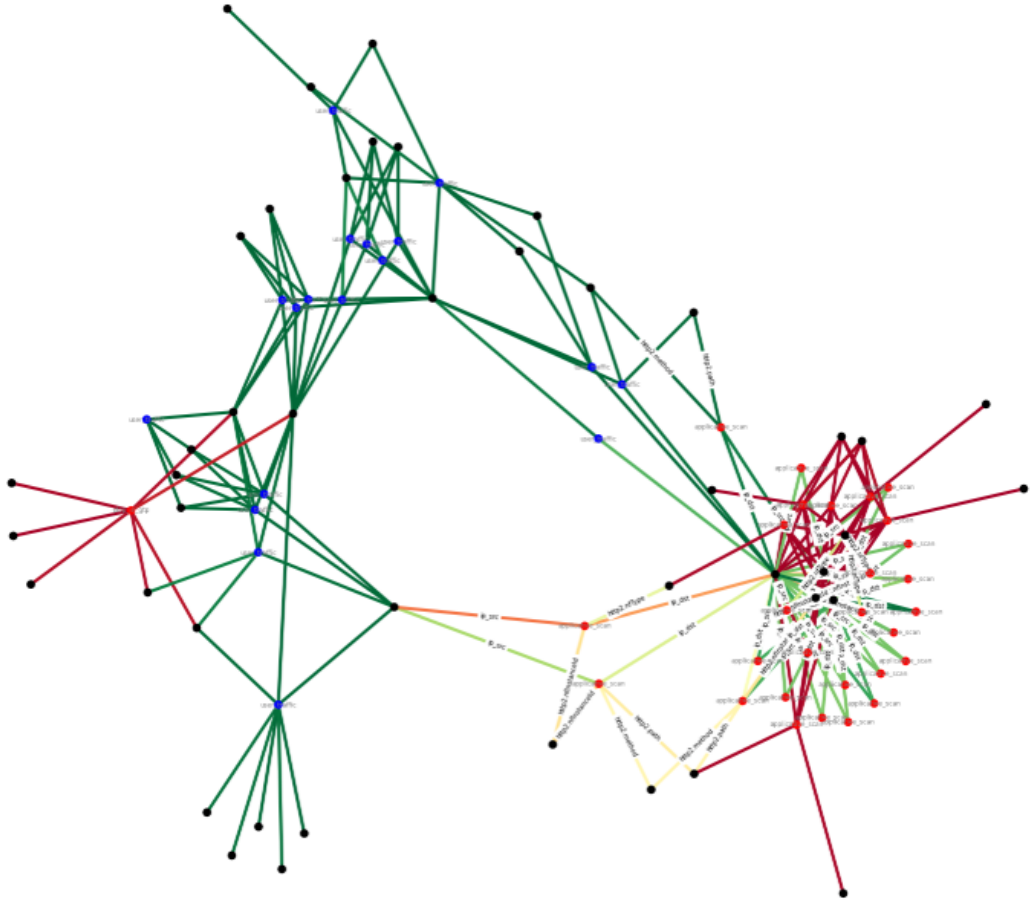
Metric	JODIE	DyRep	CAWN	DyGFormer	TCL	GraphMixer	TGN
Accuracy	0.7432	0.7581	0.7514	0.8386	0.8466	0.8361	0.9497
Precision	0.7226	0.8112	0.9611	0.9224	0.8916	0.9041	0.9509
Recall	0.1954	0.3568	0.1548	0.4879	0.5404	0.4906	0.8727
F1 Score	0.3077	0.4956	0.2666	0.6383	0.6729	0.6360	0.9102

https://github.com/yule-buaa/dyglib

Results : Explainability



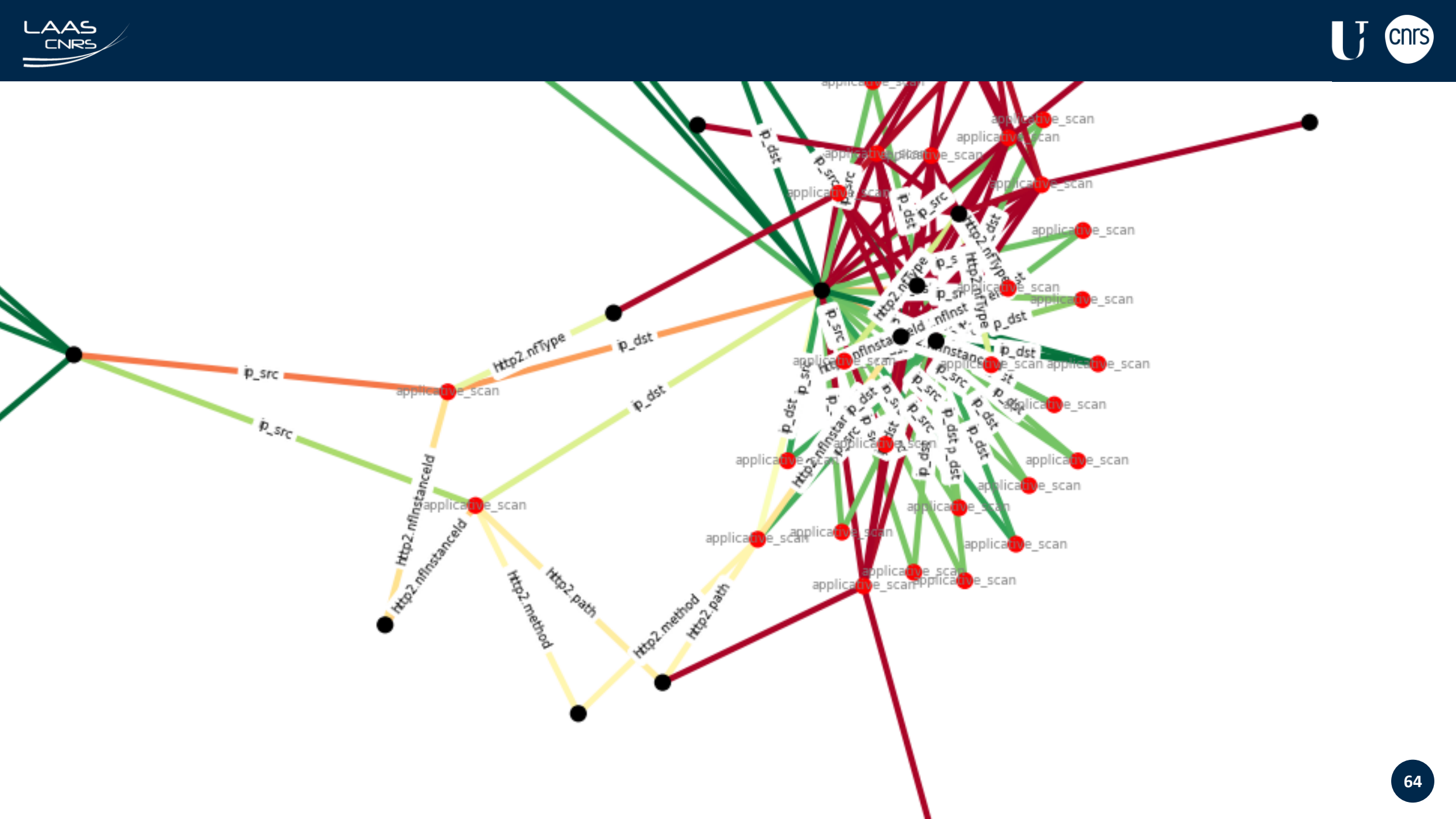
Benign (UE registration)



Attack (NF Scanning)

Thank you for your attention

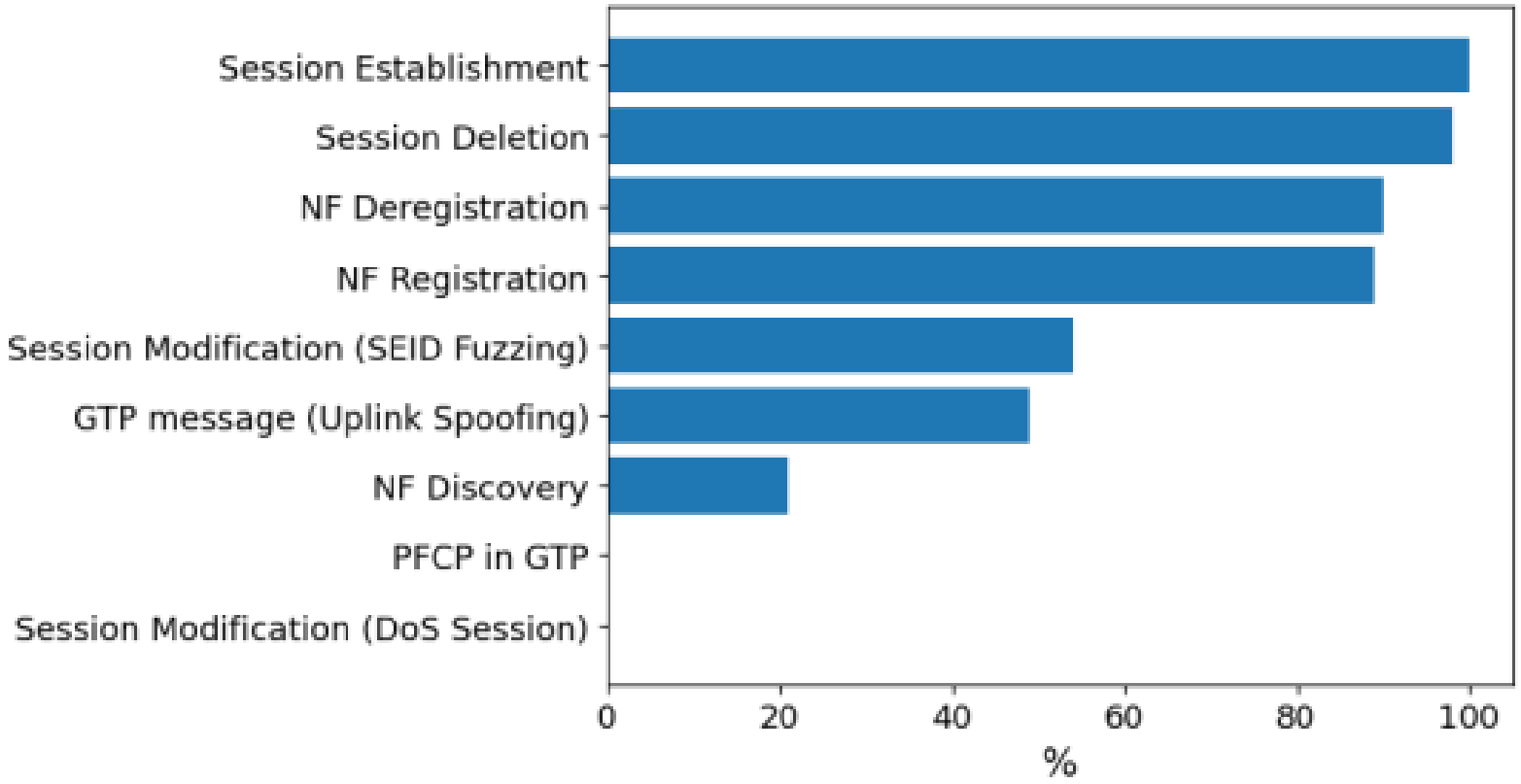
Do you have questions ?


ip_src
ip_dst
http2.nfType
http2.nflnstanceId
http2.path
http2.method
applicative_scan

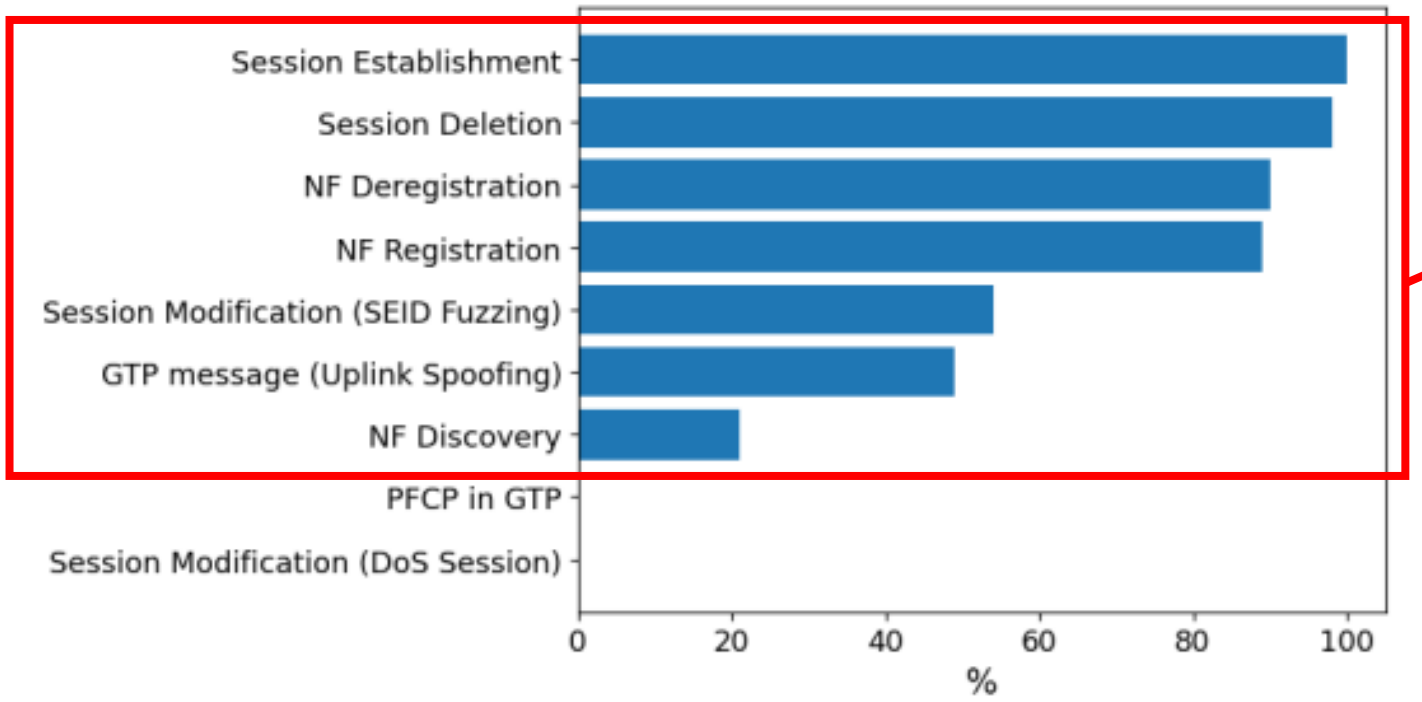
Property Evaluation

Characterizing each type of attacks

Analyzing semantic diversity

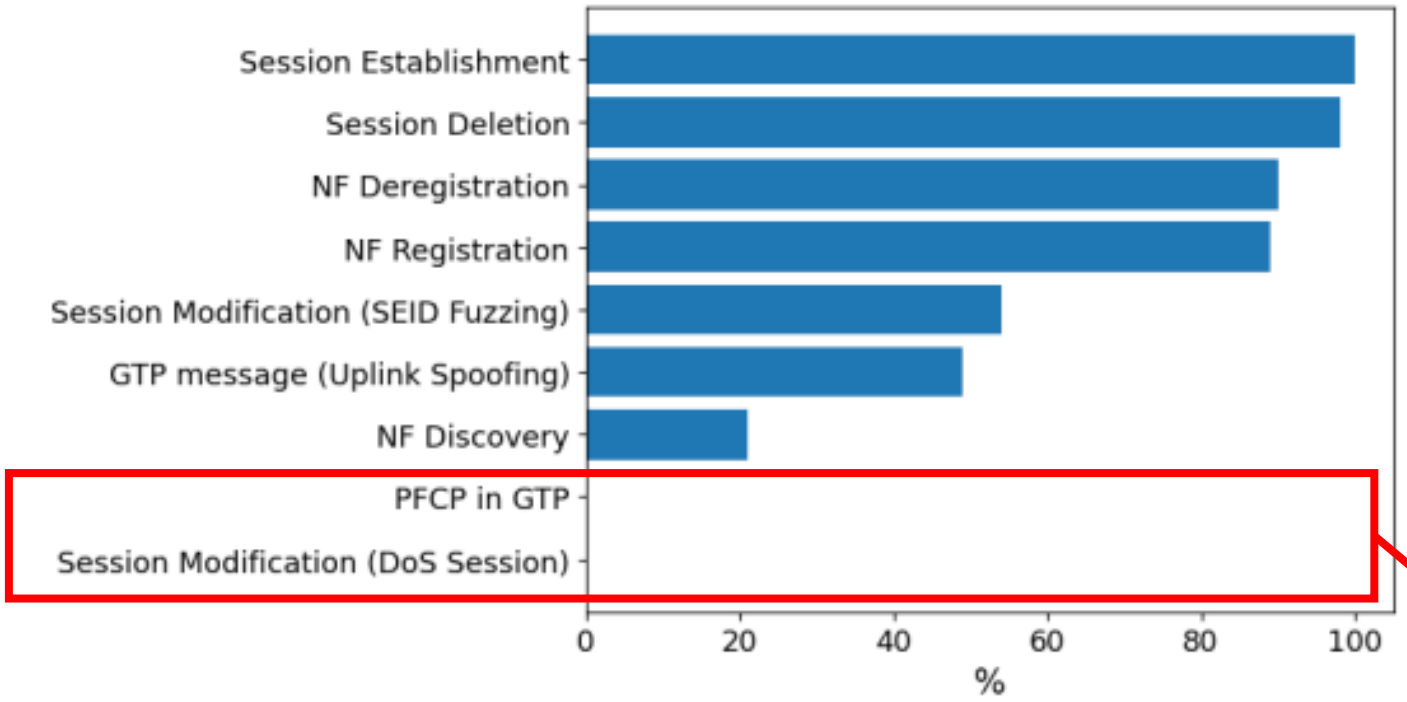


Analyzing semantic diversity



There exist at least **some** benign packets that are semantically identical to attack packets

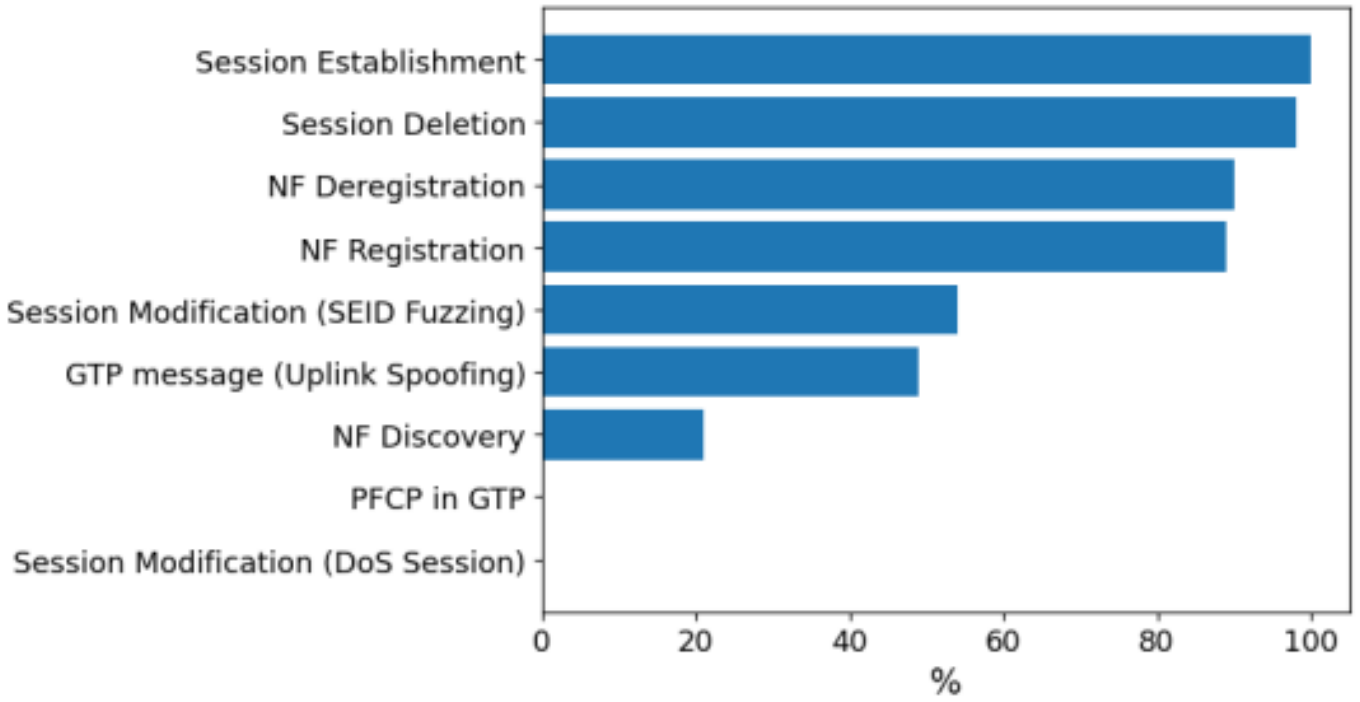
Analyzing semantic diversity



Malicious procedure	Comparable benign messages	Detection Type
Applicative NF scanning	NF Discovery	Repetition
API fuzzing	Any API call	Repetition / Semantic
Man-in-the-middle in the CN	NF Discovery and (De)registration	Interactions
Establishment flooding	Session establishment	Repetition
Deletion flooding	Session deletion	Repetition
Session DoS	Session modification	Repetition / Semantic
SEID fuzzing	Session modification	Repetition
PFCP-in-GTP	Any GTP message	Semantic
Uplink spoofing	Any GTP message	Interactions

There is no such message in benign trafic

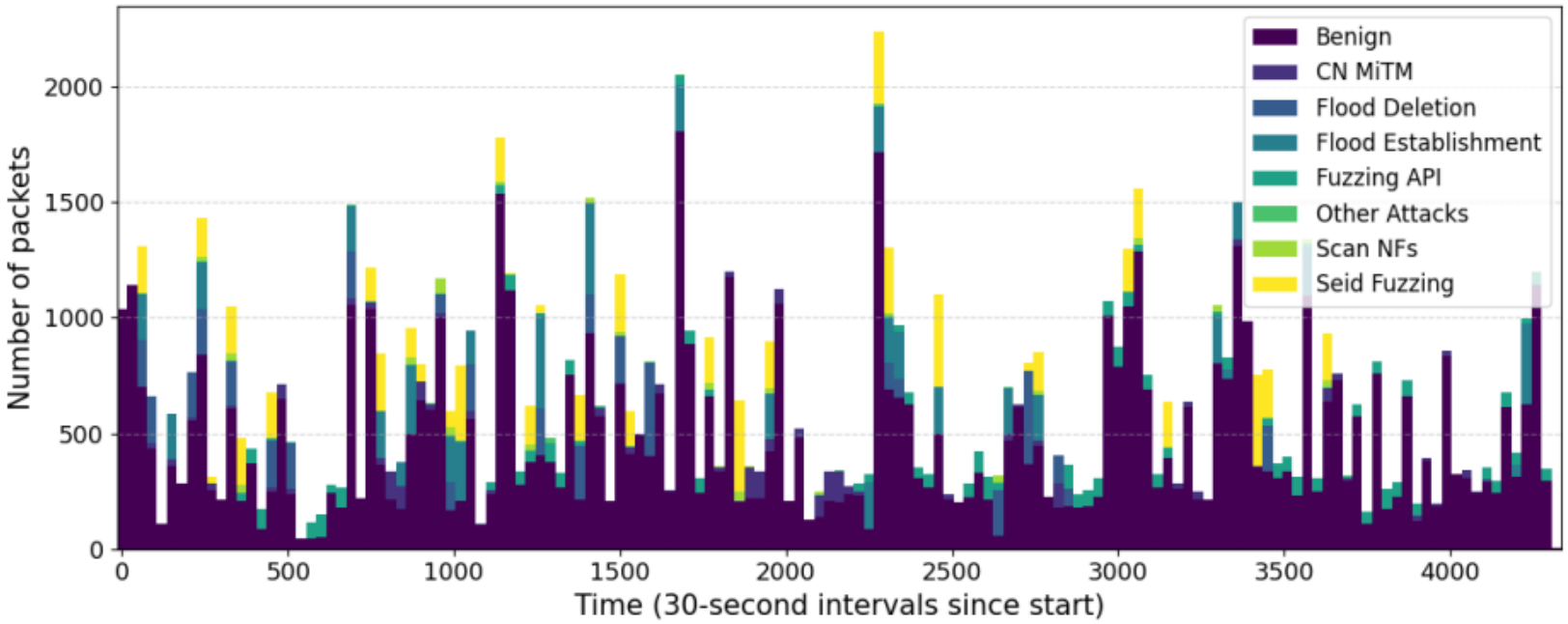
Analyzing semantic diversity



Malicious procedure	Comparable benign messages	Detection Type
Applicative NF scanning	NF Discovery	Repetition
API fuzzing	Any API call	Repetition / Semantic
Man-in-the-middle in the CN	NF Discovery and (De)registration	Interactions
Establishment flooding	Session establishment	Repetition
Deletion flooding	Session deletion	Repetition
Session DoS	Session modification	Repetition / Semantic
SEID fuzzing	Session modification	Repetition
PFCP-in-GTP	Any GTP message	Semantic
Uplink spoofing	Any GTP message	Interactions

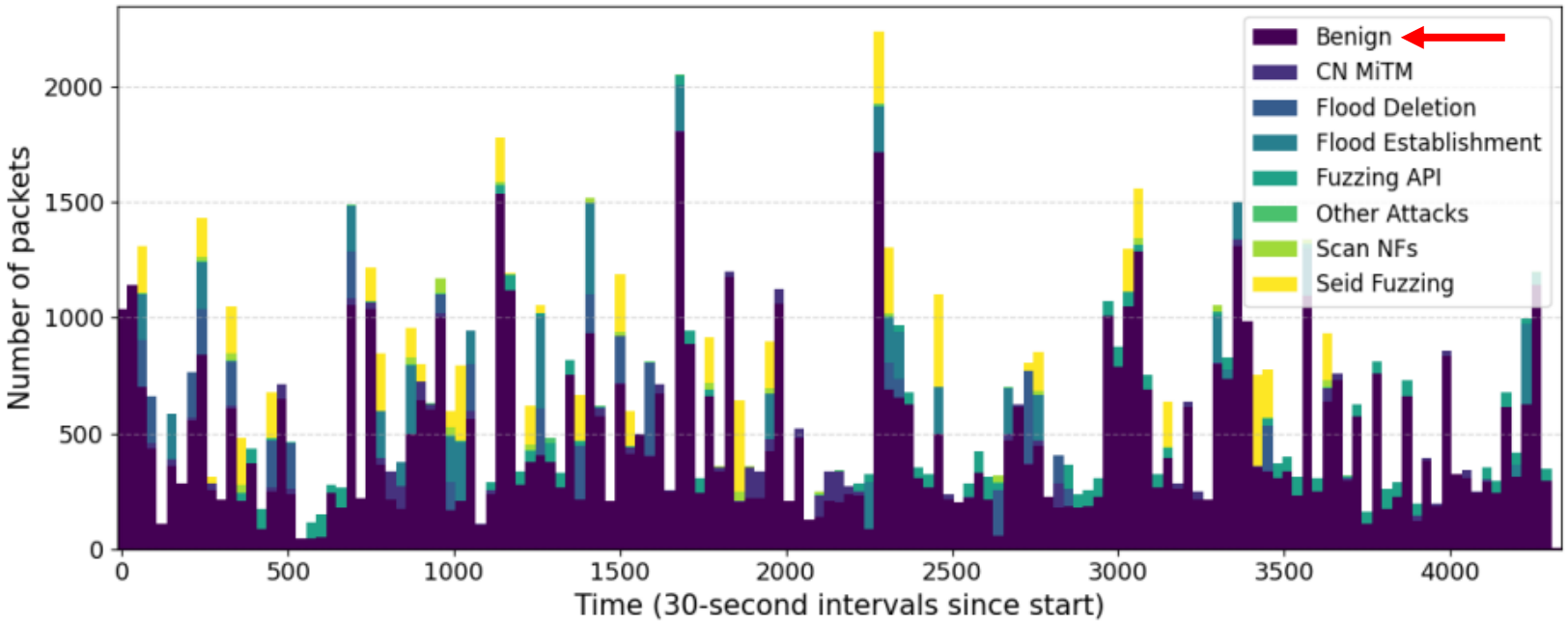
89% API Fuzzing message do not have semantically identical benign counterpart

Analyzing sequence diversity



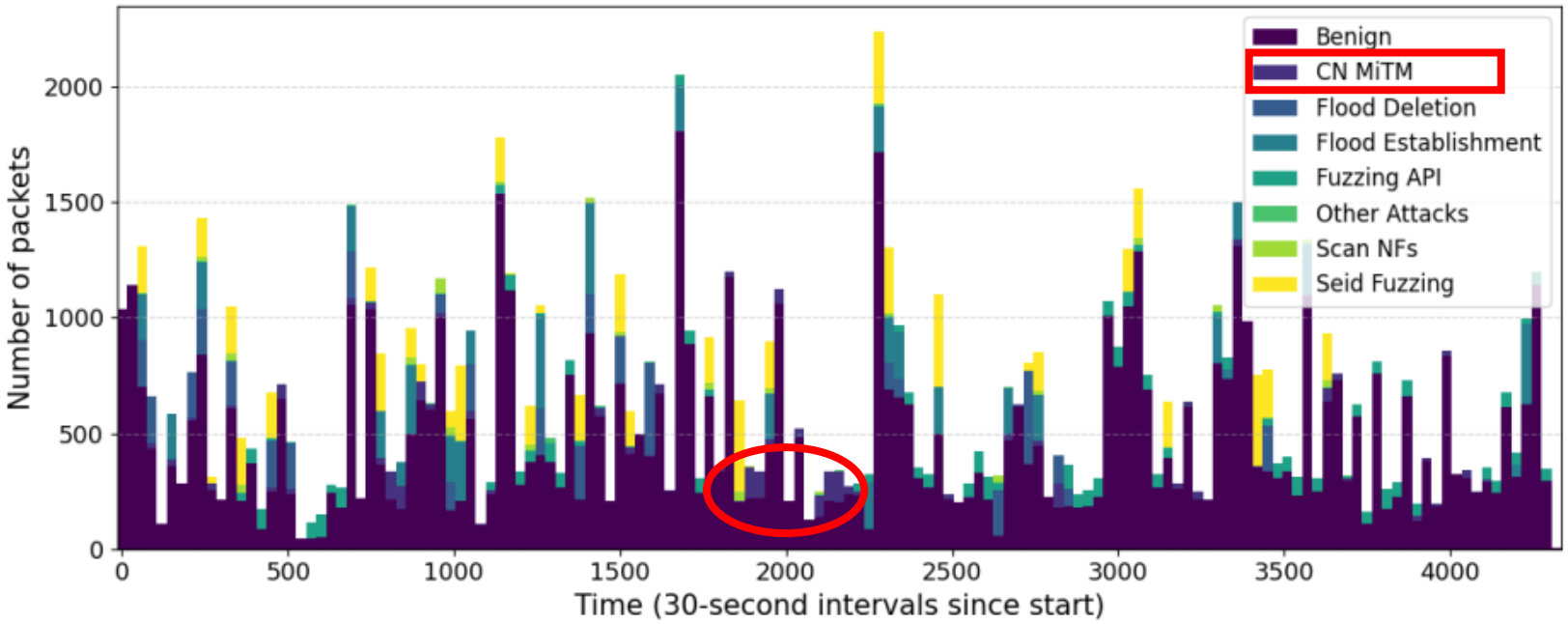
Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

Analyzing sequence diversity



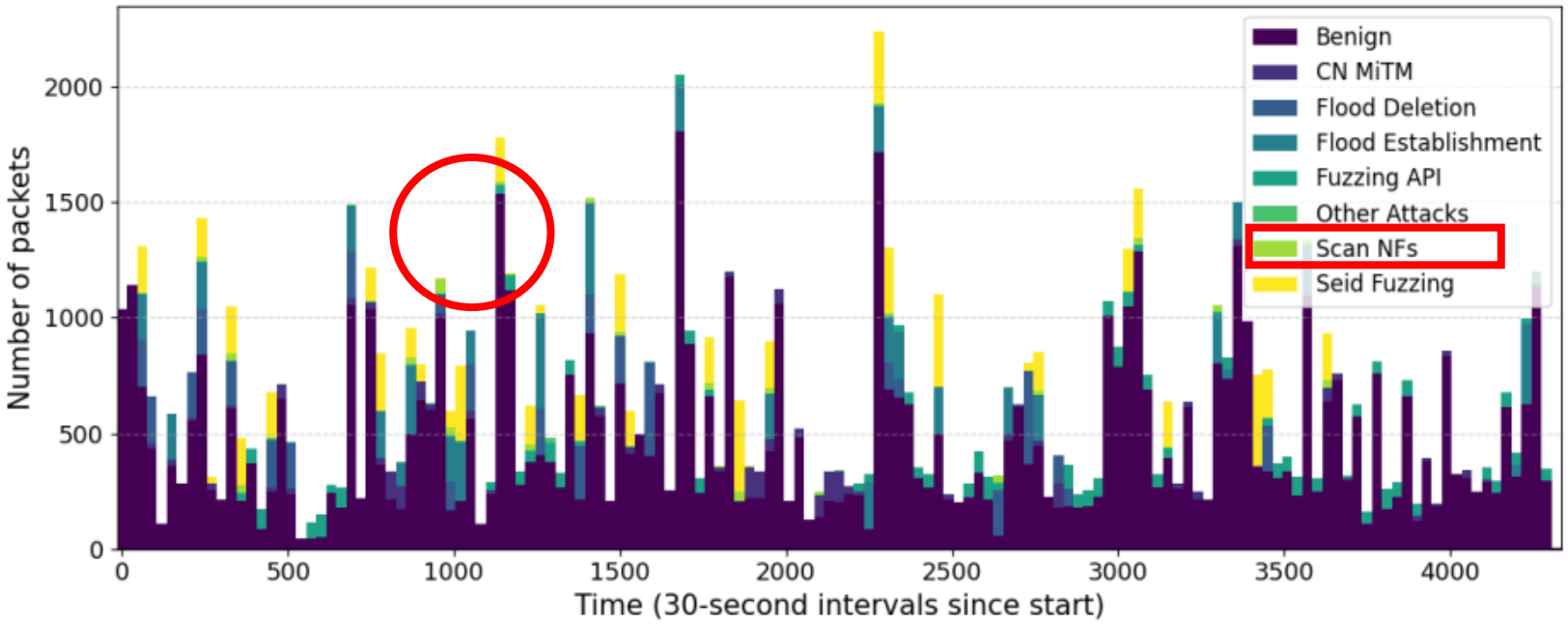
Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

Analyzing sequence diversity



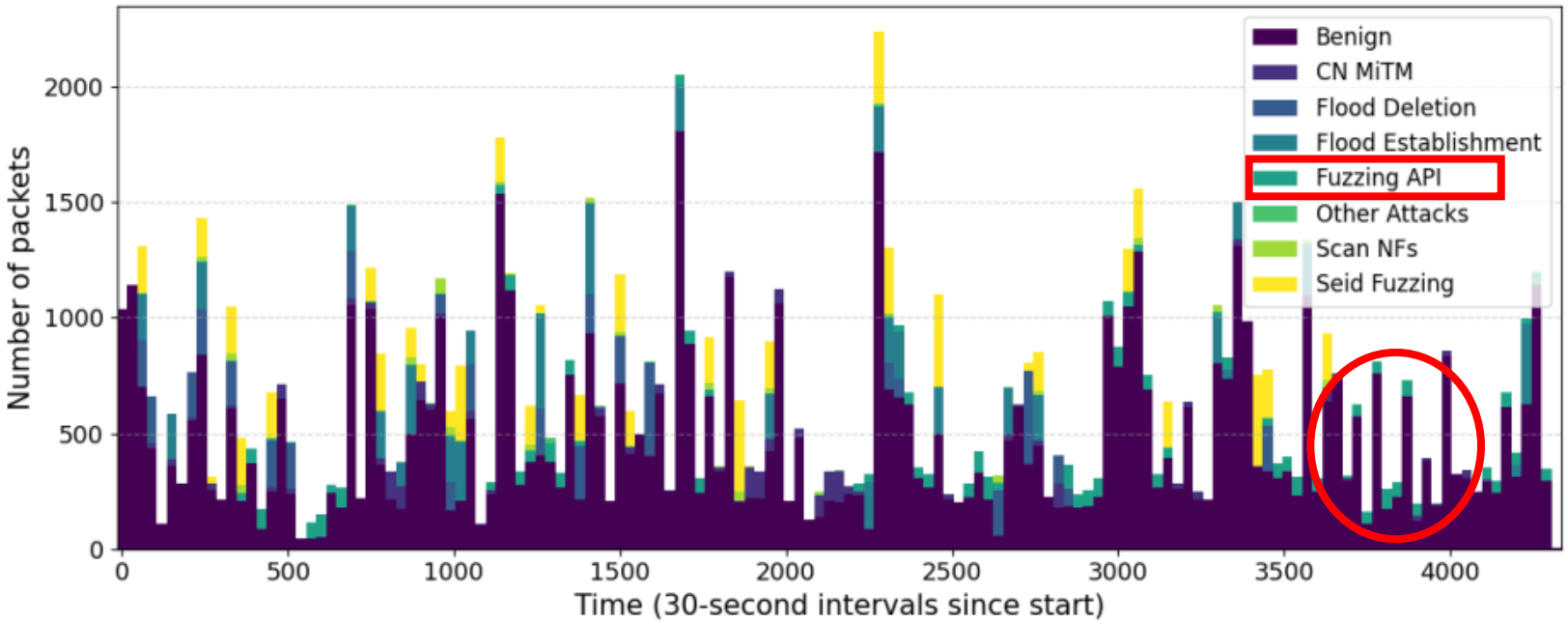
Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

Analyzing sequence diversity



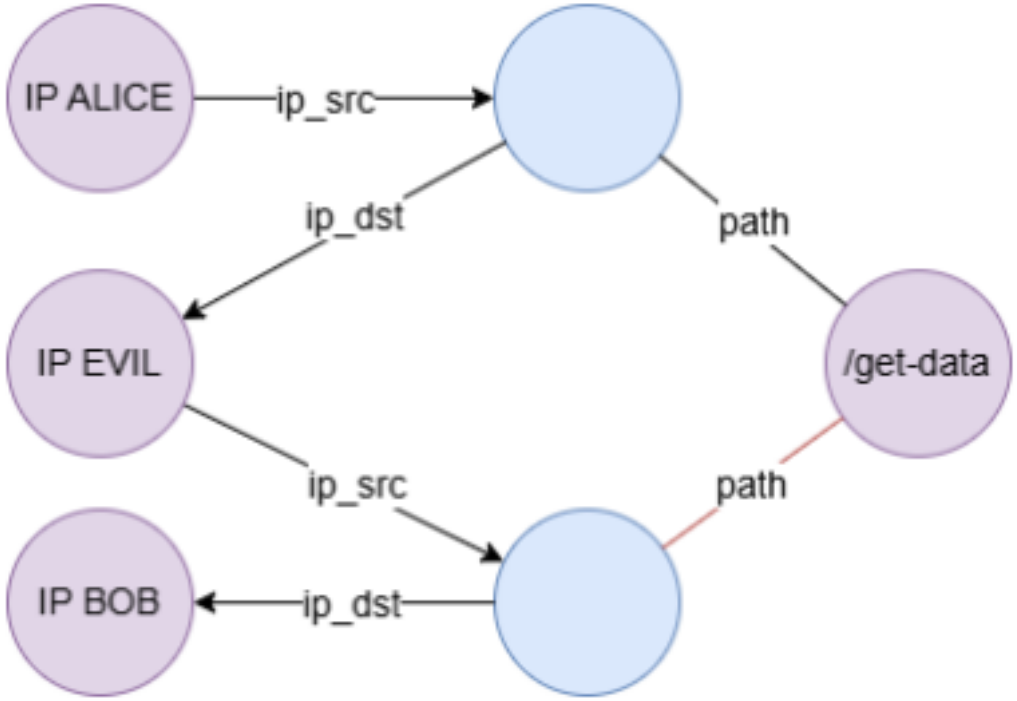
Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

Analyzing sequence diversity



Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

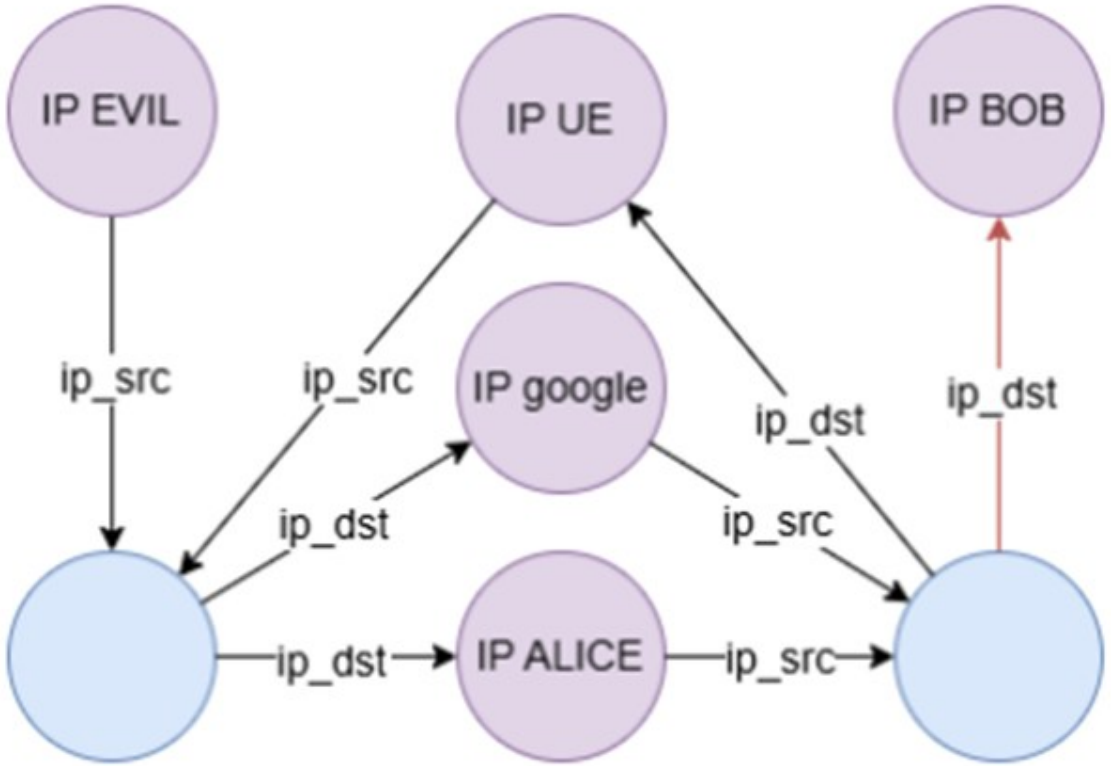
Analyzing interaction diversity



Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

4500 matches of redirection pattern

Analyzing interaction diversity



Malicious procedure	Detection Type
Applicative NF scanning	Repetition
API fuzzing	Repetition / Semantic
Man-in-the-middle in the CN	Interactions
Establishment flooding	Repetition
Deletion flooding	Repetition
Session DoS	Repetition / Semantic
SEID fuzzing	Repetition
PFCP-in-GTP	Semantic
Uplink spoofing	Interactions

72 matches / 92 procedure execution (packet loss)