Analyzing the Impact of DoS and Slicing Attack on Network Functions in 5G Core

By – Anand Keshav (210101014)

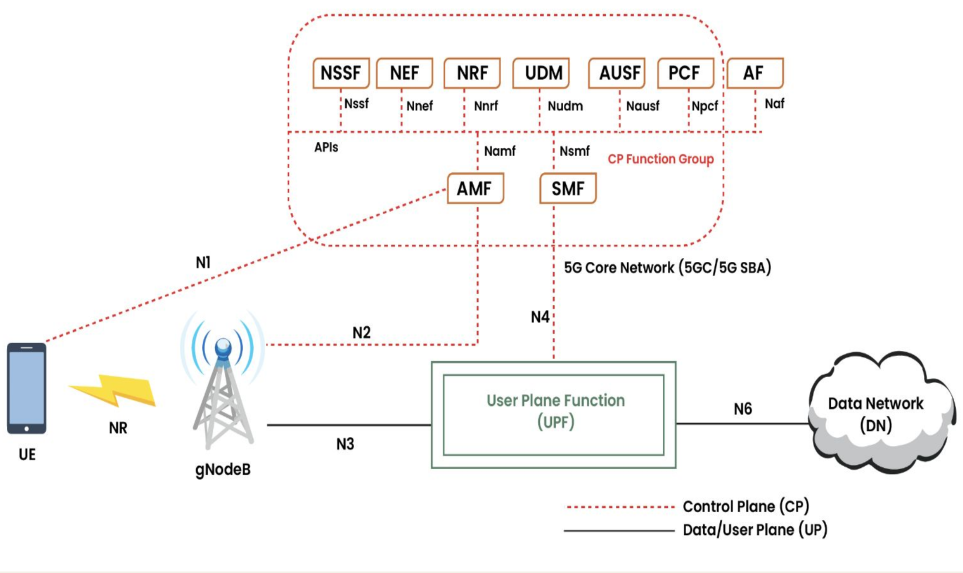
Under supervision of Dr. Moumita Patra

Abstract

This work focuses on detecting Denial of Service (DoS) and slicing attacks in the 5G core network by modeling inter-NF communications as provenance graphs. Building on Free5GC and UERANSIM, we enhance logging, simulate multiple attack scenarios, and develop a multi-model GraphSAGE-based detection framework capable of identifying anomalous NF behavior.

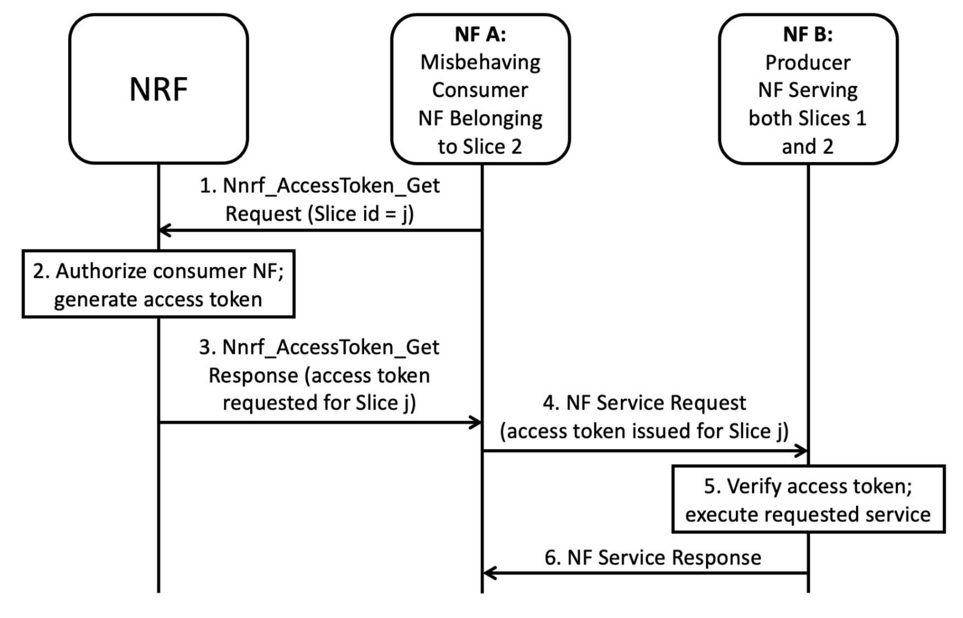
Introduction

- Service based Architecture (SBA)
- Network Slicing in 5G
- Critical Role of NRF in SBA

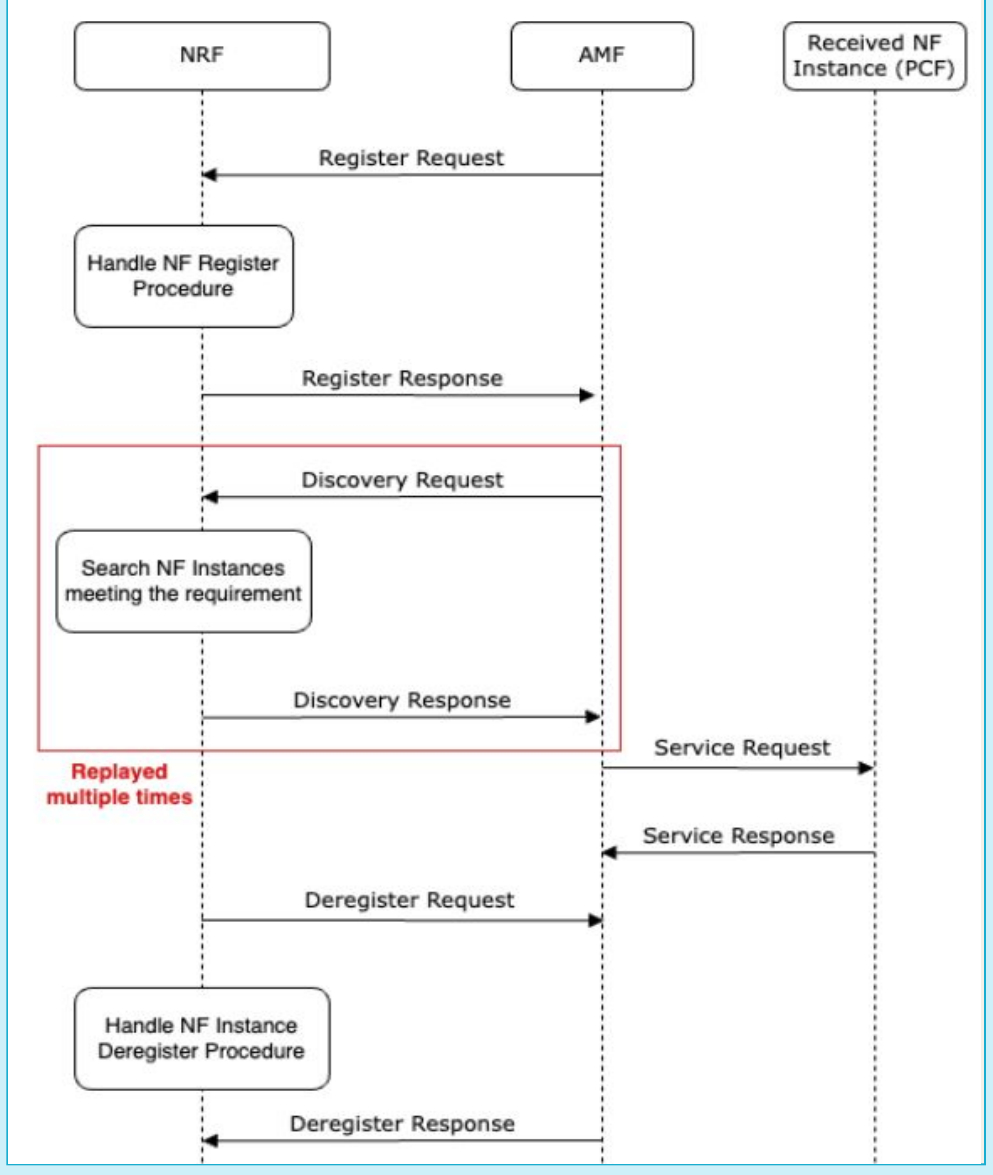


Threat Model

Slicing Attack

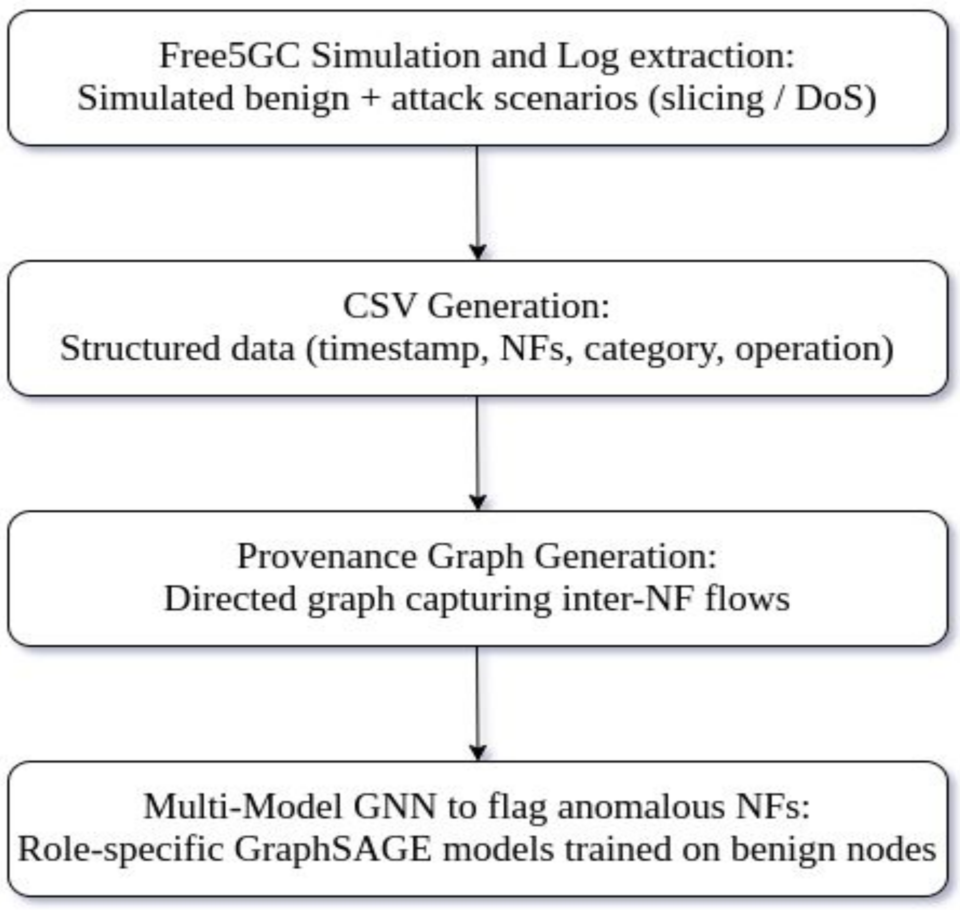

NRF
NF A: Misbehaving Consumer NF Belonging to Slice 2
NF B: Producer NF Serving both Slices 1 and 2
1. Nnrf_AccessToken_Get Request (Slice id = j)
2. Authorize consumer NF; generate access token
3. Nnrf_AccessToken_Get Response (access token requested for Slice j)
4. NF Service Request (access token issued for Slice j)
5. Verify access token; execute requested service
6. NF Service Response

NRF targeted DoS attack



Detection Framework

Anomaly Detection Pipeline



Free5GC Simulation and Log extraction: Simulated benign + attack scenarios (slicing / DoS)

CSV Generation: Structured data (timestamp, NFs, category, operation)

Provenance Graph Generation: Directed graph capturing inter-NF flows

Multi-Model GNN to flag anomalous NFs: Role-specific GraphSAGE models trained on benign nodes

Example **Provenance Graph** illustrating NF registration and gNodeB setup events captured from Free5GC logs.

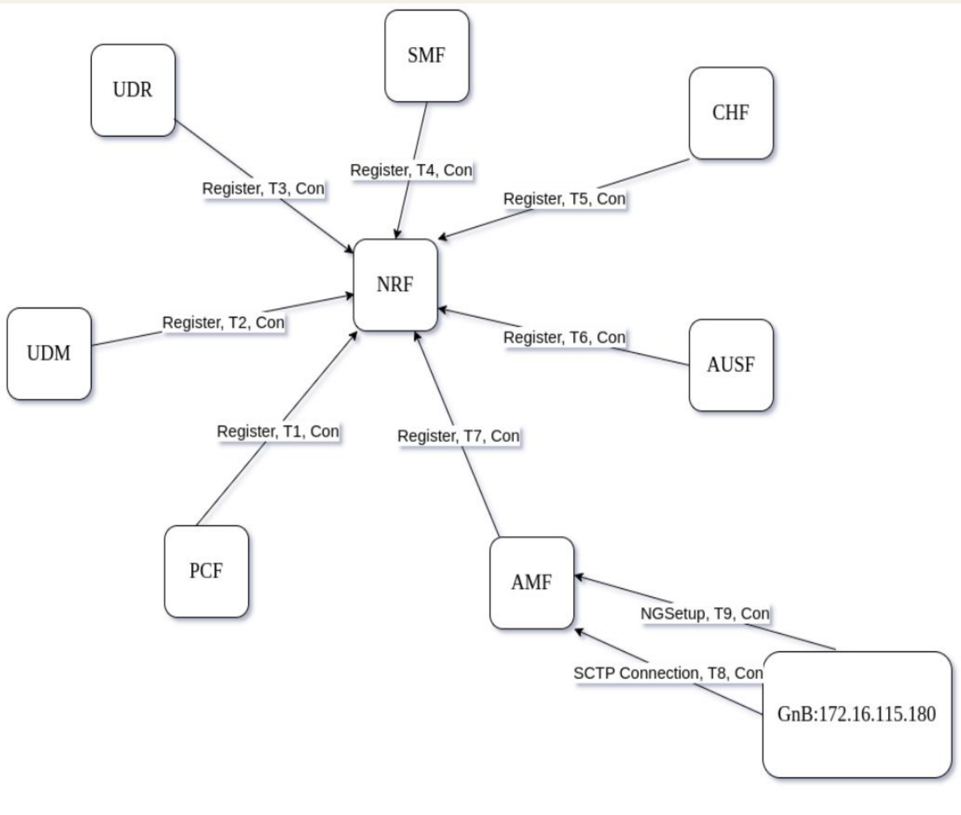


Fig. 5.1 Provenance Graph capturing NF registration and GnB setup

Feature Vector: (16 dimensional)NFRegister, NFDiscover, AccessToken, UEAuthentication, PDUSessionCreate, RequestLocationInfo, SessionModification, and SessionRelease

$$F(v) = [a_0, a_1, \ldots, a_{N_e-1}, a_{N_e}, \ldots, a_{2N_e-1}],$$

We use GraphSAGE with K=2 to capture structural features up to the **2-hop** neighborhood of each node. The Following These equations are applied iteratively for k=1,…,K during training.

$$\mathbf{m}_v^{(k)} = \mathrm{MEAN}(\{\mathbf{h}_u^{(k-1)} : u \in \mathcal{N}(v)\}),$$

$$\mathbf{h}_v^{(k)} = \sigma(W_k \parallel [\mathbf{h}_v^{(k-1)} \parallel \mathbf{m}_v^{(k)}]),$$

Normalized Entropy-Based Anomaly Score:

$$i^* = \arg\min_i H_i(v)$$

$$\mathrm{AnomalyScore}_{\mathrm{entropy}}(v) = \frac{H_{i^*}(v)}{\log C}$$

Confidence Score: Benign Condition for nodes

$$M_i(v) = \mathrm{softmax}(z_v^{(i)}) \quad \text{where } z_v^{(i)} \in R^C$$

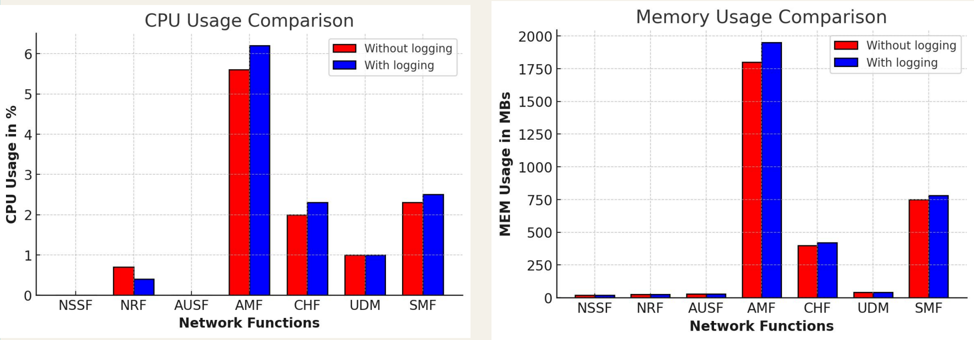
$$\frac{M_i(v)[\hat{c}]}{M_i(v)[\tilde{c}]} > R_t$$

Results

NRF targeted DoS - Metrics Comparison

Metric	**Before Attack**	**During Attack**
RAM Usage	5.97 GB	9.21 GB
CPU Util.	1–3%	16%
Load Average	0.22, 0.16, 0.13	1.36, 1.69, 1.37
Active Processes	Light load	Multiple NRF processes

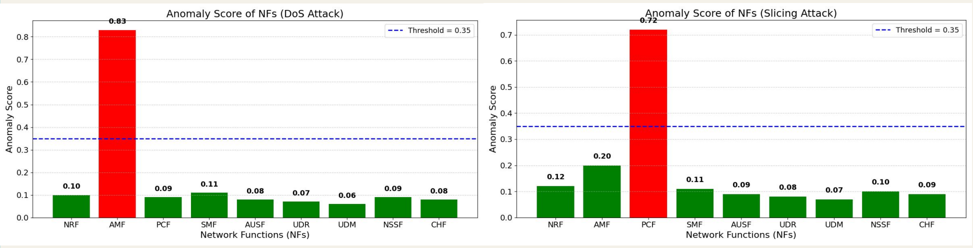
Performance Overhead of Enhanced Logging

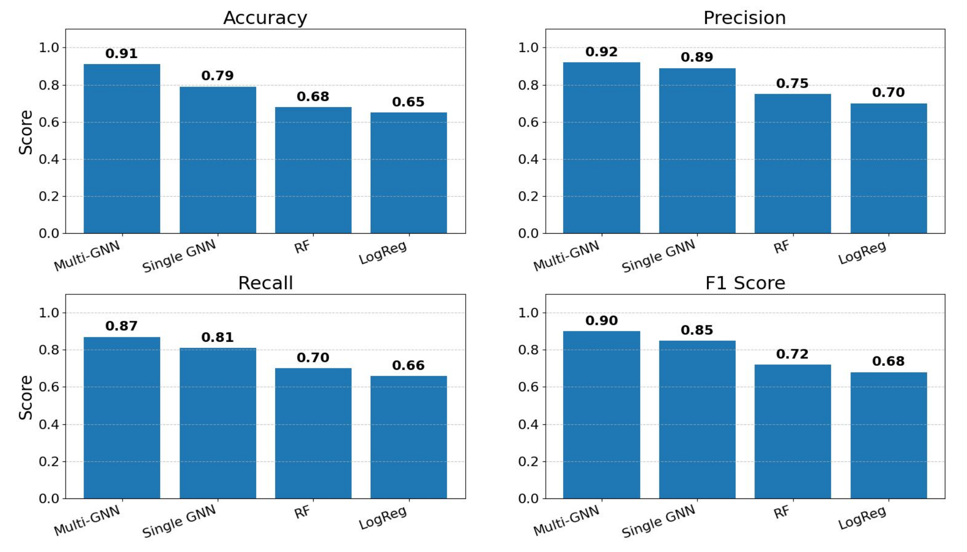


Free5GC logs confirming slicing attack success.

```
[INFO][PCF][Consumer] Sending Nnrf_AccessToken_Get request to NRF for Slice 1.
[INFO][NRF][Main] Received Nnrf_AccessToken_Get request from PCF.
[INFO][NRF][Main] Granted access token for PCF to access services of AMF for Slice 1.
[INFO][AMF][Producer] Handle Provide Location Info Request
[INFO][AMF][GIN] | 200 |       127.0.0.1 | POST    |
/namf-loc/v1/imsi-208930000000001/provide-loc-info |
[INFO][PCF][Consumer] Received response from AMF for UE Context ID
imsi-208930000000001 with status: 200
[INFO][PCF][Consumer] Received location information for UE Context ID
imsi-208930000000001: map[currentLoc:true
location:map[nrLocation:map[ageOfLocationInformation:-3.54575929e+08
ncgi:map[nrCellId:000000010 plmnId:map[mcc:208 mnc:93]] tai:map[plmnId:map[mcc:208
mnc:93] tac:000001] ueLocationTimestamp:2024-11-12T09:09:27.49813236Z]]
timezone:+05:30]
```

Anomaly score for various NF instances





Conclusion

Work done in Phase 1 of BTP:

- Setup and Simulation of attacks in Free5gc and UERANSIM.
- Analysed key vulnerabilities in the NRF and cross-slice communication.

Work done in Phase 2 of BTP:

- Instrumented Free5GC to log detailed SBI interactions (NF-to-NF, UE-to-NF).
- Generated structured CSV files for benign, slicing, and DoS scenarios and constructed provenance graphs.
- Applied a multi-model GraphSAGE based anomaly detector achieving robust attack detection.