5G Slice Isolation Through Resource Allocation

Dr. Ashraf Matrawy
Carleton University
Next Generation Networks Lab - carleton.ca/ngn

Presentation at KFUPM
November 26, 2024

Acknowledgement

I would like to acknowledge the contributions of my students to the research presented in these slides, Danish, Mahyoub, AbdulAziz, Emmanuel, Ezekiel, and Adam.

We work on ML in network security, security in IoT, 5G and beyond, misinformation, and usable security.

Please visit our group page for more information.
The Next Generation Networks Group carleton.ca/ngn

Agenda

1. Security Analysis of Critical 5G Interfaces
2. Earlier Work: Using Slice Isolation to Mitigate DDoS Attacks in 5G
3. Security-aware Network Function Sharing Model for 5G Slicing
4. Impact of Flooding Attacks on 5G Slicing with Different VNF Sharing Configurations
5. A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

Security Analysis of Critical 5G Interfaces

- Mahyoub, M., AbdulGhaffar, A., Alalade, E., Ndubisi, E. and Matrawy, A., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*
- This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and TELUS Communications through Collaborative Research and Development (CRD).


Security Analysis of Critical 5G Interfaces

Security Analysis of Critical 5G Interfaces

- Conduct a 5G security analysis from the perspective of the critical interfaces because of their importance.
- An in-depth analysis of the security measures recommended by 3GPP and other active SDOs on the critical 5G interfaces. Furthermore, our study covers the improved security measures proposed to improve the recommendations of 3GPP.
- Identify possible threats associated with each critical interface under study in the absence of security measures and categorizing these threats according to the STRIDE model and the type of traffic.

Security Analysis of Critical 5G Interfaces

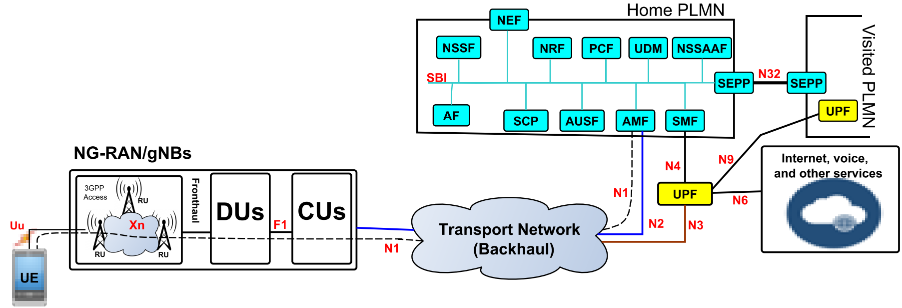


Figure: Service-based representation of 5G Architecture showing the studied interfaces and their endpoints. The lines with red legends represent the critical interfaces studied. The boxes with aqua and yellow represent the CP and UP network functions, respectively. Mahyoub et al., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*

Security Analysis of Critical 5G Interfaces

- For each organization we considered, we study their recommendations for these goals on each one of the interfaces. Fig. from Mahyoub et al., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*

Figure: 5G security goals considered for the analysis in this paper.

Security Analysis of Critical 5G Interfaces

- We follow these steps for each one of the interfaces, and we categorize the threats per gtraffic type. Fig. from Mahyoub et al., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*

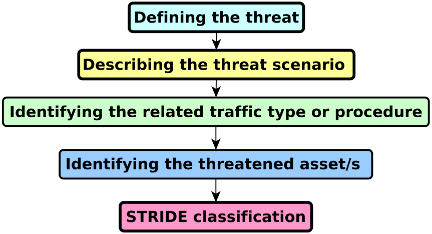


Figure: Threat analysis methodology

Security Analysis of Critical 5G Interfaces

Table: Security Recommendations for the N1 interface, from Mahyoub et al., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*

Security goal	**3GPP/ETSI**	**IETF**	**ITU**	**GSMA**
Confidentiality	NEA0, 128-NEA1, 128-NEA2 (mandatory), 128-NEA3 (optional)	—	128-NEA1, 128-NEA2, 128-NEA3 for encryption (Confidentiality protection)	128-NEA1, 128-NEA2 (mandatory), 128-NEA3 (optional)
Integrity	NIA0, 128-NIA1, 128-NIA2 (mandatory), 128-NIA3 (optional)	—	128-NIA1, 128-NIA2, 128-NIA3 for MAC (Integrity protection)	128-NIA1, 128-NIA2 (mandatory), 128-NIA3 (optional)
Authentication	EAP-TLS, EAP-AKA', 5G-AKA	EAP-AKA', EAP-TLS 1.3, EAP-TLS (with Raw Public Key), PEAA (5G-AKA enhancement)	—	5G-AKA (MILENAGE and TUAK), EAP-AKA , EAP-AKA', and EAP-TLS 1.3
Replay Protection	Only accept each NAS/PDCP COUNT value once, K_{SEAF} update	—	—	—
Privacy	Using SUCI and 5G-GUTI	—	—	ECIES profiles to conceal SUPI

Security Analysis of Critical 5G Interfaces

Table: Threats to the N1 Interface, from Mahyoub et al., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*

Interface	End Points	Traffic Type	Threat/Vulnerability	Threatened asset(s)	STRIDE Category					
					S	T	R	I	D	E
N1	UE $\leftrightarrow$ AMF	SMC procedure	A bidding down of UE capabilities	UE radio capabilities		•		•		
		Registration and authentication procedures	AMF impersonation	UE identity				•		
			Registration request flooding	System resources					•	
			Inaccurate SUCI de-concealment	System resources					•	
			NAS protocol-based attack	UE data				•	•	
			NAS null integrity protection	Processing capacity						•
			NAS integrity selection and utilization	System resources		•		•	•	
			Reuse 5G-GUTI	Mobility management data		•		•		
			IMSI catcher	UE identity				•		
			IMEI visibility	Device and user identity				•		
		UP and CP traffic	Incorrect implementation of UE security capacity handling	User accounts, data, and credentials		•		•		
		AMF authentication	Discharge of non-emergency bearer	System resources					•	
		AKA procedure	RES verification failure	Processing capacity					•	
			Re-synchronization	Processing resources					•	
			Initial registration, message integrity check failed	Processing resources					•	
		SMC procedure	A bidding down of Security features	UE data credential		•		•	•	
		NSSAA procedure	False NSSID	System resources						•
		AMF re-allocation procedure	Selection of NAS integrity protection algorithm based on AMF change	User data and credentials				•		
		Cell changing initial request	5G-GUTI and IMEI correlation	User location		•		•		
		Cell selection and reselection procedures	Logical gNB jamming	Service availability					•	
		All traffic types	Physical radio jamming	Service availability and system resources					•	

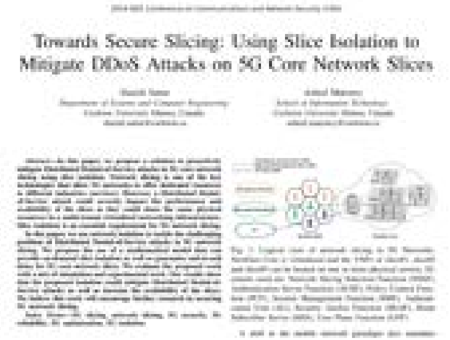
Security Analysis of Critical 5G Interfaces

Table: Mapping Assumptions to Threats, from Mahyoub et al., 2024. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials.*

Threat/Vulnerability	Interfaces	Assumption
Resynchronization failure	N1	Resynchronization of sequence numbers do not work correctly if the synchronization parameters AUTS (sent from the UE) and RAND (sent to the UE) are not involved when the synchronization fails [10], [58]
CP integrity protection	Xn	The integrity protection mechanism is not implemented by the gNBs for control plane packets [58], [62]
Key stream reuse	Xn	The gNB does not update AS while reusing the PDCP COUNT value for the same RB identity and K_{gNB} [58], [62]
Bidding down on Xn-handover	N2 and Xn	The AMF cannot confirm the security capabilities of the UE transmitted by the gNB [58], [62], [90]
Eavesdropping	F1	An attacker can eavesdrop on CP signaling or UP packets if the E2E security protection is not applied [77]
Weak protection for UP data	N3 and N9	The user's traffic can be altered by attackers if it is not integrity protected [58]
Fake PDU session establishment flood	N4	A malicious SMF under the control of the attacker floods the UPF to overwhelm the UPF resources resulting in a DoS for legitimate users [90]
JSON parser robustness issues	SBI	If the JSON keys (i.e. names) used are duplicated and not unique, it can lead to inconsistency in their values which would cause a DoS [58], [84]
IPX impersonation	N32	A malicious SEPP poses as an intermediary IPX provider and misuses the cryptographic resources of peer SEPPs can trick SEPP into accepting fake N32-f JSON patches [58]
Malformed GTP-U messages	N6	A Malicious attacker can transmit malformed GTP-U communications to the target UPF with IPUPS capabilities potentially causing a DoS attack [58]

Earlier Work: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices

- Sattar, D. and Matrawy, A., 2019, June. Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices. In *2019 IEEE Conference on Communications and Network Security (CNS)* (pp. 82-90). IEEE.


Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices

Earlier Work: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices

- Propose an optimization model to proactively mitigate DDoS attacks on 5G Network Slicing.
- Hardware-level resource isolation for inter-slice and intra-slice isolation.
- The model optimizes resource utilization and end-to-end delay.
- **In the next paper, we consider standard 5G VNFs, standard 5G procedures, new security constraints, and VNF-level isolation.**

Security-aware NF Sharing Model for 5G Slicing

- Mahyoub, M., AbdulGhaffar, A., Alalade, E. and Matrawy, A., 2023. A security-aware network function sharing model for 5g slicing. *arXiv preprint arXiv:2303.03492.*
- This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and TELUS Communications through Collaborative Research and Development (CRD).


A Security-aware Network Function Sharing Model for 5G Slicing

Contributions

- Propose a multi-objective MINLP model aiming at minimizing the processing capacity needed and procedures' latency of all requested slices.
- Provide a systematic way to decide on the sharing property of a particular VNF by introducing new security constraints that define the VNF's criticality.
- Consider the granularity at the procedure level instead of abstracting a slice as a unit.
- The proposed model is tested using standard procedures and VNFs of the 5G architecture that are described in 3rd Generation Partnership Project (3GPP) standards rather than using generic VNFs or symbolic procedures.

Model Overview

- The objective function

$$\min_{\gamma_{v_i,p}^{n,s}} \sum_{v\in\mathcal{V}} \sum_{i\in I_v} \sum_{n\in\mathcal{N}} \zeta_{v_i}^{n} + \sum_{s\in\mathcal{S}} \sum_{p\in\mathcal{P}_s} \delta_p^s \qquad (1)$$

The total required computational capacity for all VNFs

The total delay of all procedures

Model Overview

- The total VNF's required computational capacity

The traffic capacity

$$\zeta_{v_i}^{n} = \zeta_{v_i}^{n,B} \cdot \beta_{v_i}^{n} + \zeta_{v_i}^{n,T} \qquad \forall v \in \mathcal{V}, \quad i \in I_v, \; n \in \mathcal{N} \qquad (2)$$

The base capacity

Is the vnf instance v_i activated?

$$\zeta_{v_i}^{n,T} = \sum_{s \in \mathcal{S}} \sum_{p \in \mathcal{P}_s} \lambda_p^s \, \gamma_{v_i,p}^{n,s} \, \mu_v \qquad \forall v \in \mathcal{V}, \quad i \in I_v, \; n \in \mathcal{N} \qquad (3)$$

The capacity needed for one traffic unit

The procedure's packet rate

Model Overview

- The procedure delay computation

The link (n,m) delay

$$\delta_p^s = \sum_{v \in \mathcal{V}_p^s} \sum_{i \in I_v} \sum_{n \in \mathcal{N}} \delta_{v_i}^n \; \gamma_{v_i,p}^{n,s} \; + \sum_{(v_i,z_j) \in \mathcal{R}_p^s} \sum_{(n,m) \in \mathcal{L}} d(n,m) \; \chi_{(v_i,z_j),p}^{(n,m),s} \qquad \forall s \in \mathcal{S}, p \in \mathcal{P}_s \tag{4}$$

The VNF-instance's delay

$$\delta_{v_i}^n = 1/\omega_v \; + \; 1/(\omega_v - \sum_{s \in \mathcal{S}} \sum_{p \in \mathcal{P}_s} \lambda_p^s \; \gamma_{v_i,p}^{n,s}) \qquad \forall s \in \mathcal{S}, p \in \mathcal{P}_s \tag{5}$$

Processed data per unit time

Model Constraints: Security constraints

- **Maximum Traffic Constraint:** Constraint (6) is the VNF's maximum traffic constraint

$$\zeta_{v_i}^{n,T} \leq \zeta_{v}^{T,max}, \qquad \forall v \in \mathcal{V}, \quad i \in I_v, \; n \in \mathcal{N} \tag{6}$$

Model Constraints: Security constraints

- **Exposure Constraint:**
  Constraints (7), (8) and (9) ensure that any VNF instance that is exposed to external procedures will not be shared

Is the procedure p sourced externally?

$$\sum_{p \in \mathcal{P}_s} \eta^s_{p,v} \, \psi^s_p \, \gamma^{n,s}_{v_i,p} \leq \mathcal{C} \, \Omega^{n,s}_{v_i} \quad \forall s \in \mathcal{S}, v \in \mathcal{V}, \; i \in I_v, \; n \in \mathcal{N} \tag{7}$$

Is the VNF v the first hit on the VNFs sequence of the procedure?

$$\Omega^{n,s}_{v_i} - \sum_{p \in \mathcal{P}_s} \eta^s_{p,v} \, \psi^s_p \, \gamma^{n,s}_{v_i,p} \leq 0 \quad \forall s \in \mathcal{S}, v \in \mathcal{V}, \; i \in I_v, \; n \in \mathcal{N} \tag{8}$$

$$\sum_{s \in \mathcal{S}} \Omega^{n,s}_{v_i} \leq 1 \quad \forall v \in \mathcal{V}, \; i \in I_v \; n \in \mathcal{N} \tag{9}$$

Indicating whether v_i is exposed externally

Where $\mathcal{C}$ is a parameter greater than the maximum number of procedures mapped into the v_i and sourced externally.

System Setup

Table: Implemented Scenario

Number of slices	Two
Procedures for Slice# 1	1) Registration with AMF re-allocation procedure 2) Handover procedure 3) Authentication procedure
Procedures for Slice# 2	1) General registration procedure 2) Handover procedure 3) Authentication procedure
Number of external procedures	Variable
Maximum VNF traffic capacity	Variable

Table: Parameters used in the Model

Parameter	**Value**
Number of physical nodes	3
Maximum capacity of nodes	30 capacity units
Network connectivity	Mesh topology
Physical link delay	5ms
Physical link maximum bandwidth	40 bandwidth units
Number of VNFs	14
Maximum capacity of VNF instance	10 capacity units
VNFs base capacity	1 capacity unit
Maximum VNF traffic allowed	2 (variable in some experiments)
VNFs delay unit	Random between 1000 and 2000 packets/sec
Number of instances per VNF	4
Number of Procedures	4
Allowed delay for procedure	1 second
Number of slices	2

From Mahyoub et al. A security-aware network function sharing model for 5g slicing. *arXiv preprint arXiv:2303.03492.*

Impact of the Exposure Constraint

- In this experiment, the VNF's maximum traffic constraint is disabled
- If the first VNF of an external procedure is shared with other procedures, then the other procedures would be exposed to external threats as well.
- Figure (a) shows the security goals achieved by using the security constraint, while figure (b) shows the cost of including security.

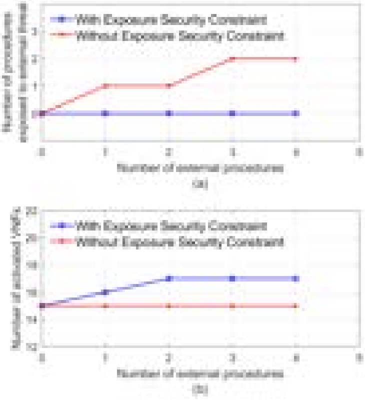


Figure: Impact of exposure constraint.

From Mahyoub et al. A security-aware network function sharing model for 5g slicing. *arXiv preprint arXiv:2303.03492.*

Impact of the Maximum VNF Traffic Constraint

- The exposure security constraint is disabled; only one procedure is assumed to be externally sourced
- The figures show the benefit and cost of using the security constraint.

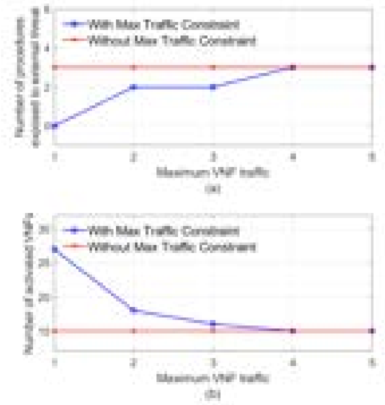


Figure: Impact of maximum VNF traffic constraint. From Mahyoub et al. A security-aware network function sharing model for 5g slicing. *arXiv preprint*

Main Benefits

- Using the maximum VNF traffic constraint, the maximum allowed traffic for a critical VNF instance can be set at a lower value, and hence it will not be shared with other traffic, which will protect the critical VNF.
- The exposure constraint will ensure that the VNF that is exposed to the outside network cannot be assigned to more than one slice.
- The use of security constraints will ensure the protection of critical network infrastructure from external threats such as DDoS attacks

Impact of Flooding Attacks on 5G Slicing

- AbdulGhaffar, A., Mahyoub, M. and Matrawy, A., 2024, May. On the Impact of Flooding Attacks on 5G Slicing with Different VNF Sharing Configurations. In *2024 20th International Conference on the Design of Reliable Communication Networks (DRCN)* (pp. 136-142). IEEE.
- This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and TELUS Communications through Collaborative Research and Development (CRD).

Impact of Flooding Attacks on 5G Slicing - Contributions

- Evaluate the performance of the proposed VNF sharing network configurations during flood attacks on each of the data and control planes in a 5G testbed environment.
- Compare the performance of both network configurations with multiple UE applications, including iPerf downlink data transfer, ping RTT, and UE procedures delay, under flood attack traffic.
- Consider two flood attack scenarios, one to flood the data plane network using a ping flood attack, and the second to exhaust the resources of the control plane VNFs in the core network with a registration request flood attack.

The following configuration digrams and associated results are from AbdulGhaffar et al. (2024) On the Impact of Flooding Attacks on 5G Slicing with Different VNF Sharing Configurations. In *20th International Conference on the Design of Reliable Communication Networks (DRCN)* (pp. 136-142). IEEE.

Impact of Flooding Attacks on 5G Slicing

- Testbed Setup:
  - Physical server: 32 cores of Intel Xeon Processor and 24 GB of RAM
  - 5G core network: Free5GC
  - Radio Access Network (RAN): UERANSIM
  - Deployed two network slices
  - Slice 1: UE 1 and UE 3
  - Slice 2: UE 2

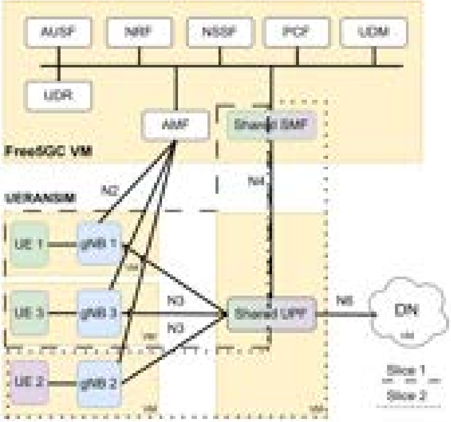


Figure: Testbed Setup

Impact of Flooding Attacks on 5G Slicing

- Network Configuration #1 (C1)
  - SMF and UPF VNFs are shared between the two slices

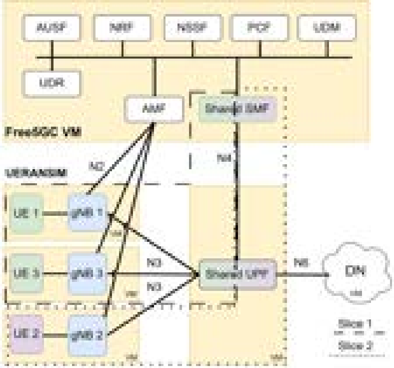


Figure: Network configuration C1 with shared SMF and UPF

- Network Configuration #2 (C2)
  - SMF and UPF VNFs are isolated for the two slices

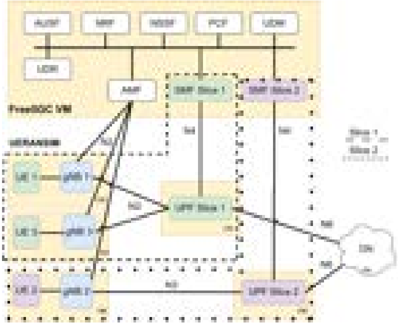


Figure: Network configuration C2 with isolated SMF and UPF

Impact of Flooding Attacks on 5G Slicing

- Threat Model
  - Assumptions:
    1. The operator's 5G network supports multiple network slices.
    2. The UEs, including the attacking UEs, are legitimate users of the 5G network.
    3. It is not possible for the attacker to modify the hardware configurations of the bare-metal systems.
    4. The attackers can generate a high volume of traffic that can exhaust the resources of the operator's 5G VNFs.
  - Adversaries:
    1. We consider the attacker as a legitimate user of the network slice.
    2. The attackers will generate large traffic to impact the performance of the legitimate UEs in other slices that share the same VNFs as the attacker's slice.

Impact of Flooding Attacks on 5G Slicing

- Attack Scenario:
  - Data plane flood attack:
    - Attacking UEs initiates a ping flood attack
- Evaluation Methodology:
  1. Downlink data transfer rate during data plane flood attack
  2. Round-trip time (RTT) during data plane flood attack

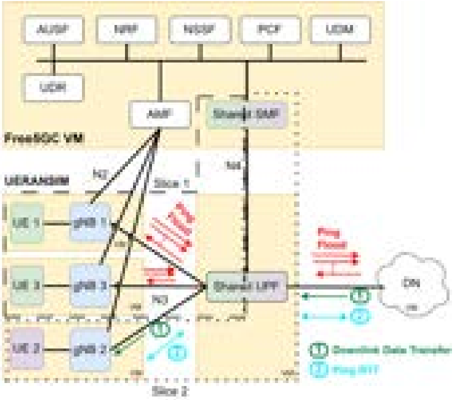


Figure: Data plane (ping) flood attack (shown in red arrows)

Impact of Flooding Attacks on 5G Slicing

- Attack Scenario:
  - Control plane flood attack:
    - Attacking UEs perform registration request flood attack targeting the control plane VNFs
- Evaluation Methodology:
  1. Procedures delay during control plane flood attack

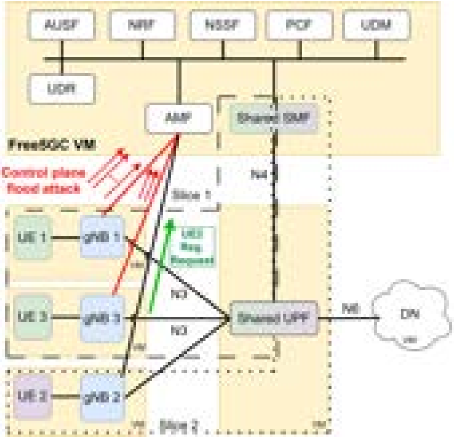


Figure: Control plane flood attack (shown in red arrows)

Impact of Flooding Attacks on 5G Slicing

- Results
  - Downlink data transfer rate during data plane flood attack:
    - The data transfer rate of UE 2 in C1 drops significantly from 100 Mbps to around 2 Mbps when the attack starts at 10 seconds (red dotted line)

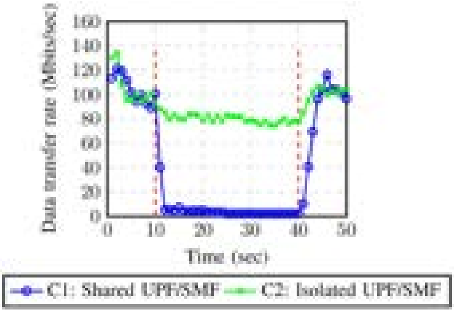


Figure: Average downlink data transfer rate for UE 2 within slice 2 during data plane flood attack

Impact of Flooding Attacks on 5G Slicing

- Results
  - Downlink data transfer rate during data plane flood attack:
    - The average data downloaded by UE 2 in the C1 configuration is 242.4 Megabytes (MB), compared to 532.8 MB for C2 configuration
    - The confidence interval does not overlap, there is a statistically significant difference between the performance of the C1 and C2

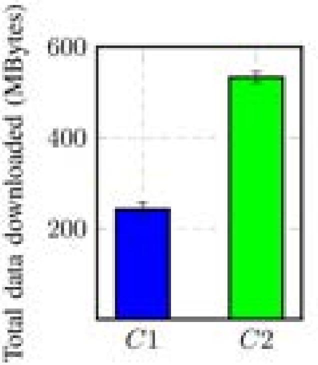


Figure: Average total data downloaded from DN to UE 2 during data plane flood attack

Impact of Flooding Attacks on 5G Slicing

- Results
  - Round-trip time (RTT) during data plane flood attack:
    - Before the attack, the RTT for both configurations (C1 and C2) is approximately around 15 ms
    - With the attack traffic, the RTT for configuration C1 increases significantly
    - The benefit of having isolated VNFs is prominent for configuration C2, as the flooding attack does not affect the RTT in this case

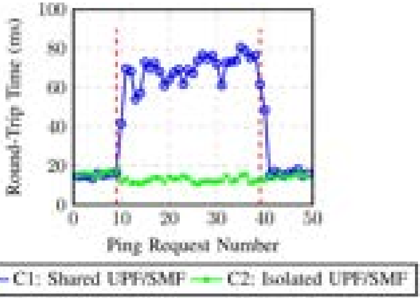


Figure: Round-Trip Time (RTT) of pings initiated by UE 2 within slice 2 during data plane flood attack

Impact of Flooding Attacks on 5G Slicing

- Results
  - Procedures delay during control plane flood attack:
    - The attack traffic is present throughout the entire experiment
    - The intervals for both configurations overlap, indicating that the difference between C1 and C2 is statistically insignificant
    - The impact of a control plane flood attack on the results remains relatively indistinguishable

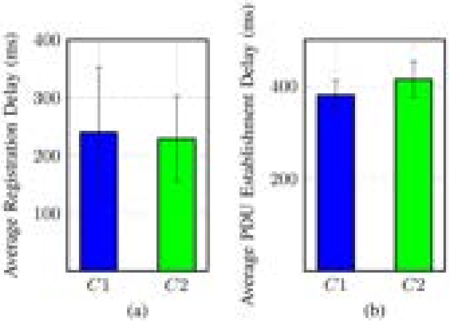


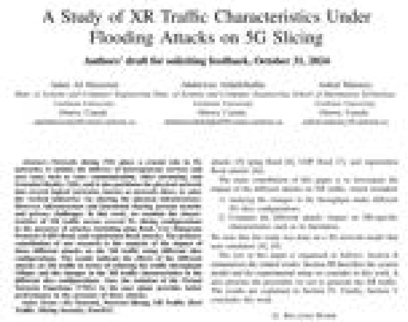
Figure: Average (a) Registration, (b) PDU Establishment Delay for UE 2 during control plane flood attack

Main Benefits

- Isolating the resources of the slices mitigates the impact of attacks launched from a different slice.
- The results clearly demonstrate the advantages of isolating VNFs among different slices, as the impact of attacks on the UE downlink data rate and the RTT is significantly diminished compared to configurations with shared VNFs.

A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

- Husseinat, A.A., AbdulGhaffar, A. and Matrawy, A., 2024. A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing. *Authorea Preprints*.


A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

Authors' draft for soliciting feedback, October 31, 2024

A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

- The main contribution of this paper is to investigate the impact of the different attacks on XR traffic, which included:
- Studying the changes in the throughput under different 5G slice configurations.
- Compare the impact of the different attacks on XR-specific characteristics such as its burstiness.

A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

- Husseinat, A.A., AbdulGhaffar, A. and Matrawy, A., 2024. A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing. *Authorea Preprints*.

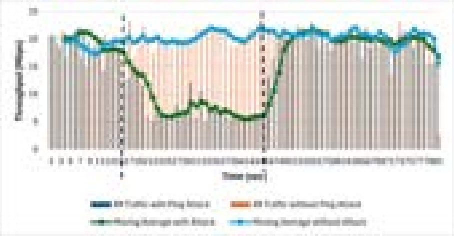


Figure: Shared UPF and Dedicated SMF with Ping Attack

A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

- Husseinat, A.A., AbdulGhaffar, A. and Matrawy, A., 2024. A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing. *Authorea Preprints*.

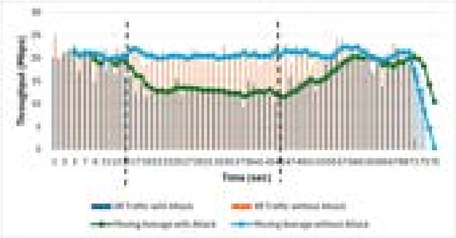


Figure: Dedicated UPF and Dedicated SMF with Ping Attack

A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing

- Husseinat, A.A., AbdulGhaffar, A. and Matrawy, A., 2024. A Study of XR Traffic Characteristics Under Flooding Attacks on 5G Slicing. *Authorea Preprints*.
- **An interesting result**

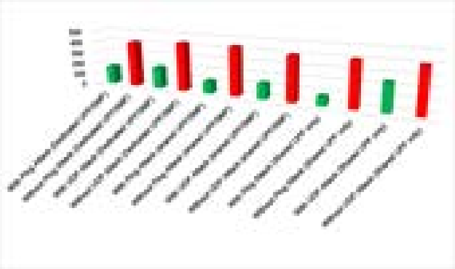


Figure: XR Traffic Variance