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

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





- 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).







- 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.





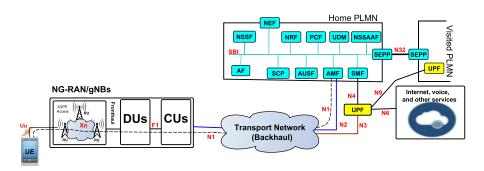


Figure: Service-based representation of 5G Architecture showing the studied interfaces and their endpoints. The lines with red legends represent the critical interfaces studied. The boxes with aqua and yellow represent the CP and UP network functions, respectively. Mahyoub et al., 2024. Security analysis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

 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.

 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.

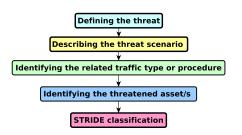


Figure: Threat analysis methodology





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 Pro- tection	Only accept each NAS/PDCP COUNT value once, K _{SEAF} update	_	_	_
Privacy	Using SUCI and 5G-GUTI	_	_	ECIES profiles to conceal SUPI

5G Slice Isolation Through Resource Allocati

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 Valuerability	Threatened assets:	STRIBE Category				
	5				TI	RIL	D	1.0	
NI UE ++ AME		SMC procedure	A bubling down of UE capabilities AMF improvements	UE radio capabilities UE identity		•			Г
			Registration request flooding	Nestern resources	\vdash		-1-		\vdash
	Registrative and atalientication	Inacounter SUCI de concestrant	Nestron munureau UK data				:	Ε	
		NAS potential based attack NAS tall integrity protection	Processing capacity	\vdash	-				
		boxingate	NAS integrity selection and utilization	Nystern researces		•			E
	17 110		Bress SG-GUTI IMSI carcher	Mobility management data UE identity	=	٠	-:		F
		IMEI visibility	Device and may identity	\vdash				+	
	UP and CP multic	Decreed implementation of CE security capacity handling	Unit accounts, data, and-crofemials		٠			Г	
		AMF authoritistics	Discharge of non-emergency beaser	System revolutes					E
		AND consistent	RES verification failure Re-conclusions	Processing capacity	\Box	_	_	:	₽
		AKA president	Initial regulation, message integrity, affect failed	Processing resources	Н		+	•	t
		SMC procedure	A hidding down of Society framers	UE data coolential		•			
		NSSAA procedure	False NSID	Nysiam menana					
	AMF re-allocation procedure	Solution of NAS imaginy proaction algorithm based on AMF change	User data and cookentals						
		Cell abouging initial require	5G-GUTI and IMEE combation	User location.		•	•		Г
		Cell selection and resolution procedures	Logical gNB jamming	Service availability					
		All traffic types	Physical ratio juneing	Service availability and system movements				٠	Γ

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

Threat/Vulnerability	Interfaces	Assemption		
Resynchemization failure	NI	Resynchronization of sequence numbers do not work correctly if the synchronization parameters AUTS (seen from the UE) and RAND (sent to the UE) are not involved when the synchronization (tab. 1010, 25%)		
CP integrity protection	Xa	The integrity protection mechanism is not implemented by the gNBs for control plane packets [58], [62]		
Key stream news	Xe	The gNB does not update AS while reusing the PDCP COUNT value for the same RB identity and K _{aNB} [58], [62]		
Bidding down on Xn-handover	N2 and Xn	The AMF cannot confirm the security capabilities of the UE transmitted by the gNB [50], [62], [90]		
Eurestropping	FI	An attacker can cave-drop on CP signaling or UP packets if the E2E security protection in nor applied [77]		
Weak protection for UP data	N3 and N9	The over's traffic can be altered by attackers if it is not integrity protected [58]		
Fake PDU session establishment flood	84	A multicious SMF under the control of the attacker fisade the UFF to overwhelm the UFF resources resulting in a DoS for legitimate users [80]		
JSON purser robustness issues	588	If the JSON keys (i.e. trames) used are duplicated and not unique, it can lead to inconsistency in their values which would cause a DoS [38], [84]		
BX impersuation	N32	A multirus SEPP poses as an intermediary IPX provider and minuses the cryptographic resources of peer SEPPs can trick SEPP into accepting false N32-f ISON patches [58]		
Mulformed GTP-U messages	N6	A Mulicious attacker can transmit multiremed GTP-U communications to the target UPF with IPCPS capabilities potentially causing a DeS attack [58]		

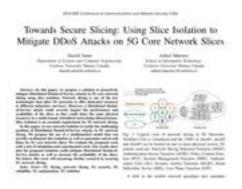
5G Slice Isolation Through Resource Allocati





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.



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.

below? that for infelling biologic, March 6, 2007 mer Britisch, Britisch, Mathematiker, Bereiger, Mathematik und Arbeit Mathemati blind of biometra Televisy; Epitre Forests, Finals. and of Ericon and Company Supramore Challeng Advances I below to Company

at the ball of the second ball of the second of the second at the second make different ability of the framework of the a property many in people in come tegenments are after th district in the special proper contribution TW during made in 10 account. To proposed autisms. to set lette in area systematical studio, the chance the storm to beauty tipe other tree, and THE R. LEWIS CO., LANSING, MICH. S. ROOM. particle TW back is no young of common for the In casing Section . The solid group is the solid room persons for the property is the most, the persons a side districts to accomply to APE partition passes. Fig. 198. his dening profess to homeland to dilow to photological marking that white the experiments of the impacts in the calculate. The probability has been been been all the part of the OR PLANT INTO RELIGION OF THE STUDY CO. the course were the branching and present applicating the process. me step old to second performant it man if

Thereto an incident a second more second 5G the photol column is the arminosis or the formula follow. White the big and another the second properties of the last amondo, 100 mateiro M. santane in diales, mattain button photosis no beauti alcolo di reconsir y ratio talle, casaluni and different amount of the figure after an analysis of

particular for finance for formatter of the procedure constrainty for etc.). Although ches forcages feeder codulated the feeder separts of 1981 to the coupling process, they adjust to Anish to the property and so if you in the most Figure and there is \$6 her pay to reducing a reducent way. to allow relation a particular PMF is selected uses if No. 4 cost theirsy I storage little. In the proposal section land and made common by territory a date by \$100 provides. The two colonians is the becomes made, that us in proceed in a patients VML Ex. VM for it process degra feet and named wides, it has blooming a beditten trial makes a lateral and their dealings for these forces. All the second day a capacity is also dear account to attended made the past before it woman in \$1.000. in respect to provide a compared to the second compared to represed TVM to compressive I. Not care regard till rather office. had show it. As the case preceding printing to calledge PARS. a new contract of the contract colonia, in larger of the process Declarate the constitution of the part on the SEC

a Praymag a cost obstacle. West image Suitane Str. processor fulfill? proof plotte is employed to processing regional survival and particulation agreed in a Revolta i schedati, van di tariali sii de steta property of course the 150 to accomply on school contraction felt at the At The Toller, and coma Committing for provided their provincial distinct of effectively color to a set. To be less of section beautique





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

$$\min_{\gamma_{v_i,p}^{n,s}} \sum_{v \in \mathcal{V}} \sum_{i \in I_v} \sum_{n \in \mathcal{N}} \zeta_{v_i}^n + \sum_{s \in \mathcal{S}} \sum_{p \in \mathcal{P}_s} \delta_p^s \tag{1}$$
The total required computational of all procedures

capacity for all VNFs



Model Overview

The total VNF's required computational capacity

$$\zeta_{v_i}^n = \zeta_{v_i}^{n,B}. \ \beta_{v_i}^n + \zeta_{v_i}^{n,T} \quad \forall v \in \mathcal{V}, \quad i \in I_v, \ n \in \mathcal{N}$$
 The base capacity \(\begin{align*} \text{1s the vnf instance } v_i \text{ activated?} \end{align*}

$$\zeta_{v_i}^{n,T} = \sum_{s \in \mathcal{S}} \sum_{p \in \mathcal{P}_s} \lambda_p^s \gamma_{v_i,p}^{n,s} \mu_v \quad \forall v \in \mathcal{V}, \quad i \in I_v, \ n \in \mathcal{N}$$
 (3) The capacity needed for one traffic unit

The procedure's packet rate



Model Overview

The procedure delay computation

The procedure delay computation
$$\delta_{p}^{s} = \sum_{v \in \mathcal{V}_{p}^{s}} \sum_{i \in I_{v}} \sum_{n \in \mathcal{N}} \delta_{v_{i}}^{n} \gamma_{v_{i,p}}^{n,s} + \sum_{(v_{i},z_{j}) \in \mathcal{R}_{p}^{s}(n,m) \in \mathcal{L}} \sum_{d(n,m)} \chi_{(v_{i},z_{j}),p}^{(n,m),s}$$

$$\text{The VNF-instance's delay} \forall s \in \mathcal{S}, p \in \mathcal{P}_{s}$$

$$\delta_{\nu_i}^n = 1/\omega_{\nu} + 1/(\omega_{\nu} - \sum_{s \in \mathcal{S}} \sum_{p \in \mathcal{P}_s} \lambda_p^s \gamma_{\nu_i, p}^{n, s}) \quad \forall s \in \mathcal{S}, p \in \mathcal{P}_s \quad (5)$$

Processed data per unit time





Model Constraints: Security constraints

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

$$\zeta_{v_i}^{n,T} \leq \zeta_v^{T,max}, \quad \forall v \in \mathcal{V}, \quad i \in I_v, \quad n \in \mathcal{N}$$
(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?

$$\sum_{p \in \mathcal{P}} \eta_{p,v}^{s} \psi_{p}^{v} \gamma_{v_{i},p}^{n,s} \leq \mathcal{C} \Omega_{v_{i}}^{n,s} \quad \forall s \in \mathcal{S}, v \in \mathcal{V}, \ i \in I_{v}, \ n \in \mathcal{N}$$
 (7)

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

$$\Omega_{\nu_{i}}^{n,s} - \sum_{p \in \mathcal{P}_{s}} \eta_{p,\nu}^{s} \ \psi_{p}^{s} \ \gamma_{\nu_{i},p}^{n,s} \leq 0 \ \forall s \in \mathcal{S}, \nu \in \mathcal{V}, \ i \in I_{\nu}, \ n \in \mathcal{N}$$
 (8)

$$\sum_{s \in \mathcal{S}} \Omega_{v_i}^{n,s} \le 1 \qquad \forall v \in \mathcal{V}, \ i \in I_v \ n \in \mathcal{N}$$

$$\uparrow \text{ Indicating whether } v_i \text{ is exposed externally}$$
(9)

Where 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.

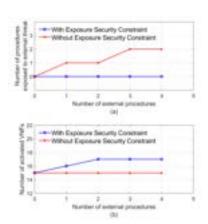


Figure: Impact of exposure constraint.

model for 5g slicing. arXiv preprint arXiv:2303.03492.

From Mahyoub et al. A security-aware network function sharing

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.

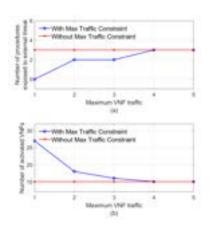


Figure: Impact of maximum VNF traffic constraint. From Mahyoub et al. A security-aware network function sharing model for 5g slicing.arXiv preprint.

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





- 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).



4 D > 4 A > 4 B > 4 B >

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.

Testbed Setup:

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

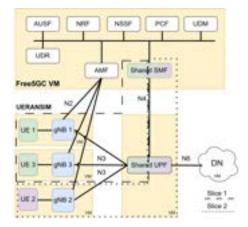


Figure: Testbed Setup



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

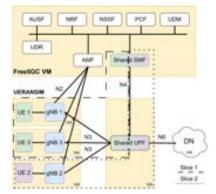


Figure: Network configuration C1 with shared SMF and UPF

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

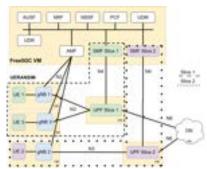


Figure: Network configuration C2 with isolated SMF and UPF

Threat Model

- Assumptions:
 - The operator's 5G network supports multiple network slices.
 - The UEs, including the attacking UEs, are legitimate users of the 5G network.
 - It is not possible for the attacker to modify the hardware configurations of the bare-metal systems.
 - The attackers can generate a high volume of traffic that can exhaust the resources of the operator's 5G VNFs.
- Adversaries:
 - We consider the attacker as a legitimate user of the network slice.
 - 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.





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

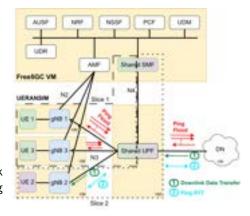


Figure: Data plane (ping) flood attack (shown in red arrows)

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

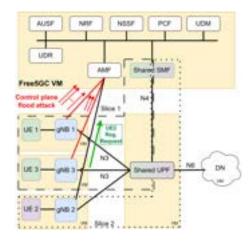


Figure: Control plane flood attack (shown in red arrows)



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)

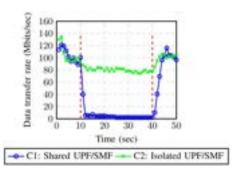


Figure: Average downlink data transfer rate for UE 2 within slice 2 during data plane flood attack





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

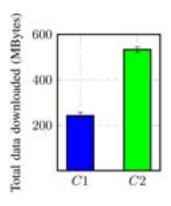


Figure: Average total data downloaded from DN to UE 2 during data plane flood attack

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

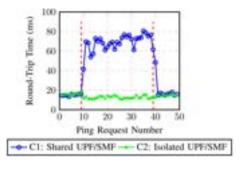


Figure: Round-Trip Time (RTT) of pings initiated by UE 2 within slice 2 during data plane flood attack





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

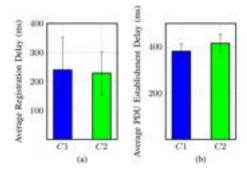


Figure: Average (a) Registration, (b) PDU Establishment Delay for UE 2 during control plane flood attack

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.





 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

hadour' draft for soliciting feedback, Orniber 31, 3004

Sales Mines than at history and history displacement than at history and impact than to Ji Revenuese Serimona Davis Card Stewart Laborator Home, French

Steam Street, Brook Str., And A Justice Sales St. um, n print, m select of borrograms come call more hadred substates facilities at streeted, Misc. II who to the account of advanta, horizona also, frost, "the Pleasane. on Albert shall in the 10 table was fillered the ARREST TO LOSS SERVE SE JOSE SE SE SERVE min Planting, 1795; In the and allied minter, below Printers & Revenue of the printer

Analy 17 less than 16, 16# had 17; 46 seconds And obside the The main committee of this paper is to investigate the

make of the efficient spices; or "M collections are properly It looking the range in its throughput make different Si do relación I friend to three dark hard in Minaria

rhistoriani act a 't besteri. to less the low real training of the description has

with reductions (IC), EV, No. bet or No. Japan of respond to Advent Seaton & communicate the committee beauty flactors MI beautiful tip, solvers medit and the commissional edge on combine in the well, it also provides the provided for some to provide the MI hould

the could be continued to become its fraction because it S. Annual Street





- 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.





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

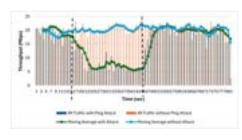


Figure: Shared UPF and Dedicated SMF with Ping Attack





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

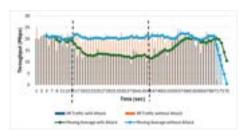


Figure: Dedicated UPF and Dedicated SMF with Ping Attack





- 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

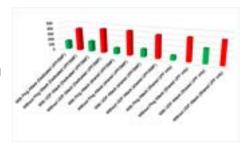


Figure: XR Traffic Variance



