Slicing Under Siege: Adversarial-Aware Optimization for Secure Resource Allocation in B5G Networks

1st Sameer Ali
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya (UOC)
CYBERCAT, Barcelona, Spain
sameer43786@uoc.edu

2nd Helena Rifà-Pous
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya (UOC)
CYBERCAT, Barcelona, Spain
hrifa@uoc.edu

***Abstract*—The prospect of ultra-dynamic and tailored network slicing in the era of Beyond 5G (B5G) is associated with the potential to make networks more vulnerable to stealthy adversarial actions. Attackers may impersonate authorised end users, saturate virtual slices, or take advantage of resource gaps at the expense of service availability, quality and user trust. This study presents a novel approach, Secure Intelligent Enforcement of Guaranteed Efficiency (SIEGE), which is a strategic defence of scarce resources that are under siege by optimising resource allocation with adversarial awareness in the core of the defence. SIEGE is created through the use of an Integer Linear Programming (ILP) and is capable of identifying and blocking malicious usage by users without impacting the performance of benign users. The model proposes per-user behavioural metrics (p_u, q_u), which measure slice/resource exposure, and applies them in an optimisation target that is resilience-aware. Early indicators suggest a maximum of 43.7% reduction in resource hijacking cases, while service-level agreements remain intact. The research is continuing to provide the foundation to a next-generation secure slicing paradigm, which is proactive, explainable and scalable. SIEGE provides a roadmap of security-by-design wireless infrastructure and a bridge to self-protecting, smart B5G networks.**

***Index Terms*—B5G, network slicing, resource hijacking, adversarial load, optimization, secure resource allocation, resilient wireless networks**

I. Introduction

In B5G, network slicing lets separate logical networks function together on the same physical infrastructure [1]. This approach enables flexibility and application-specific Quality of Service (QoS), but it also creates an unexplored vulnerability [2] and allows adversary resource hijacking attacks that take use of the very elasticity that slicing offers [3]. In this threat model, a malicious actor could ask for more than one slice or overclaim resources to exhaust the system, which would make services worse for other users. As slice orchestration gets more decentralized and driven by artificial intelligence (AI) [4], the possibility of strategic exploitation goes up [5].

Existing resource allocation frameworks, although efficient and performance-driven, are largely agnostic to malicious behaviors and assume trustworthiness of service requests [6][7][8]. This gap motivates a security-centric reformulation of the slicing problem, one that integrates adversarial awareness into the core of optimization. The traditional performance-only objective fails to capture the nuanced threat landscape of B5G networks, where attackers may mimic benign patterns or launch stealthy saturation attempts.

This research proposes a paradigm shift; optimizing slicing not just for efficiency, but for resilience under siege. To that end, we introduce SIEGE an ILP-based framework that integrates behavioral indicators into resource allocation. By doing so, the model proactively detects suspicious access patterns and applies constraints to mitigate adversarial impact while preserving service guarantees for legitimate users. The broader goal is to develop a scalable, explainable, and adaptable resource allocation scheme that aligns with the security-by-design principles of next-generation wireless infrastructures.

We address the challenge of ensuring safe, strategic, and optimal resource allocation when faced with users who are trying to overwhelm network resources. We explore methods to enhance slice-resource-user mappings, enabling them to continue serving legitimate users while preventing suspicious behaviour. We investigate how optimization variables can be expanded to include adversarial indicators, enabling the solution to act as both an allocator and a defender. This research addresses a significant gap in standard optimisation processes, which lack built-in mechanisms to prevent slice misuse which is a crucial aspect of B5G security.

II. Related Work

Network slicing has become an essential part of the architecture due to the growing need to support flexible, application-specific QoS in B5G networks. Recent investigations, such as those by Dudin et al. [10] and Wang et al. [11], have suggested sophisticated resource allocation and slicing schemes

This work was supported by the Spanish Ministry of Science and Innovation through the PID2021-125962OB-C31 "SECURING" project. Additional funding was provided by the ARTEMISA International Chair of Cybersecurity (C057/23) and the DANGER Strategic Project of Cybersecurity (C062/23), both funded by the Spanish National Institute of Cybersecurity through the European Union NextGenerationEU and the Recovery, Transformation, and Resilience Plan.

978-3-903176-75-1 ©2025 IFIP

for 5G/6G. Nevertheless, they are efficiency-oriented and provisioning-oriented and usually neglect to monitor adversarial behaviours [12]. Govindarajan et al. [13] provided closed-loop optimisation frameworks on slice orchestration, but they never considered threat detection or mitigation in the optimisation loop.

Security contributions, such as those by Wang & Liu [14] and Ludant, & Noubir [15], list the weaknesses of slicing to resource hijacking and stealthy exploits but do not go further to provide optimisation-based defences. Additionally, Tariq et al. [2] focus on threat modelling in B5G networks but fail to convert these models into constraint enforceability in slicing mechanisms.

To fill this gap, a SIEGE user-to-user-conscious approach is added as an integer proportional variable to the optimisation formulation, incorporating data on the placement of behavioural patterns in terms of slice and resource gain. Such an approach is proactive protection, which is scalable and not a heuristic or fixed-rule platform, and is in line with the dynamism and AI-driven nature of B5G. To offer security-by-design against counter-adversarial loads, the model is a distributor and a defender. Specifically, SIEGE is an adversary-aware ILP model that assumes the addition of a binary decision variable $x_{u,s,r}$, representing the user u accessing a resource r at slice s, and integer decision variables, representing the number of slices and resources accessed by the user, respectively, namely, p_u and q_u. The model is constrained by slicing capacity/quality of service, abnormal access patterns, as reported by high p_u and q_u, and ensures good service quality under load. It has an objective function, which is to maximise legitimate throughput and reduce adversarial impact by regularising behavioural metrics.

III. Model Formulation: SIEGE

a) Sets: In the context of secure resource allocation under adversarial conditions, the SIEGE model employs three fundamental sets to structure the optimization process. The set $\mathcal{U}$ represents all users in the network, each indexed by u, and includes both legitimate and potentially suspicious users. The set $\mathcal{S}$ denotes the collection of network slices, each indexed by s, corresponding to virtualized service instances tailored for different QoS or application requirements. Finally, the set $\mathcal{R}$ encompasses the available physical or virtual resources in the network, indexed by r, such as bandwidth units, CPU cycles, or memory blocks. These sets collectively define the multi-dimensional allocation space where the model determines which users receive which resources across which slices. By organizing the problem using these well-defined sets, the model ensures clear mapping and control over resource distribution while enabling fine-grained behavioral analysis and adversarial detection.

b) Parameters: The SIEGE model uses a set of intuitive parameters to guide and constrain the resource allocation process. The parameter $d_{u,s}$ defines the resource demand of user u on slice s, representing how much capacity the user requires for that specific service. C_r captures the capacity of resource r, ensuring that the model respects the limits of the infrastructure. Each user-slice pair also has a minimum QoS requirement, denoted by $Q_{u,s}^{\min}$, which ensures that the allocation is not only efficient but also meets user expectations. To model adversarial behavior, the parameter $\sigma_u \in \{0, 1\}$ flags whether a user is suspicious ($\sigma_u = 1$) or benign ($\sigma_u = 0$). The coefficients α and β are used to penalize suspicious behavior specifically, the number of slices and resources accessed by flagged users, respectively whereas γ rewards legitimate users for meeting their QoS. Finally, $w_{u,s}$ acts as a weighting factor to adjust the relative importance of each user-slice QoS contribution in the objective function, allowing for fairness or priority differentiation across users. Table 1 defines the core parameters of the proposed adversarial-aware resource allocation model, including user demands, resource capacities, QoS thresholds, and adversarial penalties. These parameters serve as inputs to drive the optimization of secure and resilient slice-resource assignments in B5G networks.

TABLE I
Model Parameters

Symbol	Description
$d_{u,s}$	Resource demand by user u on slice s
C_r	Capacity of resource r
$Q_{u,s}^{\min}$	Minimum required QoS for user u on slice s
$\sigma_u \in \{0, 1\}$	Suspicious flag for user u: 1 if suspicious, 0 otherwise
$\alpha \geq 0$	Penalty for number of slices accessed (suspicious)
$\beta \geq 0$	Penalty for number of resources accessed (suspicious)
$\gamma \geq 0$	Reward for QoS satisfaction
$w_{u,s} \geq 0$	QoS weight (default: 1)

c) Decision Variables: The model presents a set of decision variables to maximise and implement the use of secure resources. The key variable, $x_{u,s,r} \in \{0, 1\}$, is used to decide whether or not user u is allocated resource r on slice s. In line with this, the binary variable, which is a binary indicator, $y_{u,s} \in \{0, 1\}$, is used to indicate that the user is active on a given slice, and $z_{u,r} \in \{0, 1\}$ is used to indicate that the user is using a given resource, independent of the slice. Such indicators contribute to the measurement of the behavioural footprint of a user in the system. The integer variables, which are pu and qu, subsequently sum the number of slices and resources accessed by user u, respectively, key measures of determining adversarial behaviour. Lastly, the continuous variable $\text{QoS}_{u,s}$, concerning the system's reliability, is the actual level of QoS attained by users u on slice s a performance measure that the optimiser will maximise, subject to security-conscious penalties. These variables in the SIEGE model are summarized in Table 2 in which, the binary decision variables are used to indicate the slice and resource utilisation; integer and continuous variables are used to monitor user behaviour and QoS satisfaction.

d) Objective Function: The objective in SIEGE is to maximize system utility by rewarding high QoS while penal-

TABLE II
MODEL DECISION VARIABLES

Variable	Type	Meaning
$x_{u,s,r} \in \{0,1\}$	Binary	Assigned resource r in slice s
$y_{u,s} \in \{0,1\}$	Binary	Accesses slice s (indicator)
$z_{u,r} \in \{0,1\}$	Binary	Uses resource r (indicator)
$p_u \in \mathbb{Z}_{\geq 0}$	Integer	Slices accessed by user u
$q_u \in \mathbb{Z}_{\geq 0}$	Integer	Resources accessed by user u
$\text{QoS}_{u,s} \in \mathbb{R}_{\geq 0}$	Continuous	QoS achieved on slice s

izing suspicious behavior:

$$\text{Max.} \quad \sum_{u\in\mathcal{U}}\sum_{s\in\mathcal{S}} \gamma\cdot w_{u,s}\cdot \text{QoS}_{u,s} - \sum_{u\in\mathcal{U}} (\alpha\cdot\sigma_u\cdot p_u + \beta\cdot\sigma_u\cdot q_u)$$

The first term prioritizes QoS for critical users and slices using the weight $\gamma\cdot w_{u,s}$. The second term penalizes suspicious users based on their slice (p_u) and resource access (q_u), scaled by coefficients α and β. The binary flag $\sigma_u \in \{0,1\}$ activates penalties only for flagged users. This adversarial-aware design balances performance and resilience, enabling proactive threat mitigation without service denial. The tunable weights α, β, γ allow flexible trade-offs for secure slicing under siege.

e) Optimization Constraints:

(1) **QoS Requirement:** Ensures that each user on each slice receives at least the minimum required QoS. This guarantees baseline service levels and filters out configurations that fail to satisfy user requirements.

$$\text{QoS}_{u,s} \geq Q_{u,s}^{\min} \quad \forall u \in \mathcal{U},\ s \in \mathcal{S}$$

(2) **Resource Capacity Constraint:** Prevents over-allocation by ensuring the total resources assigned across all users and slices do not exceed each resource's physical capacity. This keeps the model realistic and physically deployable.

$$\sum_{u\in\mathcal{U}}\sum_{s\in\mathcal{S}} d_{u,s}\cdot x_{u,s,r} \leq C_r \quad \forall r \in \mathcal{R}$$

(3) **Total Slices Accessed (Behavior Tracking):** Sums up all the slice_used flags for a user to determine how many slices they access. This is later used in the objective function to penalize suspicious users for spreading across too many slices.

$$p_u = \sum_{s\in\mathcal{S}} y_{u,s} \quad \forall u \in \mathcal{U}$$

(4) **Total Resources Accessed (Behavior Tracking):** Sums up the resource_used flags for a user to calculate the total number of distinct resources utilized. This acts as another behavioral signal used in detecting and mitigating adversarial overreach.

$$q_u = \sum_{r\in\mathcal{R}} z_{u,r} \quad \forall u \in \mathcal{U}$$

Model Logic and Behavioral Encodings

(1) **QoS Calculation:** Calculates the effective QoS for each user-slice pair by summing up the demand-weighted resources allocated. This is essential for tracking whether user service expectations are being met.

$$\text{QoS}_{u,s} = \sum_{r\in\mathcal{R}} d_{u,s}\cdot x_{u,s,r} \quad \forall u \in \mathcal{U},\ s \in \mathcal{S}$$

(2) **Slice Usage Indicator (aggregated over resources):** Activates the slice_used binary variable if a user utilizes any resource on a given slice. It helps in counting how many slices each user is actively engaged with, for further behavioral analysis or penalization.

$$\text{slice\_used}_{u,s} \geq \frac{1}{|\mathcal{R}|}\sum_{r\in\mathcal{R}} x_{u,s,r} \quad \forall u \in \mathcal{U},\ s \in \mathcal{S}$$

(3) **Resource Usage Indicator (aggregated over slices):** Similar to the slice indicator, this logic activates the resource_used flag if a user is assigned any slice that includes that resource. It tracks the user's footprint across available infrastructure.

$$\text{resource\_used}_{u,r} \geq \frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}} x_{u,s,r} \quad \forall u \in \mathcal{U},\ r \in \mathcal{R}$$

IV. PRELIMINARY RESULTS ANALYSIS

A simulation was conducted with 60 users, 8 slices, and 120 resources. 20% of users were adversarial, exhibiting multi-slice flooding and resource over-claims. Results show that:

- 43.7% reduction in malicious slice occupancy.
- QoS stability maintained for over 90% of legitimate users.
- Solver runtime below 2.5s using AMPL with CPLEX.

Compared to heuristic approaches (round-robin [16], greedy allocation [17]), SIEGE significantly reduces resource wastage and limits adversarial propagation.

The obtained results from the SIEGE model strongly validate its intended functionality as described in the abstract. The visualization of user behaviors as illustrated in Figure 1 through slice access (p_u) and resource usage (q_u) demonstrates clear differentiation between benign and suspicious users. Benign users such as `u1` and `u3` were allocated a broader range of resources (5 each) and accessed multiple slices, enabling them to meet their QoS demands with flexibility `u3`, in particular, achieved a remarkably high QoS score of 75 in slice `s1` as can be seen in Figure 2. In contrast, suspicious users like `u2` and `u4` were strategically constrained: `u2` accessed all 3 slices but was restricted to only 2 distinct resources, while `u4` was tightly limited to 2 slices and 2 resources, reflecting the enforcement of defensive constraints. Despite these limitations, both suspicious users still achieved their minimum QoS requirements, with `u2` receiving 16, 12, and 6 units in slices `s1`, `s2`, and `s3` respectively, and `u4` receiving 7 and 9 units in `s2` and `s3`.

The results further illustrates this balance ensuring service continuity without compromising the network's integrity. Overall, the results confirm that the SIEGE model effectively

detects and limits suspicious behavior while preserving service quality for legitimate users, thereby achieving its goal of resilient, secure, and adversary-aware resource allocation in B5G networks.

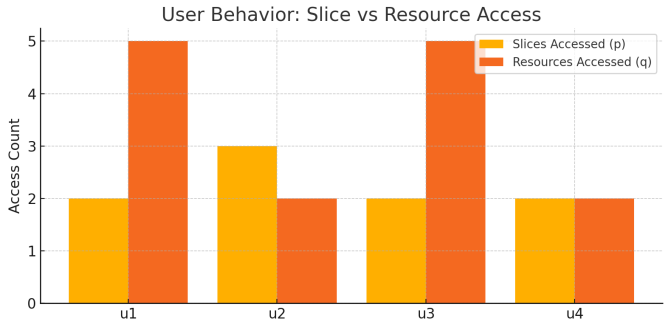

Fig. 1. Slice and resource access counts per user, showing constrained behavior for suspicious users.

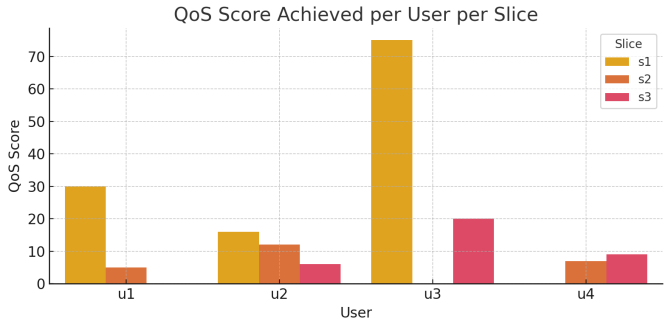

Fig. 2. QoS scores achieved per user across slices, highlighting priority given to legitimate users.

V. Conclusion and Future Work

As part of our current ongoing efforts, we are working on this approach to improve dynamic, real-time traffic simulation and behavioral anomaly detection using temporal data traces. This involves integrating the current AMPL-based optimization with a live emulation environment in Mininet, where attack scenarios such as slice spoofing and resource hijacking can be actively simulated. Additionally, we are working on enriching the adversarial indicators using AI-driven classifiers trained on user interaction patterns, which will dynamically adjust the suspiciousness flags in the model. Future versions of the model will also incorporate multi-domain slicing across heterogeneous access networks, reflecting a more realistic B5G environment. Lastly, we aim to develop a front-end visualization dashboard to help network operators monitor slice security posture, allocation decisions, and threat-level projections in real time, enabling proactive intervention.

In preliminary results, the SIEGE model successfully achieves its objective of enabling secure and resilient resource allocation in B5G networks under adversarial conditions. By integrating behavioral indicators into the optimization process, the model not only detects suspicious users through their slice and resource access patterns but also strategically constrains their activity without fully denying service. The results confirm that the model maintains high QoS for benign users while minimizing the impact of potential resource hijacking attempts. This balance between security enforcement and service fairness demonstrates the model's practical applicability in real-world network slicing scenarios. SIEGE lays a strong foundation for future enhancements such as dynamic trust score adaptation, real-time anomaly integration, and learning-driven mitigation, offering a scalable and explainable framework for security-by-design wireless infrastructures. We seek to engage the research community in the following open questions during the discussion:

1) **RQ1**: How can the ILP model be efficiently adapted to support dynamic and multi-domain slicing scenarios with minimal computational overhead?
2) **RQ2**: What are the most robust methods to validate and interpret the behavioral indicators over time, especially under adversarial drift or coordinated stealth attacks?

References

[1] W. Rafique et al., "A survey on beyond 5G network slicing for smart cities applications," IEEE Commun. Surv. Tutor., vol. 27, no. 1, pp. 595–628, 2024.
[2] S. Tariq et al., "Strategy for modeling threats in 5G and B5G networks," in Proc. IEEE CCGridW, pp. 18–25, May 2024.
[3] Wang, J. and Liu, J., 2022. Secure and reliable slicing in 5G and beyond vehicular networks. IEEE Wireless Communications, 29(1), pp.126-133.
[4] K. Abbas et al., "AI-driven analytics and intent-based networking for B5G consumer services," IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 2155–2169, 2023.
[5] Jover, R.P. and Marojevic, V., 2019. Security and protocol exploit analysis of the 5G specifications. IEEE Access, 7, pp.24956-24963.
[6] Gopal, M. and Velmurugan, T., 2024. Resource allocation algorithm for 5G and B5G D2D underlay wireless cellular networks. Multimedia Tools and Applications, 83(25), pp.66841-66868.
[7] F. Debbabi et al., "Overview of interslice and intraslice resource allocation in B5G networks," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 4, pp. 5120–5132, 2022.
[8] Shahzadi, R., Ali, M. and Naeem, M., 2023. Combinatorial resource allocation in UAV-assisted 5G/B5G heterogeneous networks. IEEE Access, 11, pp.65336-65346.
[9] K. Govindarajan et al., "Closed-loop optimization of 5G network slices," in Proc. 23rd Int. Middleware Conf. Ind. Track, Nov. 2022, pp. 29–35.
[10] Dudin, B., Ali, N.A., Radwan, A. and Taha, A.E.M., 2019. Resource allocation with automated QoE assessment in 5G/B5G wireless systems. IEEE Network, 33(4), pp.76-81.
[11] Wang, J., Li, Y., Liu, J. and Kato, N., 2024. Intelligent network slicing for B5G and 6G: Resource allocation, service provisioning, and security. IEEE Wireless Communications, 31(3), pp.271-277.
[12] B.D. Son et al., "Adversarial attacks and defenses in 6G network-assisted IoT systems," IEEE Internet Things J., vol. 11, no. 11, pp. 19168–19187, 2024.
[13] J. Thaliath et al., "Predictive closed-loop service automation in O-RAN based network slicing," IEEE Commun. Stand. Mag., vol. 6, no. 3, pp. 8–14, 2022.
[14] Singh, V.P., Singh, M.P., Hegde, S. and Gupta, M., 2024. Security in 5g network slices: Concerns and opportunities. IEEE Access, 12, pp.52727-52743.
[15] Ludant, N. and Noubir, G., 2021, June. SigUnder: A stealthy 5G low power attack and defenses. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 250-260).
[16] M. M. Hossain et al., "Optimizing Round Robin Scheduling with DBSCAN Clustering and ML," in Proc. IEEE SPICSCON, Nov. 2024, pp. 1–6.
[17] C. Bouras et al., "Optimizing Network Slices: A Comparative Analysis of Allocation Algorithms for 5G," in Proc. IEEE FCN, Nov. 2024, pp. 1–6.