Silent Drain: From Energy Profiling to Practical Denial-of-Energy Attacks in 5G

Alessandra Dino
alessandra.dino01@unipa.it
Università degli Studi di Palermo
Palermo, Italy

Fabrizio Giuliano
fabrizio.giuliano@unipa.it
Università degli Studi di Palermo
Palermo, Italy

Stefano Mangione
stefano.mangione.tlc@unipa.it
Università degli Studi di Palermo
Palermo, Italy

Domenico Garlisi
domenico.garlisi@unipa.it
Università degli Studi di Palermo
Palermo, Italy

Ilenia Tinnirello
ilenia.tinnirello@unipa.it
Università degli Studi di Palermo
Palermo, Italy

ABSTRACT

In this work, we present *Silent Drain*, a practical Denial-of-Energy attack against commercial 5G User Equipment (UE). Our approach combines extensive energy profiling across RRC states, DRX cycles, scheduling policies, MCS levels, and MIMO configurations with forged Downlink Control Information (DCI) messages that trigger high-consumption states. In a controlled testbed, we show that periodic DCI replays or forged uplink grants keep the UE in *RRC Connected* or induce persistent uplink transmissions, maintaining a +1 W power draw and continuous uplink activity for more than 30 minutes even after detachment. We discuss operational feasibility, testbed limitations, and propose potential countermeasures, including physical layer signaling authentication and energy-aware intrusion detection. Our findings reveal that energy efficiency mechanisms can become powerful and predictable attack vectors in 5G.

CCS CONCEPTS

• **Networks** → **Link-layer protocols**; *Network experimentation*; **Denial-of-service attacks**; **Mobile networks**.

KEYWORDS

5G, Energy Attacks, DCI Spoofing, Energy Profiling.

ACM Reference Format:
Alessandra Dino, Fabrizio Giuliano, Stefano Mangione, Domenico Garlisi, and Ilenia Tinnirello. 2025. Silent Drain: From Energy Profiling to Practical Denial-of-Energy Attacks in 5G. In *ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH '25), November 4–8, 2025, Hong Kong, China.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3737895.3768308

WiNTECH '25, November 4–8, 2025, Hong Kong, China

ACM ISBN 979-8-4007-1972-1/2025/11
https://doi.org/10.1145/3737895.3768308

1 INTRODUCTION

Energy efficiency is a fundamental design goal of 5G networks, crucial for extending the operational lifetime of battery-powered mobile devices and IoT nodes [1]. To achieve this, the 5G NR standard integrates mechanisms such as lean carrier design, flexible Radio Resource Control (RRC) states, and Discontinuous Reception (DRX) [2, 3]. These mechanisms significantly reduce idle power consumption by minimizing always-on transmissions and enabling long sleep cycles. However, they also rely heavily on physical layer control signaling, which is not cryptographically authenticated and may be manipulated by a capable adversary [4].

Previous research has separately investigated the energy consumption characteristics of 5G User Equipments (UEs) under various configurations [1] and the feasibility of control-channel spoofing attacks [4]. However, the connection between *systematic energy profiling* and the *design of targeted denial-of-energy (DoE) attacks* remains underexplored.

In this paper, we bridge this gap by introducing **Silent Drain**, a practical DoE attack against a commercial 5G smartphone. We first conduct an extensive experimental profiling campaign to identify network configurations that maximize the power consumption of the UE. We then leverage these insights to craft forged Downlink Control Information (DCI) messages that systematically trigger high-energy states without delivering useful data. Our main contributions are:

- **Comprehensive energy profiling** of a commercial 5G UE across RRC states, DRX cycles, scheduling policies, MCS levels, and MIMO configurations.
- **Attack design and implementation** of *Silent Drain*, exploiting the most energy-demanding conditions identified during profiling.

- **Experimental validation** showing that the attack sustains high-power operation and uplink activity for over 30 minutes post-detachment, increasing power draw up to 1 W.

By linking profiling and exploitation, we reveal that the mechanisms intended to improve 5G can become predictable and powerful attack vectors. These findings highlight the urgent need for physical layer control signaling protection and energy-aware intrusion detection.

2 RELATED WORK

The security framework for 5G networks has been a central topic in standardization bodies, resulting in an architecture designed to support a wide range of services, from massive Internet of Things (IoT) deployments to Vehicle-to-Everything (V2X) communications [5]. This architecture introduces new security functions and procedures intended to provide a robust defense against a variety of threats [6]. However, despite the continuous development of new countermeasures, the inherent openness of the wireless medium means that the physical layer remains susceptible to attacks that can undermine network performance and security. A significant consequence of such attacks, focus of this work, is the impact on the energy consumption of network devices.

Energy efficiency is a foundational requirement for 5G systems, particularly given the projected scale of mobile devices. Physical layer attacks are a direct method for executing such service denials. Wang et al. provide a comprehensive survey of physical layer security in 5G networks, categorizing threats into active and passive types [7]. Active attacks, such as jamming and spoofing, force legitimate devices to engage in energy-intensive operations, including increasing transmission power, performing complex signal processing for interference cancellation, or engaging in repeated retransmissions, all of which directly deplete power reserves.

Specific attack vectors have been studied to understand their impact on energy resources. Flooding attacks, a form of Denial of Service (DoS), are examined in the context of dense wireless sensor networks, a scenario analogous to massive IoT in 5G [8]. This work shows that flooding a network with superfluous packets forces legitimate nodes to needlessly process incoming data, consuming significant energy and reducing network lifetime. A more targeted approach is the Depletion of Battery (DoB) attack[9]. In this work authors, investigate this threat in 5G-connected UAV networks, demonstrating how an adversary can exploit high-priority control plane messages, such as the Packet Forwarding Control Protocol (PFCP), to keep a device's processor active and prematurely drain its battery life. This highlights how vulnerabilities in higher-layer protocols can be leveraged to mount an attack with direct physical layer consequences on energy consumption as described in[10].

The potential for applying machine learning to identify recurring network issues, as explored in [11], for predicting technical ticket reopening, suggests a possible direction for detecting patterns associated with persistent energy-draining attacks. Finally, Maiwada et al. establish a direct connection between network attacks and energy inefficiency, identifying Distributed Denial of Service (DDoS) attacks as a primary cause of excessive power drain [1].

3 BACKGROUND

In 5G-NR, the power consumption of a UE is strongly influenced by its connection state and by the parameters it receives over the physical layer control channel. The RRC protocol defines three main states. In *RRC IDLE*, the UE performs only basic cell search and paging reception, consuming minimal power. The *RRC INACTIVE* state retains the network context while reducing radio activity, enabling faster resumption of data transfer. In *RRC CONNECTED*, the UE maintains an active link with the gNB, sustaining full radio and baseband operation.

The transitions between these states are regulated by inactive timers [2], which are reset upon receiving DCI messages carried on the Physical Downlink Control Channel (PDCCH). The scheduling of transmissions is also governed by these DCI messages, which instruct the UE on when and how to send or receive data, specifying parameters such as allocated resource blocks (RB), modulation and coding scheme (MCS), and the number of MIMO layers. Although a cyclic redundancy check (CRC) masked with the UE's RNTI and Scrambling ID is used for validation, this mechanism does not provide cryptographic authentication.

A key energy-saving feature is DRX, which allows a UE in *RRC CONNECTED* to periodically turn off its receiver and wake up at scheduled intervals to monitor the PDCCH. Short DRX cycles result in frequent wake–ups and higher processing activity, while longer cycles extend sleep periods at the cost of higher latency.

Finally, physical layer parameters such as MCS and MIMO configuration also impact the energy profile. In 5G NR, the UE determines the number of spatial layers according to Signal to Interference Plus Noise Ratio (SINR) measured through Channel State Information Reference Signals (CSI-RS). As reported in the 3GPP Standard [3] [12], the UE communicates to gNB its channel quality report (CQI), and, according to this, gNB selects the corresponding MCS value. Higher-order modulation can reduce airtime per bit and improve efficiency, while multilayer MIMO increases processing load, but can shorten transmission time if channel conditions allow. Understanding how these mechanisms interact is essential for

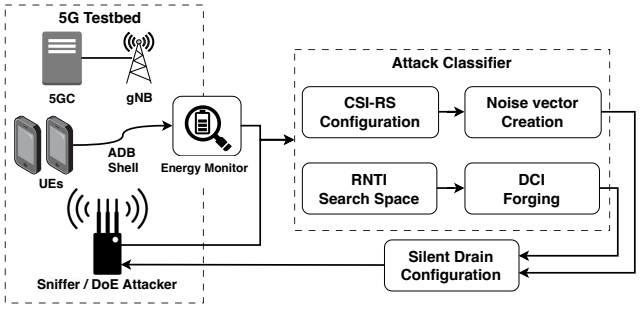


Figure 1: Workflow of the proposed method.

identifying network configurations that lead to sustained high-power operation, a prerequisite for the attack described in the following sections.

4 METHODOLOGY

Our methodology follows a two-phase approach (see Fig. 1): (1) systematic profiling of UE energy consumption under controlled network configurations, and (2) targeted exploitation of the most energy-demanding conditions through a DoE attack.

4.1 Phase 1: Energy Profiling

4.1.1 Testbed Setup. We deploy a private 5G Stand-Alone (SA) network using `Open5GS` for the 5G Core [13] and `srsRAN` [14] for the gNB. The Radio Unit (RU) is implemented with a USRP N310 SDR [15], operating as an FDD cell in band n2 [16] at 1970 MHz with 20 MHz bandwidth. The UE under test (UUT) is a commercial Google Pixel 8a smartphone connected over the air.

4.1.2 Profiling Scenarios. To characterize the UE's energy profile, we isolate and vary key network parameters:

- **RRC States**: Idle, Inactive, and Connected modes.
- **DRX Configuration**: different cycle lengths and on-duration timers.
- **Scheduling Policy**: Round Robin (RR) [17] and Proportional Fair (PF) [18].
- **Modulation and Coding Scheme (MCS)**: low (QPSK) and high (64QAM) modulation orders.
- **MIMO Configuration**: SISO and 2x2 MIMO.

For each configuration, we generate traffic patterns (moderate-intensity ping, high-intensity `iPerf`) and measure power draw using the Android Debug Bridge (ADB) interface, logging current consumption over 120-second intervals.

4.1.3 Metric. We normalize results via the *energy-per-bit* metric, defined as $\gamma_e = P/R_b$ [J/bit], where P is the average power draw and R_b the achieved bit rate.

Outcome of Phase 1. The profiling identifies configurations with the highest γ_e, such as: (1) Connected state with saturated uplink, (2) DRX disabled, (3) low MCS under high traffic, (4) suboptimal scheduling patterns, and (5) single-layer transmissions. These insights directly inform our attack design.

4.2 Phase 2: Attack Design and Implementation

4.2.1 Threat Model. We assume an attacker with: (1) An SDR capable of transmitting 5G NR-compliant downlink signals. (2) Synchronization with the target cell via PSS/SSS decoding. (3) Knowledge of the UE's RNTI and Search Space through passive sniffing [19].

The goal is to force the UE into high-energy states identified in Phase 1 without delivering useful data.

4.2.2 Attack Mechanism: DCI Spoofing. We modify the `srsUE` stack to perform cell synchronization and inject forged DCI messages targeting the victim's RNTI. Pre-computed DCI payloads (generated offline in MATLAB) are transmitted in the correct PDCCH Search Spaces to:

- Maintain the UE in *RRC CONNECTED* by replaying valid-looking DCIs at regular intervals.
- Assign uplink resources with custom MCS and RB allocations.

4.2.3 Attack Scenarios. The attack scenarios presented in this work are:

(1) **RRC Connection Keep-Alive**: periodic DCI replays prevent inactivity timers from expiring.
(2) **Single-layer Transmission Forcing**: periodic noise on CSI-RSs, forcing UE to drop to a SISO configuration.
(3) **Persistent Uplink Drain**: forged DCI messages to trigger continuous transmissions, persisting even after UE detachment due to retransmission loops.

Link to Phase 1. The DCI parameters in both scenarios are chosen based on the worst-case energy conditions observed in profiling (e.g., DRX disabled, low MCS in a single-layer cell configuration). This ensures that each forged allocation maximizes the UE's power draw.

5 UE ENERGY CONSUMPTION

This section presents a systematic measurement of UE energy consumption in various configurations of 5G networks. The objective is twofold: (1) quantify the impact of RRC states, DRX cycle, scheduling policy, MCS level, and MIMO configuration on power draw, and (2) identify worst-case configurations that can later be exploited in targeted DoE attacks. Each experiment lasts about 120 seconds, and each mechanism for energy efficiency is tested under two traffic

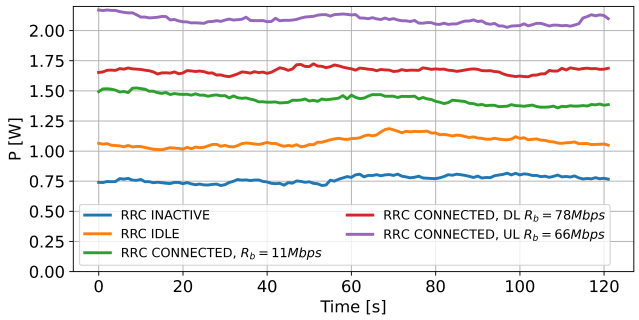


Figure 2: Impact of RRC state and traffic load on energy consumption.

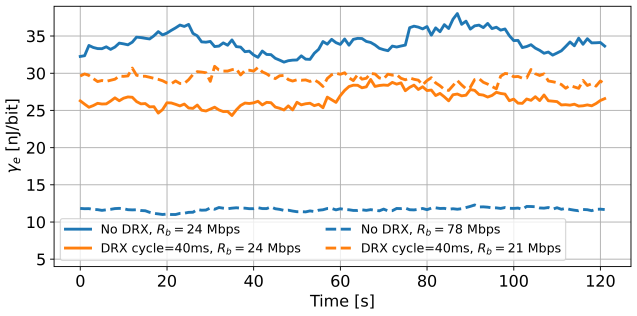


Figure 3: Impact of DRX on γ_e with moderate traffic (solid line), high traffic (dashed line) scenarios.

conditions: moderate (with flood-ping) and intensive (with iPerf).

5.1 RRC State Analysis

To estimate the energy footprint of each RRC state, we evaluated the power absorbed by the smartphone during:

- `RRC IDLE`: In this case, we are measuring the power that smartphone needs to stay-on and do cell search. We can reach this state by stopping all traffic sources and waiting for the inactivity timer to expire.
- `RRC INACTIVE`: This is the state reached by the smartphone when all traffic is stopped, but the inactivity timer is not expired yet.
- `RRC CONNECTED`: We evaluate this state under three traffic conditions to highlight the impact of different load levels:
  - **Moderate traffic (flood ping)**: Periodic ICMP echo requests were sent from the gNB to the UE, generating downlink/uplink activity (about 11Mbps in both directions, single-layer), keeping the UE in connected mode.
  - **Downlink saturation (iPerf DL)**: We generate continuous UDP downlink traffic using iPerf, saturating the UE's receive capacity, with about 76Mbps in single-layer downlink.
  - **Uplink saturation (iPerf UL)**: Similarly, the UE transmits UDP data at full capacity using iPerf in uplink mode, measuring about 66Mbps in single-layer uplink.

Although we did not directly capture state transitions, the steady-state current profiles provide insight into the energy characteristics of each RRC mode and how they scale with traffic intensity in `RRC CONNECTED`. Fig. 2 reveals a clear gradient in current draw, with idle and inactive states consuming significantly less power. As expected, the `RRC Connected` state incurs the highest energy drain, particularly under saturated traffic conditions. In particular, the difference between moderate and high traffic (both DL and UL) in `RRC Connected` demonstrates the substantial impact of data activity on the power consumption of the UE, the UL saturation case showing the highest energy drain.

5.2 Impact of DRX Configuration

To evaluate the energy-performance tradeoff introduced by DRX, we measured the current consumption of the UE under two operational modes:

- **DRX enabled:** the UE is configured to wake up for 10ms every 40ms; the configuration in srsRAN could be done using these parameters (specifically, in `drx` section): `long_cycle`= 40ms, `on_duration_time` = 10ms.
- **DRX disabled (always-on):** the UE remains continuously active by setting `long_cycle` = 0.

As shown in Fig. 3, enabling DRX in moderate traffic scenario leads to a notable lower γ_e, even with a relatively short cycle of 40ms. While longer DRX cycles could potentially yield larger energy savings, such configurations are not supported in our testbed: values above 40ms result in de-synchronization between the UE and gNB in `srsRAN`, resulting in a higher required γ_e in our experiments. In saturated downlink traffic conditions, enabling DRX can reduce instantaneous throughput to a fraction of its maximum, as data can only be scheduled during on-duration periods. As a result, the same volume of data is delivered over a longer time, extending the total UE's active period.

5.3 Scheduling Policy Impact

We evaluated the energy implications of two resource allocation strategies implemented in the `srsRAN` gNB scheduler: RR (Round Robin) and Proportional Fair (PF). RR is the default scheduler in `srsRAN`, which allocates resources uniformly among all connected UEs, regardless of channel conditions or QoS requirements. Although RR offers strict fairness in terms of time-domain resource allocation, it does not consider radio link quality or traffic priority, which can lead to inefficient spectrum usage or degraded service for latency-sensitive flows. To address these limitations, we activated the PF scheduler by enabling the `sched_expert_cfg` section in the gNB configuration file.

In both cases, a second UE was connected to the same gNB to produce independent traffic (e.g. video streaming),

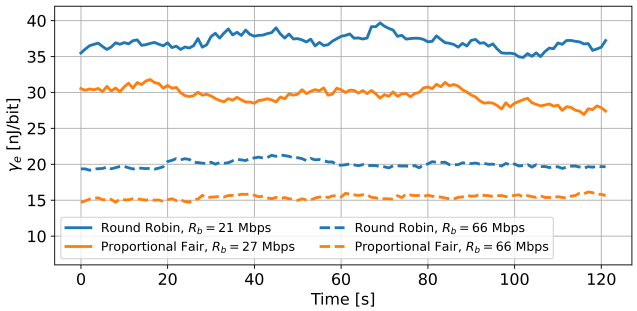


Figure 4: Impact of scheduling on γ_e with moderate traffic (solid line), high traffic (dashed line) scenarios.

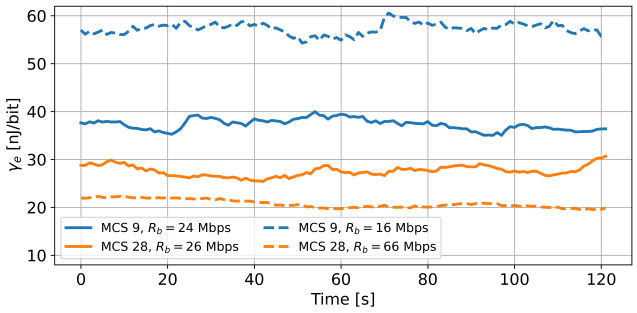


Figure 5: Impact of MCS on γ_e with moderate traffic (solid line), high traffic (dashed line) scenarios.

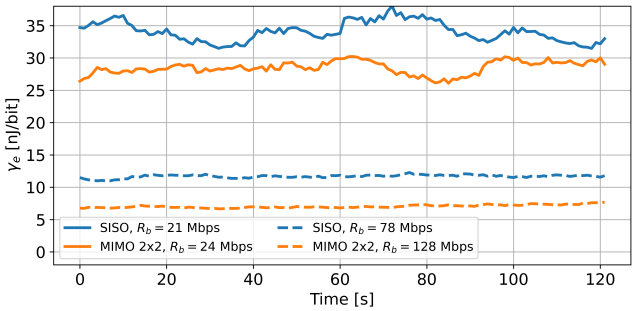


Figure 6: Impact of number of layer used on γ_e with moderate traffic (solid line), high traffic (dashed line) scenarios.

Parameter	Configuration	Exploitability
RRC State	Connected + UL Saturation	High
DRX	Depends on traffic conditions	Medium
Scheduling	Round Robin	Low
MCS	Low (QPSK)	High
MIMO	Single-Layer	High

Table 1: Summary of profiling results and exploitability assessment.

ensuring non-trivial scheduling behavior beyond single-UE allocation. Current consumption was recorded under stable radio and application-layer conditions, identical across both scheduling configurations.

The experiments expose that, (Fig. 4), the PF scheduler achieves better efficiency, in both traffic scenarios, with an improvement of up to 10nJ/bit in moderate traffic and approximately 5nJ/bit under iPerf traffic. Note that the measured γ_e is lower in the high-load iPerf case, suggesting that sustained and predictable scheduling leads to more stable RF behavior and fewer state transitions, thereby reducing waste.

5.4 Modulation Coding Scheme Impact

To evaluate the energy impact of different MCS, we forced the UE to operate at fixed uplink and downlink MCS levels by configuring the pusch and pdsch section of the gNB. We considered two modulations: QPSK (MCS = 9) and 64-QAM (MCS = 28). In both traffic scenarios, higher MCS levels consistently lead to better energy efficiency. As shown in Fig. 5, the use of lower MCS values increases γ_e due to prolonged airtime per bit, which extends RF chain activity and contributes to higher energy expenditure.

The results show as under low traffic conditions, the energy gap reaches up to 5nJ/bit in favor of the high MCS setting. This difference becomes even more pronounced under high-load traffic, where the low-MCS configuration incurs up to 30nJ/bit more than the high-MCS case.

These findings indicate that higher-order modulation not only improves spectral efficiency but also leads to better energy performance, regardless of traffic intensity.

5.5 MIMO Configuration

To assess the energy impact of spatial diversity, we examined the behavior of the UE under two MIMO configurations. Specifically, we tested a SISO configuration (Single-layer) and a MIMO 2x2 (two-layers) configurations.

Regardless of the configuration, we verified via low-level logs that the UE consistently transmits using a single antenna, while the number of receiving antennas varies depending on the channel quality [3].

Contrary to the common assumption that MIMO configurations lead to higher energy consumption due to the activation of multiple RF chains, our efficiency analysis shows the opposite trend. As illustrated in Fig. 6, we observed a reduction of approximately 5nJ/bit when using MIMO, indicating that the ability to transmit more data in less time outweighs the potential cost of activating additional hardware.

5.6 Summary of Profiling Results

Table 1 highlights configurations considered highly exploitable.

Figure 7: Experimental setup of the attack scenario.

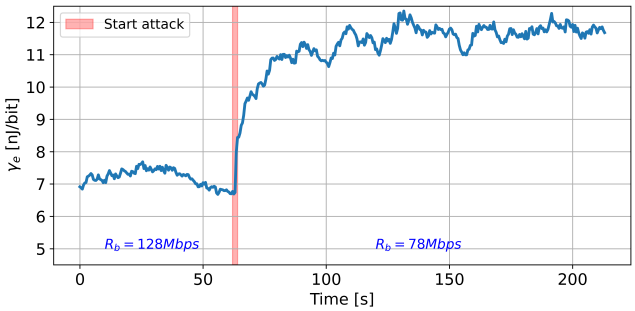


Figure 8: Impact of attack on CSI-RS on energy-per-bit.

Those marked as high exploitability represent worst-case conditions that substantially increase the UE's energy consumption. These empirical results are strictly linked to the parameter choices in the *Silent Drain* attack.

6 SILENT DRAIN ATTACKS

Based on the worst-case energy configurations identified in Section 5, we implement *Silent Drain*, a family of DoE attacks targeting different physical layer parameters of a 5G UE. The common objective is to keep the UE in highly energy-inefficient states without delivering useful data.

6.1 Threat Model

The attack setup, shown in Fig. 7, uses a USRP B210 [20] SDR, connected to a host PC running our tool, which is a custom-modified version of `srsUE`. The modifications to the stack enable the following operations:

- **Cell Search and Synchronization:** The attacker can synchronize with the target cell via PSS/SSS and PBCH decoding.
- **System Frame and Slot Timing Estimation:** After successful synchronization, the tool estimates the System Frame Number (SFN) and slot index, which are essential to ensure that signaling messages are transmitted with precise timing.
- **Transmission of Custom Signals:** Once synchronization and timing estimation are complete, the attacker can transmit noise, spoofed or replayed DCI messages targeting the RNTI associated with the victim UE.

In order to get the initial synchronization, the crystal oscillator error of USRP B210 is calibrated using [21].

The knowledge of the UE's RNTI and cell configuration is due to the prior access to the network configuration in `srsRAN`, but in a real-case scenario some passive tools, such as [19] and [22], could reveal them. Moreover, to maximize the energy impact of the attack, we spoofed both DCI 1_0 and DCI 0_0 messages. This induces the UE to unnecessarily activate its radio chains, either to transmit or to listen for data, thereby increasing power consumption even in the absence of actual traffic.

Since the `srsUE` implementation does not support the generation of custom PDCCH payloads, DCI messages are precomputed offline using MATLAB and transmitted in real time by the attacker.

6.2 Variant 1: Single-Layer Enforcement

Objective: Reduce MIMO efficiency by forcing the UE to operate with a single spatial layer.

Initial Conditions: The UE is connected to a 2×2 MIMO cell and running a DL `iPerf` session, achieving a R_b = 128 Mbps with RI = 2. The MCS index reaches 28, DRX is disabled, and the scheduler operates in RR mode.

Mechanism: At $t \approx 65$ s, the attacker transmits noise on the CSI-RS resources, preventing the UE from correctly measuring the cell's SINR. Knowing the CSI-RS slot position and periodicity from the `srsRAN` configuration, the attacker targets these resources precisely; alternatively, energy-based spectrum scans could estimate their position. Following the start of the attack, the UE's RI drops from 2 to 1, the MCS remains at 28, and the R_b decreases to around 78 Mbps.

Impact: Limiting UE to one spatial layer increases transmission time for a given throughput, increasing the γ_e (Fig.8).

6.3 Variant 2: Persistent Connected State

Objective: Prevent the UE from entering low-power RRC states (Inactive/Idle) by periodically injecting forged DCIs.

Initial Conditions: The UE is connected to a single-layer cell, operating in `RRC CONNECTED` state with DRX disabled and RR scheduling. In this baseline configuration, the UE would normally transition to lower-power states after the inactivity timer expires if no data activity is detected.

Mechanism: Every 10 ms (see Fig. 9), corresponding to the minimum DRX cycle allowed by the standard, the attacker transmits a forged allocation for the victim's RNTI, ensuring that the inactivity timer never expires.

Impact: Although no actual data is transmitted, the UE interprets the fake downlink signaling and tries to decode

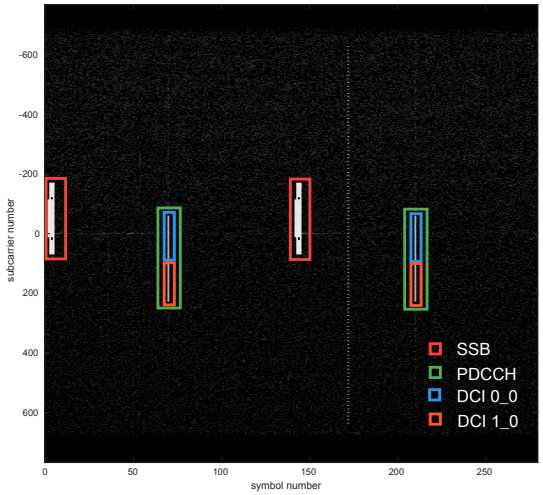


Figure 9: DCI replays transmitted every 10ms.

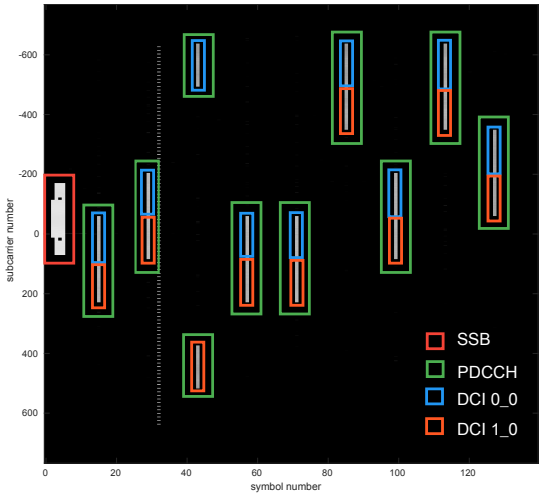


Figure 10: Forged DCI 0_0 and DCI 1_0 messages periodically injected, triggering uplink transmissions.

the downlink data, and the fake uplink grants are legitimate, triggering dummy scheduling activity. In fact, we empirically observe that upon receiving each forged uplink grant, the UE attempts a transmission, even if there is no data to send. This confirms that uplink activity is stimulated by the grant, without requiring application-layer triggers, amplifying the energy impact of the attack.

6.4 Variant 3: MCS and Resource Allocation Manipulation

Objective: Force the UE into low spectral efficiency modes while consuming maximum resources.

Initial Conditions: The UE is connected to a SISO cell with DRX disabled and RR scheduling. At the application layer, the UE is generating a traffic with $R_b = 11$ Mbps.

Mechanism: Excluding slot 0 to avoid interfering with the SSB, in every slot (see Fig. 10) the attacker injects, into the UE's Search Space, forged DCI messages that:

- Set a low MCS index (e.g., QPSK), which reduces spectral efficiency and increases the airtime required per bit.
- Set the Frequency Domain Resource Assignment (FDA) field to allocate all available RBs, forcing the UE to process the maximum channel bandwidth in each slot.

Due to the attacker's proximity, the forged PDCCH messages override the legitimate gNB control channel, effectively saturating all uplink and downlink scheduling opportunities.

Impact: The UE processes large volumes of control and data channel resources inefficiently. Upon receiving each forged uplink grant, the UE transmits on the allocated resources, leading to de-synchronization with the legitimate gNB and, eventually, AMF-triggered disconnection. However the UE enters a persistent retransmission loop, non-compliant with 3GPP standards, repeatedly sending the same transport blocks. Unexpectedly, retransmissions continue indefinitely, over 30 minutes in our experiments, even after the UE has lost connection to the serving cell.

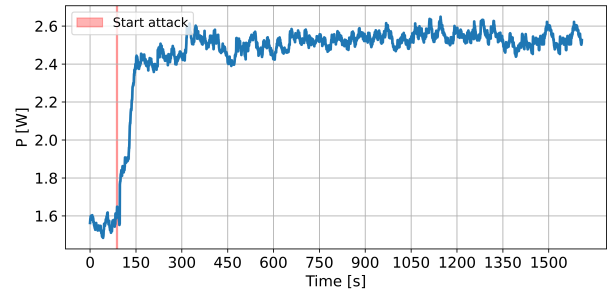
Fig. 11a reports the measured *power* consumption during this phase (not γ_e), as the uplink R_b during the disconnected retransmission loop is not under our control. In principle, the uplink throughput could be inferred by spectrum analysis, as the uplink channel appears fully occupied during the loop, but we do not explicitly measure it.

The measured power is anomalously high, as also reflected in the increase of battery temperature (Fig. 11b), remaining over +1 W compared to the `RRC Connected` baseline. This highlights a vulnerability in the UE's retransmission logic: in the absence of gNB acknowledgments, the UE continues its efforts indefinitely. Such behavior can be exploited to drain the battery with minimal attacker effort, without requiring core network interaction.

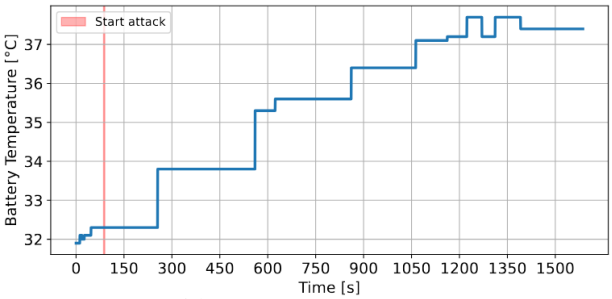
To verify that this phenomenon was not due to a device-specific firmware, we repeated the attack on a second commercial device, a Samsung Galaxy S25. The results were consistent, confirming that the observed behavior is not limited to a single model or vendor.

7 CONCLUSION AND FUTURE WORK

In this work, we showed that systematic energy profiling of a commercial 5G UE can reveal specific network configurations that significantly increase power consumption. Based on these measurements, we designed the *silent drain* attack, which injects forged DCI to force the UE into or maintain it within such high-consumption states. In our testbed, these conditions sustained $\approx +1\ W$ additional power draw and prolonged uplink activity for over **30 minutes** after disconnection from the serving cell.



(a) Absorbed average power



(b) Battery temperature

Figure 11: Effects on: (a) Absorbed mean power and (b) Battery temperature during a *Silent Drain* Attack.

To mitigate such threats, we propose: (i) integrity protection or lightweight authentication of DCI messages to prevent spoofing; (ii) UE–side anomaly detection that correlates energy usage with expected traffic and operational states; (iii) gNB–side monitoring to identify abnormal grant patterns and terminate suspicious activity promptly.

Future work will focus on profiling to multiple devices and frequency bands, assess the feasibility of the attack in real world scenario. We also plan to investigate energy–aware intrusion detection methods capable of recognizing sustained high–power states unrelated to legitimate traffic.

8 ACKNOWLEDGMENTS

This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU: partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"), project SPRINT CUP: E83C22004640001 and project Net4Future CUP: D93C22000910001; by the project SERICS (PE00000014 - CUP D33C22001300002) under the PNRRP MUR program funded by the EU-NGEU.

REFERENCES

[1] Umar Danjuma Maiwada, Kamaluddeen Usman Danyaro, Aliza Sarlan, M.S. Liew, Ayankunle Taiwo, and Umar Ismaila Audi. Energy Efficiency in 5G Systems: A systematic literature review. *International Journal of Knowledge-Based and Intelligent Engineering Systems*, 2024.

[2] 3GPP. NR; Radio Resource Control (RRC); Protocol specification. Technical Specification 38.331, 3rd Generation Partnership Project, 2024.

[3] 3GPP. NR; Physical layer procedures for data. Technical Specification (TS) 38.214, 3rd Generation Partnership Project (3GPP), 09 2024. 18.4.0.

[4] Norbert Ludant, Marinos Vomvas, and Guevara Noubir. Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous. *arXiv preprint arXiv:2403.06717*, 2024.

[5] Xiaowei Zhang, Andreas Kunz, and Stefan Schröder. Overview of 5G Security in 3GPP. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017.

[6] Xinsheng Ji, Kaizhi Huang, Liang Jin, Hongbo Tang, Caixia Liu, Zhou Zhong, Wei You, Xiaoming Xu, Hua Zhao, Jiangxing Wu, et al. Overview of 5G Security Technology. *Science China Information Sciences*, 61(8):081301, 2018.

[7] Ning Wang, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*, 2019.

[8] Gaurav Soni and Kamlesh Chandravanshi. Security Scheme to Identify Malicious Maneuver of Flooding Attack for WSN in 6G. In *2021 8th International Conference on Signal Processing and Integrated Networks*, 2021.

[9] Meenu Rani Dey, Cp Bhumika, H N Ankitha, B Nethravathi, and Moumita Patra. Early Detection of Battery Depletion Attack in 5G-based UAV Networks. In *2024 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2024.

[10] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[11] Raman Batra, Varalakshmi S, and Shashikant Patil. Enhancement of 5G N/W System for the use of ML Algorithm Based Ticket-Reopening System for the use of Attack Prediction. In *2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS)*, pages 1–5, 2024.

[12] 3GPP. NR; Physical channels and modulation. Technical Specification (TS) 38.211, 3rd Generation Partnership Project (3GPP), 07 2024. 18.3.0.

[13] Open5GS Project. Open5GS. https://open5gs.org/, 2024.

[14] SRS. Open source O-RAN 5G CU/DU solution from Software Radio Systems (SRS).

[15] Ettus Research. *USRP™ N310 Simplifying SDR Deployment.*

[16] https://www.sharetechnote.com/html/5G/5G_FR_Bandwidth.html.

[17] Ellen L. Hahne. Round-Robin Scheduling for Max-Min Fairness in Data Networks. *IEEE Journal on Selected Areas in communications*, 2002.

[18] TBLELR Ramjee, T Bu, and L Li. Generalized Proportional Fair Scheduling in Third Generation Wireless Data Networks. In *IEEE INFOCOM*, 2006.

[19] Norbert Ludant, Pieter Robyns, and Guevara Noubir. From 5G Sniffing to Harvesting Leakages of Privacy-Preserving Messengers. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3146–3161, 2023.

[20] Ettus Research. *USRP™ B200/B210 Bus Series.*

[21] Stefano Mangione, Alessandra Dino, Giovanni Garbo, and Daniele Croce. Crystal Oscillator Error Compensation in Software Defined Radios for 5G Network Testbeds. In *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pages 1–5. IEEE, 2024.

[22] Haoran Wan, Xuyang Cao, Alexander Marder, and Kyle Jamieson. NR-Scope: A Practical 5G Standalone Telemetry Tool. In *Proceedings of the 20th International Conference on emerging Networking EXperiments and Technologies*, pages 73–80, 2024.