Demo: Decoding Control Information Passively from Standalone 5G Network

Haoran Wan, Xuyang Cao
Department of Computer Science,
Princeton University
Princeton, New Jersey, USA
{haoran.w,xyc}@princeton.edu

Alexander Marder
Department of Computer Science,
Johns Hopkins University
Baltimore, Maryland, USA
amarder@jhu.edu

Kyle Jamieson
Department of Computer Science,
Princeton University
Princeton, New Jersey, USA
kylej@princeton.edu

Abstract

5G New Radio cellular networks are designed to provide high Quality of Service for application on wirelessly connected devices. However, changing conditions of the wireless last hop can degrade application performance, and the applications have no visibility into the 5G Radio Access Network (RAN). Most 5G network operators run closed networks, limiting the potential for co-design with the wider-area internet and user applications. This paper demonstrates *NR-Scope*, a passive, incrementally-deployable, and independently-deployable Standalone 5G network telemetry system that can passively measure fine-grained RAN capacity, latency, and retransmission information. Application servers can take advantage of the measurements to achieve better millisecond scale, application-level decisions on offered load and bit rate adaptation than end-to-end latency measurements or end-to-end packet losses currently permit. We demonstrate the performance of NR-Scope by decoding the downlink control information (DCI) for downlink and uplink traffic of a 5G Standalone base station in real-time.

1 Introduction

5G Standalone (SA), the ultimate phase of 5G deployment, is stepping towards the major cellular *Radio Access Network* (RAN) technology, making up 25% of mobile data at the end of 2023 and forcasted to grow to 76% by 2029 [2]. 5G SA provides higher throughput, higher capacity and lower latency than 4G through optimizations in the RAN, such as shorter *Transmission Time Interval* (TTI) and higher *Subcarrier Spacing* (SCS), and the mobile core, such as more disaggregated core functions for more flexible deployment strategies. In this way, 5G makes a rich canvas for NextG novel applications, such as interactive cloud gaming, and remote surgery.

However, wireless networks, the last mile of connectivity, suffer from highly variable throughput due to user movement, channel fading, blockage, and interference. This variable throughput poses performance challenges for many end-to-end applications, ranging from the congestion control needed for bulk data transfer [3, 7] to interactive video [6, 8, 14]. Furthermore, the closed nature of the RAN inhibits co-design of applications and the cellular network.

In this paper, we demonstrate **NR-Scope**, a RAN telemetry tool that decodes the necessary *Radio Resource Control* (RRC) messages and *Downlink Control Information* (DCI) from the 5G SA network. This information allows NR-Scope to determine a cell's configuration, physical layer traffic scheduling for all of the user equipment (UEs) in the RAN, and infer each UE's channel condition. NR-Scope works in tight synchronization with the 5G SA network, where it decodes the DCIs in every TTI, consisting of 1, 0.5, or 0.25 ms in sub-6GHz 5G cell. NR-Scope also acquires the number of bits that are delivered in each TTI —providing an *exact* throughput estimation for each UE in the RAN—so that developers can improve the performance of various applications. The result is an open design that operates entirely independently of the 5G network operator and 5G mobile devices themselves.

2 NR-Scope Demonstration

We will demonstrate NR-Scope in real-time measurements.

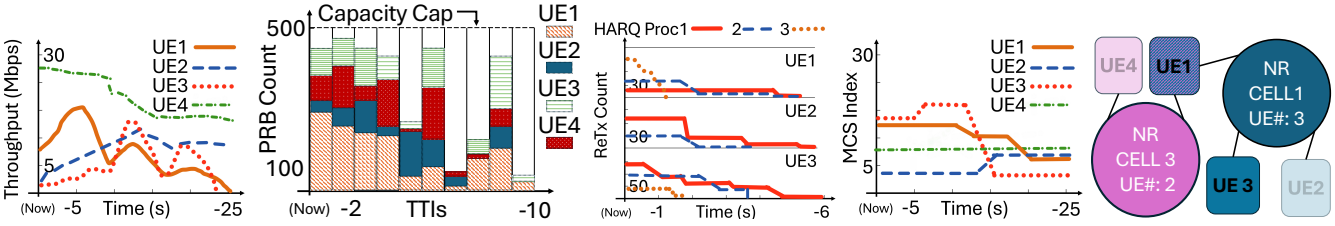
Visualization. For the telemetry result, we will use scripts to exhibit the results in real time, shown in Fig. **1**. With the fine-grained telemetry information extracted (§3), we can easily get exact throughput estimations for UEs (Fig. **1(a)**), as well as the PRB allocation among UEs (Fig. **1(b)**). Furthermore, by tracking the *Hybrid Automatic Repeat Request* (HARQ) processes and *New Data Indicator* in the DCI, we can collect the retransmission information (Fig. **1(c)**). With the *Modulation Coding Scheme* (MCS) index in the DCI plotted (Fig. **1(d)**), we can acquire rough channel condition indicator for UEs as base station would choose higher MCS with better channel condition. In the end, by counting the number of DCIs within a time window, NR-Scope can tell which UE is more actively sending/receiving the data, where the less active UEs have the more transparent circles (Fig. **1(e)**).

Hardware. We will demonstrate NR-Scope in multiple different base stations, **1)** a indoor private 5G SA cell and **2)** an industrial cellular network test equipment, additionally if possible **3)** a commercial 5G cell on the venue site. For the indoor private 5G cell, we will bring a Mosolab indoor small cell [10] and some Motorola 5G phones to the scene. We will also bring an X310 USRP with a laptop and run NR-Scope to decode the telemetry information for the UE. For the industrial cellular network test equipment, we set up the Amarisoft Callbox and UE Emulator [1] in our lab and a USRP in their vicinity. Then we access them remotely and extract the telemetry information. With the Amarisoft equipments, we can emulate up to 64 UEs and obtain the ground truth from the log for verification. For the last one, we are not certain if there is a commercial 5G SA cell nearby the conference room. So before the demo session, we will do a measurement with a phone to check if there is a 5G SA cell nearby, and if so we can also try to perform telemetry on it.

3 NR-Scope Design and Application

3.1 Telemetry Design

The goal of NR-Scope is to decode and interpret DCI, scheduled information that tells each UE where in the 5G SA physical data channels to receive or send its data, thus how much data is actually



(a) Throughput estimation. **(b)** PRB allocation. **(c)** Retransmission behavior. **(d)** MCS indexes. **(e)** UE activeness (UE1 in carrier aggregation).

Fig. 1— Real-time demonstration of NR-Scope in various metrics.

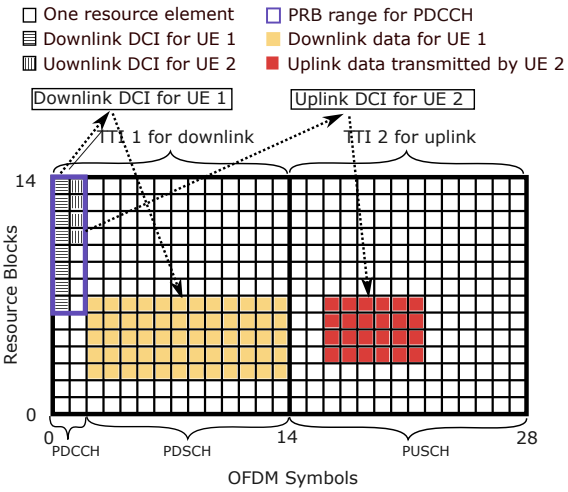


Fig. 2— A demonstration of 5G physical channel for downlink and uplink transmission within two TTIs.

present on the physical channels (Fig. 2). O-RAN has such information for monitoring and better scheduling[4, 9], NR-Scope opens it up for even closed RAN.

1) Cell Scan. The goal of this step is to extracts 5G cell's initial channel configuration parameters, which describes the structure of the channel that a UE uses to associate with the cell. NR-Scope decodes MIB and uses its information to decode *System Information Block* (SIB) 1.

2) UE Discovery. The goal of this step is to acquire each users' *Cell Radio Network Temporary Identifier* (C-RNTI), and the channel's parameters of the final telemetry. NR-Scope must decode the *Random Access Channel* (RACH) process to retrieve the C-RNTIs, as all DCIs after the RACH process are scrambled by a sequence derived from the C-RNTIs.

3) DCI Extraction. The goal of this step is to acquire the amount of resource elements for each UE in the data channel (PDSCH) in the RAN (Fig. 2), and the associated physical layer parameters. With all required information known (C-RNTI, aggregation level, DCI format), NR-Scope receives DCI through the standard 3GPP process [11, 12].

4)Throughput Estimation. In this step, NR-Scope uses the telemetry information to calculate the capacity allocated to each UE. With the DCI and RRC messages decoded in prior steps, the *Transport Block Size* (TBS) for each DCI, indicating how many bits are transmitted for the specific UE in this TTI, can be calculated. Also, DCIs contain re-transmission indicator, facilitating the actual bit-rate estimation.

3.2 Current and Future Applications

NR-Scope can facilitate many applications.

Congestion Control. With the exact in-use and spare capacity estimated passively, NR-Scope can serve as a perfect throughput estimator without posing any burden on the channel, providing sub-millisecond level granularity [15].

Cloud Gaming. Interactive cloud gaming requires low latency and high throughput, NR-Scope can help regulate the packet sending strategy to achieve high throughput and low latency by exposing the RAN's bottleneck [13].

Spectrum Consumption Models. The fundamental information model of the *Zone Management System* (ZMS) of a Radio Dynamic Zone is *Spectrum Consumption Models* (SCMs), recently standardized [5]. NR-Scope unveils the closed 5G RAN's usage, thus other wireless technologies can take advantage of the idle 5G spectrum when possible.

Security. The RRC and MAC layer information that NR-Scope provides can inform situational awareness assessments that distinguish legitimate from surveillance cells, and identify RAN components suspected of having compromised supply chains.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant Nos. AST-2232457, CNS-2223556 and ITE-2326928.

References

[1] [n. d.]. AMARI Callbox Mini. ([n. d.]). https://www.amarisoft.com/test-and-measurement/device-testing/device-products/amari-callbox-mini

[2] [n. d.]. Mobile data traffic forecast – Mobility Report. ([n. d.]). https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast

[3] Venkat Arun and Hari Balakrishnan. 2018. Copa: Practical Delay-Based Congestion Control for the Internet. In *Proceedings of the Applied Networking Research Workshop*. ACM, Montreal QC Canada, 19–19. https://doi.org/10.1145/3232755.3232783

[4] Arjun Balasingam, Manikanta Kotaru, and Paramvir Bahl. 2024. {Application-Level} Service Assurance with 5G {RAN} Slicing. 841–857. https://www.usenix.org/conference/nsdi24/presentation/balasingam

[5] Carlos E. Caicedo Bastidas, John A. Stine, Anthony Rennier, Matthew Sherman, Alex Lackpour, Mieczyslaw M. Kokar, and Reinhard Schrage. 2018. IEEE 1900.5.2: Standard Method for Modeling Spectrum Consumption: Introduction and Use Cases. *IEEE*

Communications Standards Magazine 2, 4 (Dec. 2018), 49–55. https://doi.org/10.1109/MCOMSTD.2018.1700054 Conference Name: IEEE Communications Standards Magazine.

[6] Niklas Blum, Serge Lachapelle, and Harald Alvestrand. 2021. WebRTC: real-time communication for the open web platform. *Commun. ACM* 64, 8 (Aug. 2021), 50–54. https://doi.org/10.1145/3453182

[7] Neal Cardwell, Yuchung Cheng, C. Stephen Gunn, Soheil Hassas Yeganeh, and Van Jacobson. 2016. BBR: Congestion-Based Congestion Control: Measuring bottleneck bandwidth and round-trip propagation time. *Queue* 14, 5 (Oct. 2016), 20–53. https://doi.org/10.1145/3012426.3022184

[8] Sadjad Fouladi, John Emmons, Emre Orbay, Catherine Wu, Riad S Wahby, and Keith Winstein. 2018. Salsify: Low-Latency Network Video through Tighter Integration between a Video Codec and a Transport Protocol. In *Proc. of the USENIX Symposium on Networked Systems Design and Implementation (NSDI)*. USENIX Association.

[9] Woo-Hyun Ko, Ushasi Ghosh, Ujwal Dinesha, Raini Wu, Srinivas Shakkottai, and Dinesh Bharadia. 2024. {EdgeRIC}: Empowering Real-time Intelligent Optimization and Control in {NextG} Cellular Networks. 1315–1330. https://www.usenix.org/conference/nsdi24/presentation/ko

[10] Mosolab. 2023. Mosolab Canopy Small Cell. (2023). https://opennetworking.org/products/moso-canopy-5g-indoor-small-cell/

[11] ShareTechNote. 2023. PDCCH Transmission Process, ShareTechnote. (2023). https://www.sharetechnote.com/html/5G/5G_PDCCH.html#PDCCH_Transport_Process

[12] Kazuki Takeda, Huilin Xu, Taehyoung Kim, Karol Schober, and Xingqin Lin. 2020. Understanding the Heart of the 5G Air Interface: An Overview of Physical Downlink Control Channel for 5G New Radio. *IEEE Communications Standards Magazine* 4, 3 (2020), 22–29. https://doi.org/10.1109/MCOMSTD.001.1900048

[13] Haoran Wan and Kyle Jamieson. 2024. Evolving Mobile Cloud Gaming with 5G Standalone Network Telemetry. (Feb. 2024). https://doi.org/10.48550/arXiv.2402.04454 arXiv:2402.04454 [cs].

[14] Keith Winstein, Anirudh Sivaraman, and Hari Balakrishnan. 2013. Stochastic Forecasts Achieve High Throughput and Low Delay over Cellular Networks. In *Proc. of the USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

[15] Yaxiong Xie, Fan Yi, and Kyle Jamieson. 2020. PBE-CC: Congestion Control via Endpoint-Centric, Physical-Layer Bandwidth Measurements. In *Proc. of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)*. Association for Computing Machinery, New York, NY, USA, 451–464. https://doi.org/10.1145/3387514.3405880