BeamArmor: Seamless Anti-Jamming in 5G Cellular Networks with MIMO Null-steering

Frederik Jonathan Zumegen[1,2], Ish Kumar Jain[1], and Dinesh Bharadia[1]

[1]University of California San Diego, CA, USA, [2] ETH Zürich, Switzerland
fzumegen@ethz.ch, ikjain@ucsd.edu, dineshb@ucsd.edu

Abstract

Jamming attacks pose a serious threat to the normal functioning of cellular networks, disrupting communication services and compromising emergency situations. This paper introduces BeamArmor, a practical real-time application to monitor and mitigate jamming attacks in cellular networks. Hosted on a custom RAN controller utilizing the open-source srsRAN stack, it mitigates jamming by deploying beam-nulling techniques with MIMO antennas. This ensures reduced interference impact on desired communication signals. The system ensures real-time operation of the RAN stack by efficiently managing computational resources, meeting the time requirements of the cellular network's physical layer functionalities, and seamlessly integrating with srsRAN. The BeamArmor App is evaluated with over-the-air experiments that demonstrate over 10 dB of SNR improvement in real-time by suppressing the jamming signal through beam-nulling using only two antennas. Our broader vision includes expanding the BeamArmor platform to other real-time MIMO applications, such as advanced beamforming and localization techniques, and integrating it into O-RAN standards.

CCS Concepts

• **Hardware** → **Wireless devices**; • **Networks** → **Physical links**; **Wireless access points, base stations and infrastructure**.

Keywords

Anti-jamming, cellular stack, srsRAN, O-RAN, MIMO, beam-nulling, software-defined radios, RAN controller

ACM Reference Format:
Frederik Jonathan Zumegen[1,2], Ish Kumar Jain[1], and Dinesh Bharadia[1], [1]University of California San Diego, CA, USA, [2] ETH Zürich, Switzerland, fzumegen@ethz.ch, ikjain@ucsd.edu, dineshb@ucsd.edu . 2024. BeamArmor: Seamless Anti-Jamming in 5G Cellular Networks with MIMO Null-steering . In *The 25th International Workshop on Mobile Computing Systems and Applications (HOTMOBILE '24), February 28–29, 2024, San Diego, CA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3638550.3641138

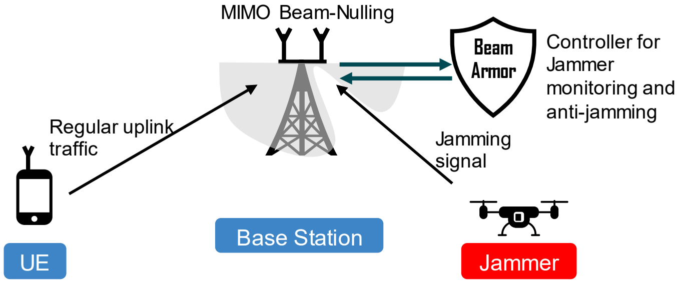


Figure 1: BeamArmor is a controller platform for jammer monitoring and MIMO null-steering anti-jamming solutions implemented with open-source srsRAN 5G cellular stack [4].

1 Introduction

Interference and Jamming pose a significant threat to both cellular networks and military communication devices. It involves intentionally or unintentionally disrupting wireless signals by transmitting powerful signals on the same frequency, rendering the original signals ineffective. In cellular networks, jamming can disrupt the normal operation of mobile phones and other wireless devices that rely on the network, which can lead to dropped calls and loss of data connectivity. As per an estimate, the anti-jamming equipment market was more than 4 Billion in 2023 and is expected to increase by 10% in the next five years [1]. Among many anti-jamming techniques in literature, MIMO-based anti-jamming is attractive because it uses null-steering techniques to selectively suppress or cancel interfering signals while preserving desired signals [2, 3]. By adjusting beamforming weights adaptively, MIMO systems can nullify jamming signals dynamically, reducing their impact on signal quality and maintaining reliable communication.

The threat of jamming is relevant in the current and the next generations of cellular networks because of increased interference at the base station due to high densification for coverage [5, 6], simultaneous utilization of spectrum for cellular and non-terrestrial communication [7] and easy availability of cheap and configurable SDRs like HackRF [8] and bladeRF [9] for malicious jamming attacks. Given the dynamic nature of jamming signals, conventional one-time solutions, such as adjusting antenna orientation during deployment, prove insufficient. Consequently, real-time monitoring of jamming signals and anti-jamming becomes necessary. However, implementing real-time and seamless jammer monitoring and nulling techniques in operational cellular networks is challenging due to limited computation resources and strict deadlines for core PHY layer functionalities. Advanced anti-jamming techniques are computationally heavy and may break the tight time budget of RANs [3, 10]. To enable real-time monitoring, it is necessary to

[2]Frederik Jonathan Zumegen conducted this research while visiting the University of California San Diego.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

HOTMOBILE '24, February 28–29, 2024, San Diego, CA, USA
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0497-0/24/02…$15.00
https://doi.org/10.1145/3638550.3641138

decouple core RAN functions from non-core functions like anti-jamming. The O-RAN initiative aims to disaggregate and virtualize RAN components, allowing jammer monitoring and nulling to be implemented outside a RAN in a machine called RAN Intelligent Controller (RIC) [11].

We present BeamArmor, a practical real-time controller framework for monitoring and nulling jamming attacks in cellular networks. It is built on the open source RAN platform srsRAN as shown in Figure 1. We consider uplink (UL) traffic from srsUE to srsenb (base station) and a jammer that tries to jam the receiver at the base station. BeamArmor is a system for monitoring the presence of a jammer, estimating the jammer's channel parameters, and implementing null-beamforming towards the jammer in real time without compromising the communication link with the genuine user. We address the following challenges while building BeamArmor.

The key challenge for BeamArmor is to provide real-time monitoring and nulling in a tight latency budget while maintaining the core functionalities of the RAN. One effective approach is to deploy the BeamArmor on the RAN controller with near-real-time processing (10 ms to 1 sec) [11]. However, many RAN controllers such as Janus [10] are proprietary and not supported by srsRAN. Although FlexRIC [12] and EdgeRIC [13] are srsRAN compatible, they have limitations in supporting per-antenna channel exposure necessary for MIMO applications. To address this, we built a specialized RAN controller for MIMO applications. We create specific interfaces (called hooks) using the ZeroMQ [14] message passing between the RAN and the BeamArmor controller to frequently exchange bi-directional information relevant to hosted applications. The choice of the ZeroMQ publish/subscriber messaging pattern emerged as the optimal design decision, ensuring minimal impact on the timely execution of PHY layer processes.

The next challenge is to modify srsRAN and extract key information from the RAN that would be useful for MIMO applications Extracting too little information may reflect low accuracy, and extracting too much information may break the real-time nature. To address this issue, we identified specific locations in the srsRAN codebase that provide data relevant to MIMO applications, such as per-antenna IQ data. Subsequently, we implemented appropriate downsampling techniques to reduce latency while maintaining high performance. This down-sampled data is used at the controller to allow the applications to apply their MIMO-based controlling and monitoring. For the BeamArmor App's anti-jamming, the beam nulling has to be applied to the incoming UL traffic in real-time. Therefore, we provide additional hooks in the RAN stack to receive the beam-nulling control information from our controller.

Finally, we perform over-the-air experiments in a large conference room at 2.4 GHz ISM band with an end-end cellular stack running in real-time. Our setup consists of srsenb, srsue, and a jammer device implemented with USRP X300 SDRs. We characterize the impact of a wideband and narrowband jammer with varying power levels on the genuine communication link in terms of SINR (signal-to-interference and noise ratio), BLER (block error rate), and throughput metrics. We show that even with two antennas in srsRAN, effective beam nulling can mitigate the harmful effect of jamming with 10 dB of nulling, thus proving the practicality of our scheme. We believe our open-source controller has a broad impact in the research community to develop and implement more advanced MIMO beamforming techniques in real-time[1].

We summarize our contributions as follows:

- Building an open-source controller for MIMO applications such as jammer nulling.
- Demonstrating anti-jamming with full-stack srsRAN and over-the-air implementation in real environments.
- Evaluating narrowband and wideband jamming scenarios showcasing 10 dB of jammer nulling.
- The open source artifacts for BeamArmor are available at https://wcsng.ucsd.edu/beamarmor and a demo at [15].

2 MIMO null-steering model for jammer mitigation

This article discusses two jamming scenarios: narrowband jamming on a single frequency, typically the UL center frequency, and wideband jamming using random data as Orthogonal Frequency Division Multiplex (OFDM) symbols. These jammers fall into the category of regular jammers. They do not follow any MAC layer protocol but instead inject the wireless channel with random signals transmitted on the carrier frequency of the UL traffic. The intention of the jamming device is to cause powerful interference, which acts as noise added to the legitimate signals and thus degrades the SINR (signal-to-interference and noise ratio) of the UL traffic, such that the BLER increases and the throughput of the cellular network drops significantly.

We consider two antenna base stations, as supported by srsRAN[2], and show that even two antennas are enough to create sufficiently wide nulls in the wave-front pattern. Increasing the number of antennas would create a larger number of nulls that could also be controlled to be of wider angle.

Our anti-jamming application controls the beamforming pattern in such a way that, ideally, zero signal power is received from the angle at which the jamming source is present to free the UL data from the jammer influence. To set the receiver beamforming pattern, we apply a weight α to the vector of received IQ samples y_1 and y_2 received by the first and second antenna of the radio front end, respectively (equation 1). We divide by the term $\sqrt{(1+\alpha^2)}$ to account for the signal power amplification resulting from applying α. Subsequently, y^* is passed to the PHY layer processing steps that follow the reception of raw IQ samples.

$$y^* = (y_1 + \alpha y_2)/\sqrt{(1+\alpha^2)} \tag{1}$$

where α resides in the time domain and is applied to all subcarrier frequencies equally, establishing the assumption of a frequency-flat channel. We compute the scalar factor α from the same objects y_1 and y_2, populated by IQ samples from the current or a prior Transmission Time Interval (TTI). α is computed from IQ samples of TTIs that do not have any users transmitting in UL. Additionally, the assumption is made that within those particular TTIs, all received signal power originates from the jammer source. Therefore, we compute α as a closed-form solution, where α is the factor that results in the combined signal power to equal zero (equation 2).

$$|y_1 + \alpha y_2|^2 = 0 \tag{2}$$

[1] Artifact link https://wcsng.ucsd.edu/beamarmor.

[2] The new version of srsRAN released in Sep 2023 supports 4 antennas

This is a linear least square problem that can be solved in a computationally efficient way. Also, this method can be extended to a large N antenna array using a $N-1$-sized α vector using standard null-steering techniques [16]. Our method does not explicitly yield the angle at which the jammer is positioned to the base station. However, when applying the computed α to the UL IQ samples (equation 1), a null in the waveform pattern will be directed towards the jammer source, given our assumptions.

If the user position and jammer position are sufficiently wide apart in angle, which we assume to be reasonably likely, the user traffic is not affected by the nulling. Our null-steering method applies null-steering to the entire frequency band of the UL traffic by being a scalar factor in the time domain. While this is an imprecise method to mitigate wideband interference, it is nonetheless a computationally light implementation.

3 BeamArmor Design

3.1 Practical, real-time, and O-RAN driven RAN controller for BeamArmor

The BeamArmor applications are driven by data we collect from the cellular RAN through our custom RAN controller, which will be described in this subsection. Through collecting IQ sample streams from the active RX antennas, our platform enables not only null-steering for jammer mitigation but also other MIMO related applications. We built the RAN controller on top of the end-to-end software solution of a cellular stack, srsRAN, aiming at making our platform open-source. The controller uses one common interface realized through the ZeroMQ messaging library to exchange the IQ sample data in one direction and control information in the other. In our setup, the RAN controller is hosted on the same machine as the srsRAN base station application and a transport layer link between the two processes is created over a shared socket.

To establish O-RAN's principle of desegregation of applications and RAN, the priority lies in providing a communication architecture between the cellular stack and the RAN controller. Figure 2 visualizes the operation of this communication with its relevant functional blocks. We chose to use the popular messaging library ZeroMQ [14] (ZMQ) to create two local communication links, although a link across separate machines in a network could be accommodated as well. To comply with the fine-grained clock of the physical (PHY) layer operations in the cellular stack, the outgoing IQ data and incoming control information must not interfere with the timely operation of the PHY layer. The ZMQ publish/subscriber messaging pattern emerged as the best design choice to meet this requirement.

Sufficiently accurate tracking of jamming activity required us to develop near-real-time control capability. In the process of creating the controller for BeamArmor, we have therefore refined the message data structures and their size sent via the ZMQ interface between the controller and RAN stack, so that the RAN can be probed for IQ data sufficiently frequently. In section 4.3, we evaluated various down-sampling rates for the IQ data at a RAN-probing periodicity of every 10 milliseconds.

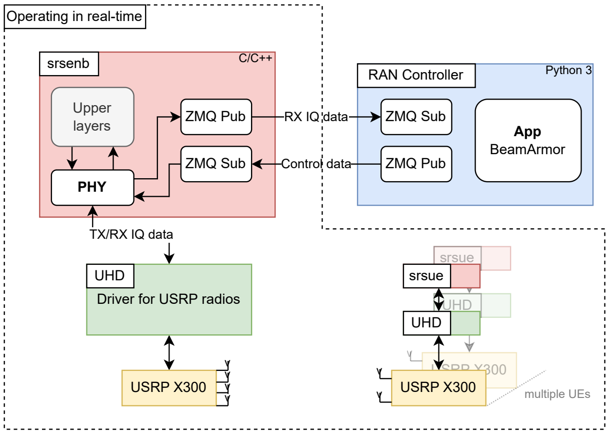


Figure 2: Core functional blocks of our RAN controller for BeamArmor in interaction with the srsenb application and the USRP radio peripheral.

3.2 BeamArmor application for jammer monitoring and nulling

The received IQ data handled by the RAN controller allows us to observe signal power across the UL spectrum and monitor SINR. During dedicated UL idle periods, i.e. users are not transmitting, peaks in received power and drops in UL SINR indicate UL interference that can be linked to jamming activity. Upon detecting jammer activity, we compute the beam-forming weight α from the received IQ data for null-steering. The estimated α is passed as control information to the srsenb using the ZMQ interface to apply beam-nulling with two antenna streams in real-time and successfully reduce the effects of jamming in the UL communication link between the base station and attached users.

In the process of this work, we evaluated applying null-steering to the PHY layer channels PUSCH and PUCCH separately. However, this approach revealed itself to be unreasonably tedious, as srsRAN does not support the PUSCH and PUCCH processing of multiple receiver channels in UL. The current version of srsRAN (Oct 2023) only supports DL 2 antenna MIMO with Alamounti codes, while UL, supports only SISO links. As a result, a separate PHY layer processing pipeline to process a second antenna port's input would be necessary to implement null-steering on the PHY channels.

Rather, we implemented a low-overhead solution in srsRAN to deploy null-steering: The unprocessed IQ data is weighed and added together in the time domain before it is passed to any further UL processing, like transformation to the time-frequency grid. Inside the PHY layer sub-process of srsRAN, the vector of RX IQ samples, denoted by $y1$ and $y2$ (antenna port 1 and 2 respectively), are processed as follows: Instead of passing the memory address of $y1$ to the UL processing, as it is done by default by srsRAN, our modification writes $y^* = (y_1 + \alpha * y_2)/\sqrt{1+\alpha^2}$ to the same address, and all further processing is done to this new data y^*. This ensures the nulling of the jammer signal when both UE and jammer are present together and ensures unobstructed communication with the UE despite the jamming signal.

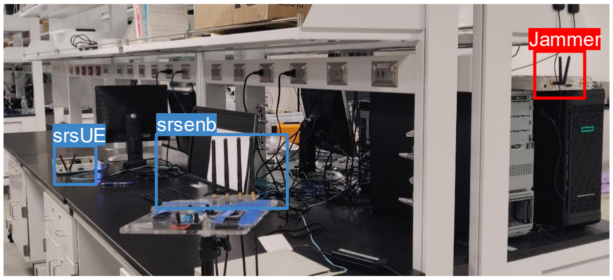
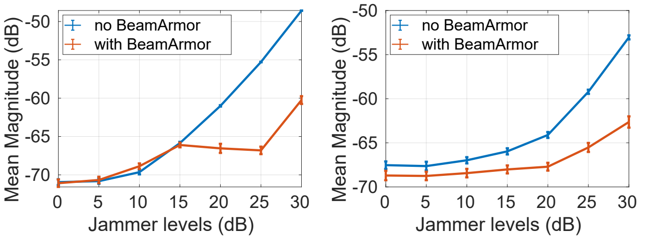


Figure 3: Experiment set up with the active elements (srsenb, srsUE, and jammer) in a lab environment. We tested with 3 different jammer locations.



(a) Single-Tone jammer **(b) 5 MHz Wideband jammer**

Figure 4: `BeamArmor`'s cancellation abilities. We present the mean received signal strength computed from received signal y in the form of $|y|^2$ as jammer power increases from 0 to 30 dBm. The red curve demonstrates how `BeamArmor`'s null-steering decreases received jammer signal power.

4 Over-the-air Experiments

We build an over-the-air setup (Figure 3) to validate our jamming monitoring and nulling application. We use three SDR USRP X300 as srsenb, srsue, and jammer. The RAN controller runs on the same server as srsenb through a ZMQ-based transport socket.

4.1 Monitoring jammer interference with `BeamArmor`

We evaluate `BeamArmor`'s jammer monitoring with varying jammer power as discussed in Section 3.2. Inside the `BeamArmor` App (see Fig. 2), the received IQ data $y1$ and $y2$ can be processed to monitor the spectrum of the UL communication link in terms of received signal power. Table 1 shows the interfering effect of a 5 MHz wideband jammer by listing the SINR metric for various jammer power levels. Most notably in this table, the SINR suffers a reduction of 12 dB between a wideband jammer transmitting at 0 dBm and 30 dBm, respectively. The srsenb application reports UL SINR by default.

Jammer Power (dBm)	UL SINR (dB)
0	14.18
5	13.62
10	13.36
15	11.81
20	9.30
25	5.78
30	2.85

Table 1: UL SINR vs. increasing jammer TX power.

4.2 Mitigating jammer with `BeamArmor`

First, we present `BeamArmor`'s capability to cancel received signals from a certain direction, such as those from a jammer source. Figures 4a and 4b show how well `BeamArmor` can suppress signal power in the case of a single-tone source (single-tone jammer) and a 5 MHz random OFDM signal source (5 MHz wideband jammer). For a jammer source transmitting at 30 dBm gain, our anti-jamming solution achieves a 10 dB cancellation compared to the default base station operation with no active anti-jamming solution. The unexpected observation of baseline cancellation capability for the measurements belonging to a single-tone jammer between 0 dBm and 15 dBm transmit power could be caused by inaccurate null-steering factors α. As a reminder, our null-steering method assumes all signal power to be from the jammer source during the computation of α. In practice, at low jammer transmit powers, the received signal power at the base station will have relatively large parts of signal power originating from other sources than the jammer, resulting in a noisy value for α. Furthermore, the evaluation of cancellation capability would be more comprehensive if various jammer positions were measured, as opposed to one position, as done for Figure 4a and 4b.

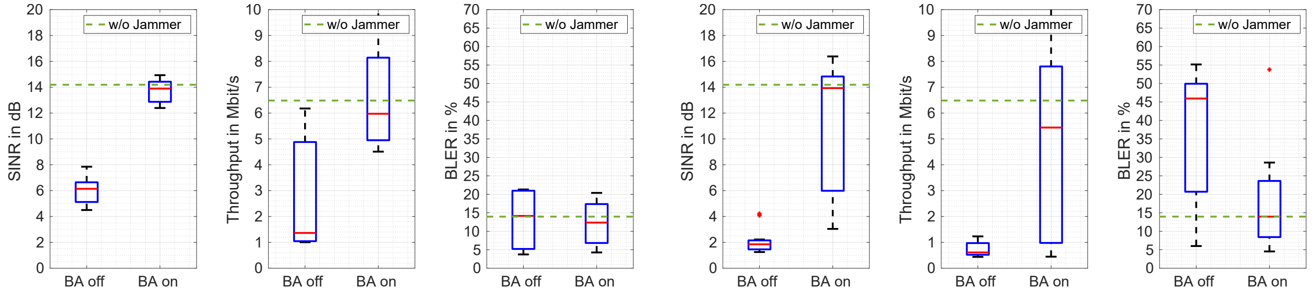
To evaluate the final performance of the RAN with `BeamArmor`'s anti-jamming active, we conducted measurement runs as follows:

(1) Turn srsenb and jammer on. Compute steering factor α.
(2) Stop computing α and start applying α to UL processing at eNB side. This activates the anti-jamming.
(3) Attach UE to eNB.
(4) Start UL traffic from UE to eNB (10 Mbit/s UDP). Observe metrics.

In total, we evaluated our application from three different jammer positions, where each position's unique feature is the angle of the position to the position of the eNB, while the distance between the jammer and eNB remained at about 1 meter. As with our cancellation experiments, we evaluated `BeamArmor`'s anti-jamming against a single-tone jammer and a wideband OFDM jammer.

The performance of our anti-jamming application was evaluated by comparing SINR, BLER, and throughput of the UL traffic received at the base station side. The communicated data is transmitted in blocks of fixed size, and BLER provides an indication of how reliable a communication link is. Figure 5 shows our results, where each boxplot bar contains 15 data points - the mean values of five individual measurement runs per each of the three jammer positions. As a benchmark, we added the mean of five measurements containing neither a jammer influence nor the application of `BeamArmor`'s anti-jamming (dotted green line in Figure 5).

We conclude as the main takeaway: For all metrics and almost all combinations, our null-steering enabled anti-jamming solution provides on average (median) nearly benchmark performance if the jammer source is in close vicinity of the base station and therefore, the line-of-sight (LoS) path is very dominant. One exception is our measurements for BLER in the case of a single-tone jammer. Generally, the impact of a single-tone jammer is always weaker than a wideband jammer that interferes with several subcarrier frequencies. As mentioned in section 2, our null-steering method



(a) Single-Tone jammer

(b) 5 MHz Wideband jammer

Figure 5: Metrics SINR, throughput, and BLER for two jamming scenarios: (a) Single Tone jammer and (b) 5 MHz Wideband jammer. Subsequently, both scenarios with and without `BeamArmor`'s anti-jamming solution (BA on/off). The green dotted line shows the ground truth scenario without (w/o) any jammer present. The red line represents the median value of one boxplot.

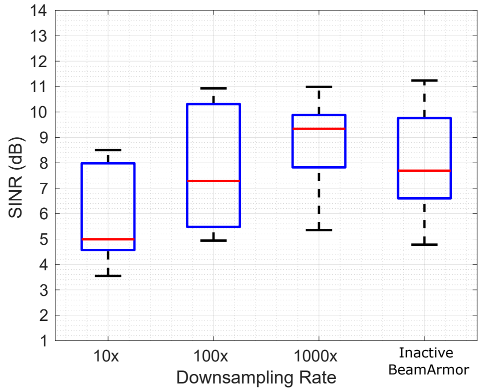


Figure 6: UL SINR during active `BeamArmor` controller communication at various down-sampling rates and at a fixed periodicity of every 10 TTI. UL SINR during an inactive `BeamArmor` controller serves as a benchmark performance.

applies a scalar factor to all subcarriers. As a result, our method does not account for varying interference levels for jamming-affected subcarriers. This circumstance can serve as an explanation for the large variance observed in our evaluation of `BeamArmor` in Figure 5b.

4.3 Platform evaluation

We decided that observing the UL traffic quality in the form of SINR (see Figure 6) would be sufficient to validate the functionality and performance of our RAN controller platform. In our measurements, we varied the rate at which we downsample y_1 and y_2 prior to sending, and fixed a send-periodicity of every 10 TTI. We compare the SINR metric with the case of "Inactive `BeamArmor` ", which is equivalent to infinite downsampling (no data is sent to the controller).

The result proves the functionality of `BeamArmor`'s controller concept and does so without damage to UL traffic quality. Without downsampling, the RAN performance is affected, as evident from the low SINR of a median of 5 dB compared to the benchmark SINR of 7.5 dB. In our measurements of six runs per downsampling rate, 1000x downsampling performance is as good as the benchmark measurement. Thus, the RAN controller platform, deployed alongside an end-end RAN, is capable of providing PHY layer data in near real-time and enables MIMO applications such as anti-jamming.

5 Related Work

The growing adoption of O-RAN standards has sparked a collective interest in RAN controller development across both industry and academia. This work advances the concept by focusing on the design of controllers and the development of applications tailored for MIMO applications.

■ **Controller platforms:** Janus [10] and FlexRIC [12] offer analytics and control capabilities for RANs in compliance with the O-RAN architecture. Janus [10] provides real-time control and inference over RAN, including support for streaming raw IQ samples to the controller. However, Janus [10] is built in an industry setting with a proprietary RAN stack, which is not compatible with open-source stacks such as srsRAN [4]. Nonetheless, our `BeamArmor` anti-jamming application can be demonstrated on Janus when this tool is available with open-source RANs such as srsRAN or Open-Air Interface [17] in the future.

■ **Testbeds for anti-jamming:** The study by [18] focuses on investigating the effects of jamming on the UL channel using a testbed powered by srsLTE and USRPs. However, it is important to note that the jammer is connected to the system using wired connections rather than a wireless link. Additionally, the study does not incorporate any anti-jamming mechanisms within the srsLTE framework. In [19], the researchers implemented jamming in the LTE UL using the Rohde & Schwarz radio communication tester CMW500 and [2] uses USRPs. They employed a signal generator and spectrum analyzer with a wired setup to investigate the power levels and EVM (Error Vector Magnitude) of the jammer, focusing on the PHY layer without considering the impact on the full cellular stack. Other testbeds are developed for WiFi [20, 21] or millimeter-wave devices [22]. In contrast, we study anti-jamming within a cellular full-stack srsRAN with wireless scenarios in real-time.

■ **Theoretical works on anti-jamming:** Several theoretical works on anti-jamming consider large antennas Massive MIMO systems [23–30] For instance, the research in [23] develops anti-jamming techniques for massive MIMO, utilizing random matrix theory. However, it should be noted that these advanced techniques are not required in small-scale MIMO systems that are commonly deployed in cellular stacks.

6 Limitations and Future Work

BeamArmor demonstrates a real-time MIMO application for anti-jamming, offering ample opportunities for future expansion and development.

■ **Advanced jammers:** BeamArmor currently targets interference originating from a single LoS jammer due to the system utilizing only two antennas for UL reception. With the continuous evolution of open-source cellular software stacks, we envision an upgrade to BeamArmor with more than 2 antennas to handle multiple jammers or strong multi-paths NLoS scenarios. While we did not evaluate moving or duty-cycled jammer sources, BeamArmor could be operated such that the null-steering is continuously re-set towards a new jammer location. In any case, this is limited to the frequency at which the steering factor α can be computed, which is, at maximum, every TTI or every 1 ms.

■ **Frequency-selective Channel:** We assumed a frequency-flat channel resulting from a strong LoS component from a jammer in close proximity to the base station. To account for frequency-selective channel conditions, BeamArmor can be extended such that the null-steering factor α is computed for each subcarrier.

■ **Downlink Jammer:** We implemented BeamArmor for the UL traffic at the base station. Jammer interference on the DL at the user device would still harm or break a full duplex communication link. While some use cases of cellular communication might only depend on UL traffic, BeamArmor's null-steering technique could be implemented along the PHY layer processing of UEs (provided they are multi-antenna receivers) to provide jammer mitigation on the DL.

■ **O-RAN specifications:** While the controller implementation is motivated to comply with the O-RAN specifications, it remains an open piece of work to refine the utilized ZMQ interface to match the O-RAN specifications exactly.

7 Conclusion and Outlook

With BeamArmor, we present a null-steering-enabled approach to mitigate the influence of jammer interference. The application, as well as the controller functioning as the host, are evaluated in over-the-air experiments for their viability. The possibility of utilizing the BeamArmor controller platform to demonstrate additional, innovative MIMO applications such as beamforming, multiplexing, antenna selection, user selection, power conservation, channel prediction, localization, and tracking based on recorded IQ samples poses a promising direction to extend this work.

8 Acknowledgement

This research was supported in part by the NSF grant 2030245 and the U.S. Department of Defense N66001-23-F-0484 P00001. We thank the anonymous reviewers and Shephard for providing insightful feedback and the members of WCSNG lab, UC San Diego for their feedback throughout the process.

References

[1] Anti-jamming market size & share analysis - growth trends & forecasts (2023 - 2028). https://www.mordorintelligence.com/industry-reports/anti-jamming-equipment-market-growth, 2023.

[2] Qiben Yan, Huacheng Zeng, Tingting Jiang, Ming Li, Wenjing Lou, and Y Thomas Hou. MIMO-based jamming resilient communication in wireless networks. In *IEEE INFOCOM*, pages 2697–2706. IEEE, 2014.

[3] Tan Tai Do, Emil Björnson, Erik G Larsson, and S Mohammad Razavizadeh. Jamming-resistant receivers for the massive MIMO uplink. *IEEE Transactions on Information Forensics and Security*, 13(1), 2017.

[4] srsRAN. srsran: Open source 4g/5g software radio access network. https://github.com/srsran/srsRAN, 2023.

[5] Agrim Gupta, Ish Jain, and Dinesh Bharadia. Multiple smaller base stations are greener than a single powerful one: Densification of wireless cellular networks. In *1st Workshop on Sustainable Computer Systems Design and Implementation (HotCarbon)*, 2022.

[6] Mahmoud Kamel, Walaa Hamouda, and Amr Youssef. Ultra-dense networks: A survey. *IEEE Communications surveys & tutorials*, 18(4):2522–2545, 2016.

[7] IEEE Spectrum. Starlink and other LEO constellations face a new set of security risks. https://spectrum.ieee.org/satellite-jamming, May 2023.

[8] Hackrf one. https://greatscottgadgets.com/hackrf/one/, 2023.

[9] Bladerf. https://www.nuand.com/bladerf-1/, 2023.

[10] Xenofon Foukas, Bozidar Radunovic, Matthew Balkwill, and Zhihua Lai. Taking 5G RAN analytics and control to a new level. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, pages 1–16, 2023.

[11] Michele Polese, Leonardo Bonati, Salvatore D'Oro, Stefano Basagni, and Tommaso Melodia. Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges. *IEEE Communications Surveys & Tutorials*, 2023.

[12] Robert Schmidt, Mikel Irazabal, and Navid Nikaein. Flexric: An sdk for next-generation sd-rans. In *Proceedings of the 17th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '21, page 411–425, New York, NY, USA, 2021. ACM.

[13] Woo-Hyun Ko, Ujwal Dinesha, Ushasi Ghosh, Srinivas Shakkottai, Dinesh Bharadia, and Raini Wu. Edgeric: Empowering realtime intelligent optimization and control in nextg networks. *arXiv preprint arXiv:2304.11199*, 2023.

[14] ZeroMQ Documentation. http://zeromq.org. Accessed May 10, 2023.

[15] Frederik Jonathan Zumegen, Ish Kumar Jain, and Dinesh Bharadia. Beamarmor demo: Anti-jamming system in cellular networks with srsran software radios. In *MILCOM 2023-2023 IEEE Military Communications Conference (MILCOM)*, pages 245–246. IEEE, 2023.

[16] Harry L Van Trees. *Optimum array processing: Part IV of detection, estimation, and modulation theory*. John Wiley & Sons, 2002.

[17] OAI. Open Air Interface 5G Radio Access Network Project. https://openairinterface.org/oai-5g-ran-project/, 2023.

[18] Felix Girke, Fabian Kurtz, Nils Dorsch, and Christian Wietfeld. Towards resilient 5G: Lessons learned from experimental evaluations of LTE uplink jamming. In *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2019.

[19] Grecia Romero, Virginie Deniau, and Olivier Stienne. LTE Physical layer vulnerability test to different types of jamming signals. In *2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE*, pages 1138–1143. IEEE, 2019.

[20] Suzan Bayhan, Piotr Gawłowicz, Anatolij Zubow, and Adam Wolisz. Null-while-talk: Interference nulling for improved inter-technology coexistence in lte-u and wifi networks. *Pervasive and Mobile Computing*, 56:71–87, 2019.

[21] Shyamnath Gollakota, Samuel David Perli, and Dina Katabi. Interference alignment and cancellation. In *Proceedings of the ACM SIGCOMM 2009 conference on Data communication*, pages 159–170, 2009.

[22] Sohrab Madani, Suraj Jog, Jesus O. Lacruz, Joerg Widmer, and Haitham Hassanieh. Practical null steering in millimeter wave networks. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 903–921. USENIX Association, April 2021.

[23] Julia Vinogradova, Emil Björnson, and Erik G Larsson. Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory. In *2016 IEEE 17th International Workshop on SPAWC*, pages 1–5. IEEE, 2016.

[24] Youness Arjoune and Saleh Faruque. Smart jamming attacks in 5G new radio: A review. In *2020 10th annual computing and communication workshop and conference (CCWC)*, pages 1010–1015. IEEE, 2020.

[25] Farhan M Aziz, Jeff S Shamma, and Gordon L Stüber. Jammer-type estimation in LTE with a smart jammer repeated game. *IEEE Transactions on Vehicular Technology*, 66(8):7422–7431, 2017.

[26] Jose A Torres, Richard M Davis, J David R Kramer, and Ronald L Fante. Efficient wideband jammer nulling when using stretch processing. *IEEE Transactions on Aerospace and Electronic Systems*, 36(4):1167–1178, 2000.

[27] Garret Okamoto. Jammer nulling via low complexity blind beamforming algorithm. In *2007 IEEE Antennas and Propagation Society International Symposium*, pages 25–28. IEEE, 2007.

[28] Shengbo Xu, Weiyang Xu, Cunhua Pan, and Maged Elkashlan. Detection of jamming attack in non-coherent massive simo systems. *IEEE Transactions on Information Forensics and Security*, 14(9):2387–2399, 2019.

[29] Gian Marti, Torben Kölle, and Christoph Studer. Mitigating Smart Jammers in Multi-User MIMO. *IEEE Transactions on Signal Processing*, 71:756–771, 2023.

[30] Hossein Akhlaghpasand, Emil Björnson, and S Mohammad Razavizadeh. Jamming suppression in massive MIMO systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(1):182–186, 2019.