NIST Internal Report
NIST IR 8560

# Towards Adversary-Resilient Interference Management in O-RAN: Requirements and Gap Analysis

Sneihil Gopal
Wesley D. Garey
Richard A. Rouil
Sridhar Kowdley

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8560

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

**NIST Internal Report**
**NIST IR 8560**

# Towards Adversary-Resilient Interference Management in O-RAN: Requirements and Gap Analysis


Sneihil Gopal
*PREP Associate, Wireless Networks Division*
*Communication Technology Laboratory*
*Georgetown University, Washington, DC*

Wesley D. Garey
Richard A. Rouil
*Wireless Networks Division*
*Communication Technology Laboratory*

Sridhar Kowdley
*Department of Homeland Security Science & Technology Directorate*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8560

January 2025

U.S. Department of Commerce
*Jeremy Pelter, Acting Secretary of Commerce*

National Institute of Standards and Technology
*Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director*

**Publication History**
Approved by the NIST Editorial Review Board on 2025-01-23

**How to cite this NIST Technical Series Publication:**
Gopal S, Garey WD, Rouil RA, Kowdley S (2025) Towards Adversary-Resilient Interference Management in O-RAN: Requirements and Gap Analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8560. https://doi.org/10.6028/NIST.IR.8560

**Author ORCID iDs**
Sneihil Gopal: 0000-0001-8843-4839
Wesley D. Garey: 0000-0003-1572-8208
Richard A. Rouil: 0000-0003-0387-0880
Sridhar Kowdley:

**Contact Information**
richard.rouil@nist.gov

8560
January2025

**Abstract**

The Open Radio Access Network (RAN) (O-RAN) Alliance seeks to establish a more open, intelligent, and flexible Radio Access Network (RAN) architecture for Fourth Generation (4G), Fifth Generation (5G), and future Sixth Generation (6G) networks. By leveraging O-RAN's standardized ecosystem, along with Artificial Intelligence (AI) and Machine Learning (ML) technologies, network operators can address complex challenges like interference management in 4G Long Term Evolution (LTE) and 5G New Radio (NR), with future applicability to 6G. A key innovation within O-RAN is its potential for enhanced interference management, particularly through the "Interference Detection, Prediction, and Optimization" use case, which builds on legacy Inter-Cell Interference Coordination (ICIC) techniques from LTE. This promises more granular control and real-time optimization in coordinated environments.

However, public safety entities such as the U.S. Department of Homeland Security (DHS) and Department of Defense (DoD) face unique interference challenges, including uncoordinated interference from external or malicious sources. This paper examines state-of-the-art interference management techniques in cellular networks and explores whether O-RAN's current capabilities can effectively manage interference in coordinated scenarios, as well as whether they can be extended to address non-ideal situations involving uncoordinated entities, faulty equipment, or malicious actors. Through a gap analysis, we compare existing O-RAN specifications with real-world interference scenarios. Our findings underscore the need for enhanced O-RAN-based solutions to manage diverse interference cases, critical for both commercial and public safety networks.

**Keywords**

Open Radio Access Network (O-RAN); Radio Access Networks (RAN); Interference Management; 5G New Radio (NR); 4G Long Term Evolution (LTE); 6G Networks; Public Safety Networks; Adversarial Interference; Inter-Cell Interference Coordination (ICIC); Diverse Interference.

# Table of Contents

# List of Tables



# List of Figures

## Acknowledgments

This work is partially funded by the Department of Homeland Security's Science and Technology Directorate (S&T).

## List of Abbreviations

| | |
|---|---|
| **2G** | Second Generation |
| **3G** | Third Generation |
| **4G** | Fourth Generation |
| **5G** | Fifth Generation |
| **6G** | Sixth Generation |
| **3GPP** | Third Generation Partnership Project |
| **5QI** | 5G Quality of Service (QoS) Identifier |
| **ABS** | Almost Blank Subframe |
| **ACI** | Adjacent Channel Interference |
| **AI** | Artificial Intelligence |
| **AP** | Application Protocol |
| **API** | Application Programming Interface |
| **BLER** | Block Error Rate |
| **BS** | Base Station |
| **BWP** | Bandwidth Part |
| **CA** | Carrier Aggregation |
| **CCC** | Cell Configuration and Control |
| **CCI** | Co-Channel Interference |
| **CN** | Core Network |
| **CoMP** | Coordinated Multipoint |
| **CLI** | Cross-link Interference |
| **CRE** | Cell Range Expansion |
| **CQI** | Channel Quality Indicator |
| **CSI** | Channel State Information |
| **CSI-RS** | Channel State Information Reference Signal |
| **CSI-IM** | Channel State Information Interference Management |
| **CRS** | Cell-specific Reference Signal |
| **D2D** | Device-to-Device |
| **DHS** | Department of Homeland Security |
| **DoD** | Department of Defense |
| **DL** | Downlink |
| **DMRS** | DeModulation Reference Signal |
| **DSS** | Dynamic Spectrum Sharing |
| **E2SM** | E2 SM |
| **E2AP** | E2 Application Protocol |
| **eICIC** | Enhanced ICIC |
| **eIMTA** | Enhanced Interference Mitigation and Traffic Adaptation |
| **EPON** | Ethernet Passive Optical Network |
| **eMBB** | enhanced Mobile Broadband |
| **FD** | Full Duplex |
| **FDD** | Frequency Division Duplex |
| **FFR** | Fractional Frequency Reuse |
| **gNB** | Next Generation Node B |
| **GSM** | Global System for Mobile Communications |
| **HARQ** | Hybrid Automatic Repeat Request |
| **HetNets** | Heterogeneous Networks |
| **ICI** | Inter-Cell Interference |
| **ICIC** | Inter-Cell Interference Coordination |
| **IE** | Information Element |

| | |
|---|---|
| **INI** | Inter-Numerology Interference |
| **IoT** | Internet of Things |
| **ITU** | International Telecommunication Union |
| **KPIs** | Key Performance Indicators |
| **KPM** | Key Performance Metric |
| **LTE** | Long Term Evolution |
| **LTE-A** | LTE-Advanced |
| **MBS** | macro base station |
| **MCS** | Modulation and Coding Scheme |
| **MIMO** | Multiple-Input Multiple-Output |
| **mmWave** | millimeter waves |
| **ML** | Machine Learning |
| **MTC** | Machine-Type Communication |
| **mMTC** | massive Machine-Type Communication (MTC) |
| **MUI** | Multi-User Interference |
| **NES** | Newtork Energy Savings |
| **NTNs** | Non-Terrestrial Networks |
| **Near-RT RIC** | Near-Real-Time RAN Intelligent Controller (RIC) |
| **Non-RT RIC** | Non-Real-Time RIC |
| **NOMA** | Non-Orthogonal Multiple Access |
| **NR** | New Radio |
| **NZP** | Non Zero Power |
| **O-Cloud** | O-RAN Cloud |
| **O-CU-CP** | O-RAN Central Unit - Control Plan |
| **O-CU-UP** | O-RAN Central Unit - User Plane |
| **O-DU** | O-RAN Distributed Unit |
| **OFDM** | Orthogonal Frequency Division Multiplexing |
| **O-RAN** | Open RAN |
| **PDSCH** | Physical Downlink Shared Channel |
| **PMI** | Precoding Matrix Indicators |
| **PRB** | Physical Resource Block |
| **PUCCH** | Physical Uplink Control Channel |
| **QoS** | Quality of Service |
| **QoE** | Quality of Experience |
| **RAN** | Radio Access Network |
| **RC** | RAN Control |
| **REST** | REpresentational State Transfer |
| **RI** | Remote Interference |
| **RIC** | RAN Intelligent Controller |
| **RIM** | Remote Interference Management |
| **RLC** | Radio Link Control |
| **RN** | Relay Nodes |
| **RRC** | Radio Resource Control |
| **RRM** | Resource Radio Management |
| **RS** | Reference Signals |
| **RSRP** | Reference Signal Received Power |
| **RSSI** | Received Signal Strength Indicator |
| **SDMA** | Space Division Multiple Access |
| **SI** | Self Interference |
| **SIC** | Successive Interference Cancellation |
| **SINR** | Signal to Interference and Noise Ratio |

| | |
|---|---|
| **SM** | Service Model |
| **SMO** | Service Management and Orchestration |
| **SLA** | Slice Level Agreement |
| **SRS** | Sounding Reference Signals |
| **SSB** | Synchronization Signal Block |
| **TDD** | Time Division Duplex |
| **THz** | Terahertz |
| **UDN** | Ultra-Dense Networks |
| **UE** | User Equipment |
| **UL** | Uplink |
| **URLLC** | Ultra-Reliable Low-Latency Communications |
| **WCDMA** | Wideband Code Division Multiple Access |
| **WG1** | Working Group 1 |
| **WG2** | Working Group 2 |
| **WG3** | Working Group 3 |
| **WSDN** | Wireless Software Defined Networking |
| **ZP** | Zero Power |

## 1. Introduction

The transition from Fourth Generation (4G) to Fifth Generation (5G)—and eventually to 5G Advanced and Sixth Generation (6G)—marks a significant shift in network design and capabilities. While 4G focused primarily on improving data rates and coverage, 5G addresses a broader set of requirements such as ultra-low latency, enhanced reliability, and extremely high data rates [1]. To meet these demands, 5G introduces groundbreaking technologies such as the use of higher frequency bands (particularly millimeter waves (mmWave)), massive Multiple-Input Multiple-Output (MIMO), cooperative network using Relay Nodes (RN), Coordinated Multipoint (CoMP), Wireless Software Defined Networking (WSDN), Device-to-Device (D2D) communication, Internet of Things (IoT), Ethernet Passive Optical Network (EPON), Big Data, Mobile Computing, network densification, and dynamic Time Division Duplex (TDD). These advancements offer greater flexibility in managing Uplink (UL) and Downlink (DL) transmissions [2].

5G is designed with high flexibility, enabling it to dynamically adjust to diverse use cases, including massive Machine-Type Communication (MTC) (mMTC) and Ultra-Reliable Low-Latency Communications (URLLC), both of which are crucial for mission-critical applications. This flexibility allows 5G to support a diverse set of QoS requirements, utilizing low, medium, and high-frequency bands across licensed and unlicensed spectrums with Carrier Aggregation (CA). It also incorporates multiple numerologies and flexible waveforms, creating a multi-tiered Heterogeneous Network (HetNet) architecture where macro and small cells operate in close proximity and often reuse the same frequency resources. Additionally, 5G supports both TDD and Frequency Division Duplex (FDD), with Full Duplex (FD) and advanced techniques like massive MIMO and beamforming considered promising solutions for future network optimization.

However, this intrinsic flexibility—while essential for supporting various applications—introduces unprecedented levels of interference. Technologies like D2D communication, multi-layer HetNets, and random device deployments further exacerbate interference, particularly Inter-Cell Interference (ICI). As the deployment of 5G and future networks accelerates, effective interference management becomes increasingly critical to ensure optimal network performance, requiring sophisticated coordination and mitigation strategies to handle the complex interference landscape introduced by 5G.

ICI has been a persistent challenge across all generations of mobile networks. Given the limited spectrum resources, frequency reuse across different cells is unavoidable, making ICI inevitable. In early mobile systems like Second Generation (2G) Global System for Mobile Communications (GSM), basic frequency reuse schemes (e.g., reuse-3 or reuse-7) were sufficient to manage interference, although they compromised spectral efficiency [3]. As networks evolved to Third Generation (3G) systems like Wideband Code Division Multiple Access (WCDMA), power control mechanisms were introduced to handle interference. With the advent of 4G Long Term Evolution (LTE), the adoption of a frequency reuse factor of one led to more severe ICI, particularly for users at the cell edges. This prompted the development of interference coordination techniques like Inter-Cell Interference Coordination (ICIC) and Enhanced ICIC (eICIC), along with approaches like Fractional Frequency Reuse (FFR), to reduce interference and improve performance in heterogeneous networks [4].

The introduction of 5G amplified these ICI challenges. To address these, 5G employs advanced interference mitigation techniques, such as enhanced beamforming with massive MIMO, dynamic spectrum sharing, and resource allocation algorithms driven by Artificial Intelligence (AI) and Machine Learning (ML). These technologies enable real-time interference prediction and management, optimizing network performance even in dense deployment environments.

Looking forward, 5G Advanced and 6G networks will further increase the complexity of interference management, especially with the use of higher frequencies such as Terahertz (THz) waves. The integration of Non-Terrestrial Networks (NTNs), including satellite and aerial systems, will introduce new interference challenges. Future networks will need innovative strategies for flexible resource management, intelligent spectrum sharing, and real-time coordination of resources across both terrestrial and non-terrestrial systems [5].

In this evolving landscape, the Open RAN (O-RAN) Alliance has emerged as a pivotal standards body. Established in 2018, the O-RAN Alliance builds on the work of the Third Generation Partnership Project (3GPP) to foster a more open, intelligent, and flexible Radio Access Network (RAN) architecture for 4G, 5G, and future 6G networks. The O-RAN Alliance has developed a comprehensive set of specifications, which include use cases that outline the expected workflow of fully realized O-RAN systems, the O-RAN architecture that defines the roles and relationships of network entities [6–10], service models (SMs) for monitoring and controlling RAN activities [11–14], and security protocols to ensure safe implementations and deployments [15, 16]. By promoting openness and standardization, the O-RAN Alliance has significantly lowered barriers for vendor participation, enabling third-party application development and the integration of AI/ML solutions for tackling complex network challenges in a more dynamic and reactive environment.

One of the key use cases defined by the O-RAN Alliance is ”Interference Detection and Optimization” [17]. This use case re-envisions how inter-cell interference coordination (ICIC), which was originally introduced in 4G LTE, can be adapted for 5G NR networks. An O-RAN-based ICIC solution offers more granular control and monitoring of resources, enabling a more adaptive and real-time workflow than previous monolithic approaches. Through real-time reports from RAN entities and the dynamic issuance of control commands, O-RAN facilitates network optimization by responding to interference conditions in real time, significantly improving network performance.

Additionally, public safety organizations, such as the Department of Homeland Security (DHS) and Department of Defense (DoD), are interested in interference detection and mitigation, particularly in non-ideal scenarios. These scenarios involve uncoordinated entities that create interference either intentionally, as in the case of malicious actors, or unintentionally, through external sources beyond the control of the network. Examples include interference along border areas where neighboring countries' networks, operating independently, may inadvertently use the same frequencies, as well as external devices that disrupt network operations or faulty and malicious internal devices that cause interference. Given these challenges, we aim to investigate whether the principles outlined in the aforementioned use case of the O-RAN specification [17] can be extended to address these types of interference detection and optimization, which are currently not covered.

In this work, we explore the potential of O-RAN to enhance interference management in 4G, 5G, and future 6G networks. We begin by examining the key concepts behind interference management and how they were applied to cellular networks. Building on this foundation, we investigate how the O-RAN architecture, particularly through its integration of AI/ML models and the RAN Intelligent Controller (RIC), can improve the detection and mitigation of interference in more dynamic and complex network environments. Furthermore, we analyze the use case "Interference Detection and Optimization," as defined by the O-RAN Alliance, and assess its viability in real-world scenarios, such as uncoordinated interference sources and cross-border network deployments. Our findings highlight the increased flexibility and granularity of control that O-RAN introduces, as well as its potential to adapt interference management strategies to meet the evolving needs of mobile networks.

The paper is organized as follows. Section 2 discusses interference management in cellular networks. Section 3 delves into the current state of the O-RAN Alliance standards and specifications, with a focus on relevant use cases. In Section 4, we perform a gap analysis comparing the available O-RAN specifications with real-world requirements, including scenarios in which O-RAN can be utilized for interference detection and optimization. Finally, Section 6 summarizes our findings and conclusions.

## 2. Interference Management in Cellular Networks

Interference management has always been a pivotal component of cellular network design, and its importance has only grown with the evolution from 4G to 5G and the anticipated advancements in 5G Advanced and 6G. While 4G networks primarily focused on boosting data speeds and enhancing coverage, 5G introduces more sophisticated demands such as ultra-low latency, high reliability, and massive data rates. These new requirements, coupled with the adoption of advanced technologies like mmWave, massive MIMO, and network densification, have introduced new layers of complexity in managing interference.

5G is designed to be highly flexible, dynamically adapting to a variety of use cases, including massive MTC and URLLC, which are critical for mission-critical applications. This flexibility, however, introduces new interference challenges, particularly with the increasing deployment of HetNets, where macro cells and small cells coexist in close proximity. The use of diverse technologies, each optimized for different scenarios, has made interference management far more complex than in previous generations. As a result, designing effective ICI management strategies has become a key research area in modern networks.

Interference challenges have persisted throughout all generations of mobile networks. In 2G systems such as GSM, interference was managed through simple frequency reuse schemes (e.g., reuse-3 or reuse-7), which minimized interference by ensuring neighboring cells used distinct frequencies. However, this approach traded off spectral efficiency for reduced interference [3]. In 3G networks like WCDMA, where users shared the same frequency spectrum, power control mechanisms were introduced to address interference. Although power control helped balance transmission power and maintain acceptable signal quality, the growing network traffic increased the complexity of ICI management.

With the arrival of 4G, particularly LTE, mobile network performance took a substantial leap forward. LTE adopted Orthogonal Frequency Division Multiplexing (OFDM), improving spectral efficiency and enabling higher data rates. However, LTE's use of a frequency reuse factor of one—where the same frequencies were reused across all cells—intensified ICI, especially for cell-edge users. To mitigate this, LTE introduced interference coordination techniques, such as fractional frequency reuse (FFR), which divided cells into center and edge regions, assigning orthogonal frequencies to cell-edge users to reduce interference [18].

As LTE advanced to LTE-Advanced (LTE-A), the deployment of HetNets, combining macro cells with smaller cells (e.g., pico and femto cells), further complicated interference management. To address this, eICIC techniques were introduced. These techniques included methods like Almost Blank Subframe (ABS), where macro cells muted transmissions during specific subframes to allow small cells to transmit without interference. CoMP transmission was also introduced to enable multiple base stations to coordinate transmissions and improve performance for cell-edge users [4].

The introduction of 5G has exacerbated ICI challenges. Operating across a wide range of frequencies, including sub-6 GHz and mmWave bands, 5G offers larger bandwidths but is more prone to interference. Moreover, 5G's ultra-dense network (Ultra-Dense Networks (UDN)) architecture, which deploys numerous small cells to meet high capacity demands, increases the potential for interference. In response, 5G incorporates advanced interference mitigation techniques, such as enhanced beamforming with massive MIMO, dynamic spectrum sharing, and sophisticated resource allocation algorithms powered by artificial intelligence (AI) and machine learning (ML). These technologies enable real-time interference prediction and management, improving network performance even in dense environments.

As the network landscape progresses toward 5G Advanced and 6G, interference management will only become more complex. The use of higher frequency bands like THz will offer greater bandwidth but also present unique interference challenges. Additionally, the integration of NTNs, such as satellite and aerial networks, will introduce new interference scenarios that current techniques may not adequately address. Thus, future networks will require more sophisticated solutions, including real-time resource management, intelligent spectrum sharing, and cross-layer coordination between terrestrial and non-terrestrial networks [5].

The evolution of cellular networks has transformed interference management from a manageable concern to a central challenge. As network complexity increases with each generation, interference management strategies must evolve accordingly, ensuring that future networks meet the growing demands for speed, capacity, and reliability. Next, we discuss the prominent types of interference in 4G, 5G, and beyond, and the various approaches used to manage interference effectively.

### 2.1. Interference Classification and Management

Interference in 5G and beyond networks is a critical challenge due to the increasing complexity of network architectures and the higher frequency bands employed. As shown in Fig. 1, interference can be classified into two broad categories: **ICI** and **intra-cell interference** [19]. Both types of interference arise from the shared use of frequency, time, and spatial resources in modern cellular systems, particularly in UDN and HetNets. With the proliferation of small cells, massive MIMO, and mmWave technologies, effective interference management has become essential for maintaining high data rates, low latency, and robust network reliability.

#### 2.1.1. Inter-cell Interference (ICI)

ICI, as shown in Fig. 2, occurs when the signals transmitted by one cell affect users in a neighboring cell, a common problem in multi-tier cellular architectures where both macro and small cells operate within close proximity [3].

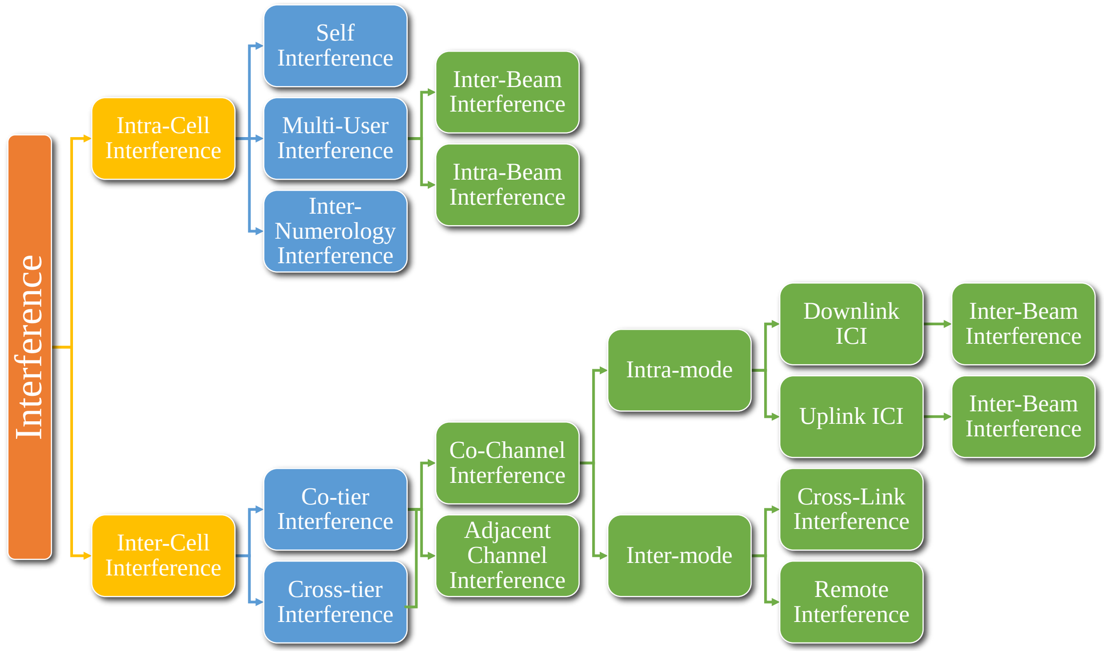



**Fig. 1.** Classification of Interference in 5G and beyond networks.

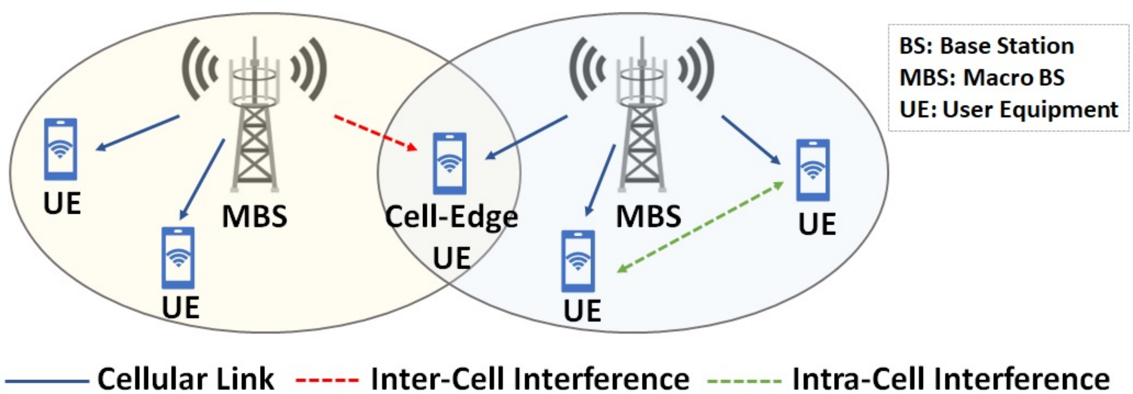



**Fig. 2.** Intra-cell and Inter-cell interference.

### 2.1.1.1 Co-tier interference

As shown in Fig. 3, Co-tier interference is a subcategory of ICI and occurs between cells of the same type—either two macro cells or two small cells [20]. As 5G networks become denser, particularly with the deployment of small cells, co-tier interference becomes a major issue. For instance, in urban environments where small cells are densely deployed, co-tier interference between adjacent small cells can degrade network performance significantly. Mitigation strategies like CoMP transmission/reception, where neighboring base stations coordinate their actions to reduce interference, and dynamic frequency reuse

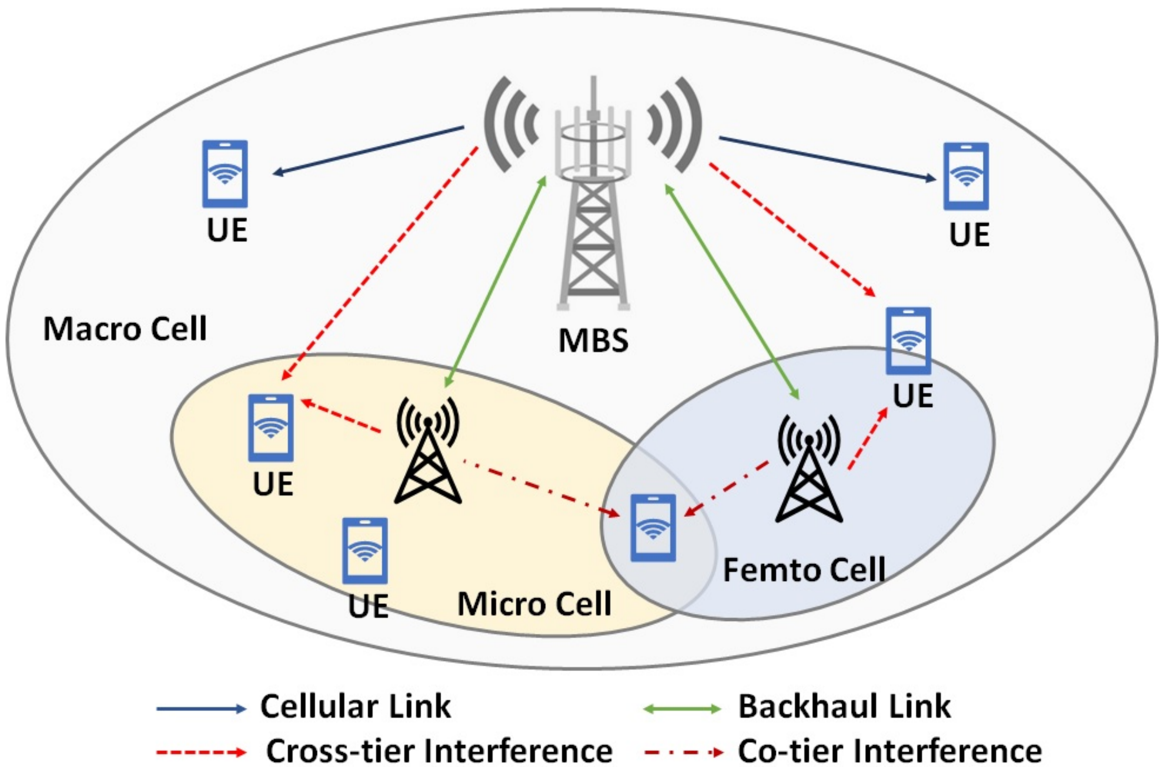



**Fig. 3.** Co-tier and cross-tier interference in HetNets.

schemes are critical in alleviating co-tier interference. CoMP can improve the Signal to Interference and Noise Ratio (SINR) by coordinating transmission, especially for cell-edge users.

#### 2.1.1.2 Cross-tier interference

Cross-tier interference, as shown in Fig. 3, is another type of ICI that occurs between different network layers, such as between macro cells and small cells [20]. In HetNets, macro cells provide wide-area coverage, while small cells, such as femto, pico, and micro cells, enhance local capacity. However, small cells often operate in the same frequency bands as macro cells, leading to cross-tier interference, particularly in dense urban areas. Users at the cell edge of a macro cell are more susceptible to this type of interference from nearby small cells. eICIC techniques, including ABS, have been introduced to mitigate cross-tier interference. ABS allows macro cells to mute their transmissions during specific subframes, giving small cells exclusive access to the spectrum, which reduces interference from the macro cell while maintaining high capacity in the small cells. Another method to reduce cross-tier interference is Cell Range Expansion (CRE), where the coverage area of small cells is artificially increased to balance the load between macro and small cells.

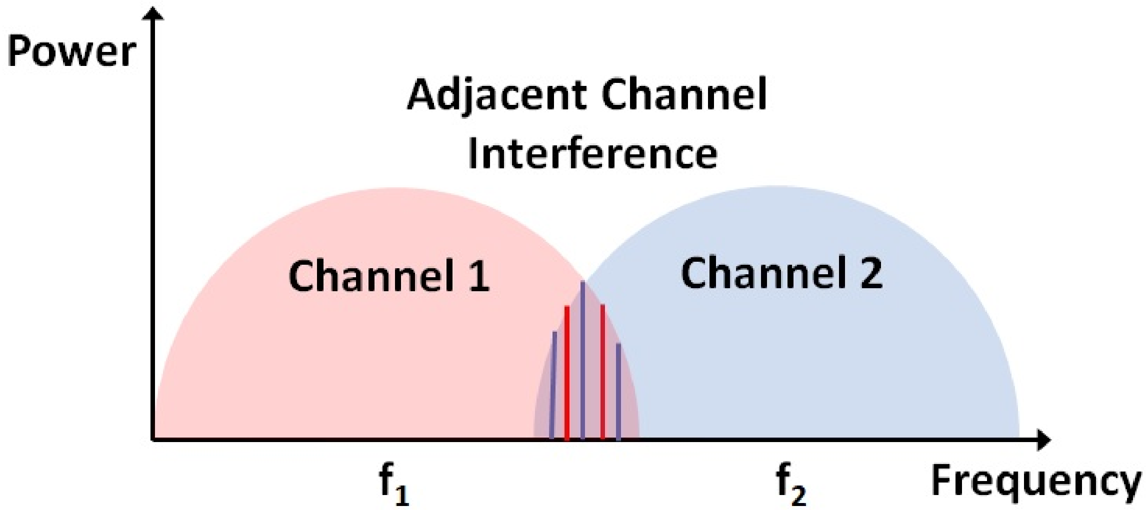



**Fig. 4.** Adjacent Channel Interference.

#### 2.1.1.3 Adjacent Channel Interference (ACI)

Adjacent Channel Interference (ACI), as shown in Fig. 4, is another critical issue that arises when signals on neighboring frequency channels interfere with each other, often due to poor filtering or non-linearities in transmission systems. This is especially problematic in OFDM systems, such as those used in 4G LTE and 5G NR, which are prone to out-of-band emissions that cause interference in adjacent channels [21]. The interference becomes more pronounced when network operators push for aggressive spectral efficiency by deploying tight frequency reuse plans, leaving little room for guard bands. Mitigating ACI requires advanced filtering techniques, such as the use of sharp filters at the transmitter and receiver ends, to minimize out-of-band emissions, employing advanced modulation schemes and signal processing techniques, and allocating adjacent channels to the cells in different geographical regions. Also, guard bands—frequency gaps between adjacent channels—can be introduced to minimize overlap, but this comes at the cost of reduced spectral efficiency [22].

#### 2.1.1.4 Co-Channel Interference (CCI)

Co-Channel Interference (CCI) is one of the most prominent forms of ICI, where neighboring cells reuse the same frequency bands [23]. While frequency reuse maximizes spectral efficiency, it also results in severe interference, particularly at the cell edges where the signal strength is low and interference from adjacent cells is high. CCI is particularly challenging in UDN, where base stations are deployed in close proximity to meet the ever-increasing data demand. Techniques like FFR can reduce CCI by dividing each cell into regions (center and edge) and assigning different frequencies to cell-edge users to avoid interference from neighboring cells. Dynamic Spectrum Sharing (DSS) allows dynamic allocation of spectrum resources to different base stations based on their real-time traffic demands, which helps mitigate co-channel interference. Furthermore, massive MIMO with advanced beamforming techniques can help mitigate CCI by steering beams toward the intended users and away from interfering cells, thus increasing SINR. CCI is of two types: intra-mode interference, which occurs in FDD or static TDD networks that are perfectly synchronized, and inter-mode interference (or cross-mode interference) which generally occurs in dynamic TDD or FD networks.

- **Intra-mode Co-Channel Inter-Cell Interference** or simply intra-mode interference, refers to interference that occurs within the same transmission mode, either DL-to-DL or UL-to-UL, in neighboring cells. In DL ICI, signals transmitted by the Base Station (BS) in one cell interfere with DL transmissions in an adjacent cell, affecting users at the edge of the coverage area. This interference is particularly prominent in 5G networks that deploy massive MIMO and small cells in close proximity, increasing the likelihood of interference between adjacent cells [24]. UL ICI occurs when multiple user devices in different cells transmit on the same frequency, causing interference at their respective BS. Users located near the cell edges, especially those using high transmission power to compensate for weak signals, are often the source of UL interference, which can significantly degrade network performance for neighboring cells.

  To mitigate intra-mode interference, networks use a range of techniques, including power control to adjust user device transmission strength, dynamic resource allocation to separate users onto different time or frequency resources, and coordinated scheduling to ensure that neighboring cells avoid simultaneous transmissions on the same frequency.

- **Inter-mode interference**, also known as **cross-mode interference**, arises when transmissions in different modes—such as UL and DL—interfere with each other. This interference is most common in TDD systems, where the same frequency band is used for both UL and DL transmissions but at different times. In scenarios where neighboring cells are not perfectly synchronized, **Cross-link Interference (CLI)** also called cross-slot interference, as shown in Fig. 5, occurs with UL transmissions in one cell interfering with DL transmissions in a neighboring cell. This type of interference becomes more prominent in dynamic TDD systems, where UL and DL configurations are constantly adjusted to match traffic demand, increasing the likelihood of interference between transmission modes [25].

  **Remote Interference (RI)**, as shown in Fig. 6, is a specific form of inter-mode interference, occurring in static synchronized TDD networks due to very large propagation delays [26]. This interference happens when distant BSs experience DL-to-UL interference caused by atmospheric conditions that form anomalous atmospheric ducts. These ducts, caused by sudden changes in the refractive index in the low troposphere, trap electromagnetic waves, allowing signals to travel much farther with

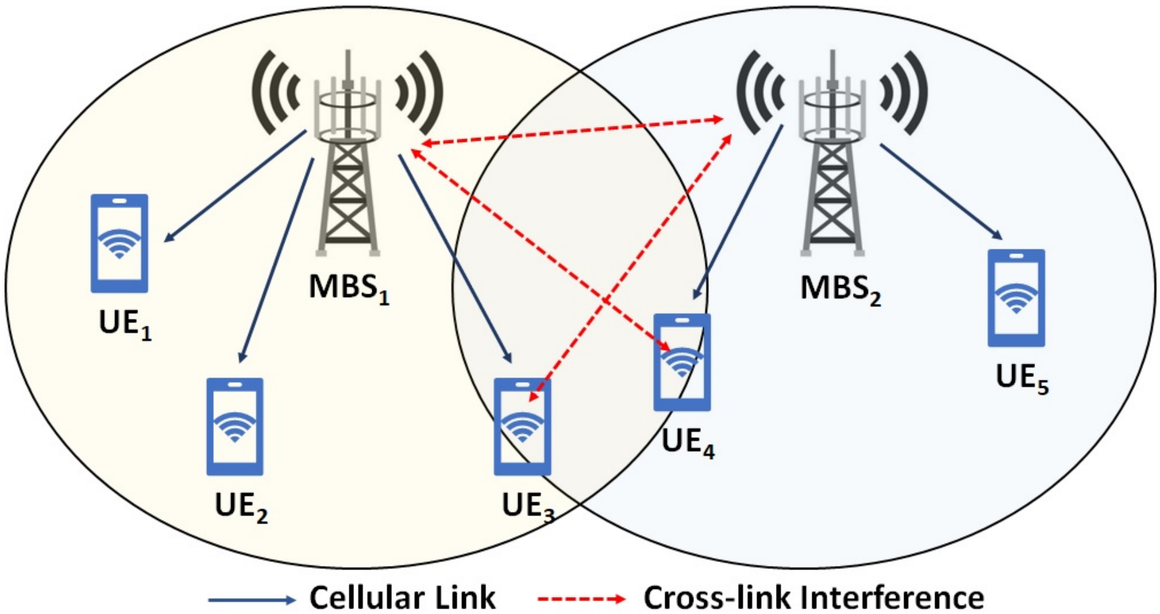



**Fig. 5.** Cross-link interference.

reduced attenuation than under normal conditions. This phenomenon, known as ducting, can cause DL signals from a distant BS to interfere with the UL reception at another base station far away.

The impact of RI is severe, as it can affect both UL data and the reception of critical UL reference signals, such as Sounding Reference Signals (SRS), which are used to estimate UL channel quality. In TDD systems that rely on channel reciprocity for UL/DL channel quality estimation, interference with the SRS leads to a deterioration of Key Performance Indicators (KPIs), such as call drop rates and handover success rates, ultimately resulting in poor user experience. Although atmospheric ducting is a rare event, when it occurs, it can disrupt thousands of BSs and significantly impact network performance. Countries like China and the United States have experienced the damaging effects of RI for years [27], drawing attention from both industry and academia. The International Telecommunication Union (ITU) has recommended considering atmospheric ducts in channel modeling, and 3GPP has initiated a project to address RI in the 5G standardization process. Many telecommunication companies have also begun monitoring and analyzing the effects of RI to mitigate its impact.

### 2.1.2. Intra-cell interference

Intra-cell interference, as shown in Fig. 2, is a growing challenge in 5G networks due to the multiplexing of several numerologies, the introduction of advanced multiple access schemes like Non-Orthogonal Multiple Access (NOMA) and Space Division Multiple Access

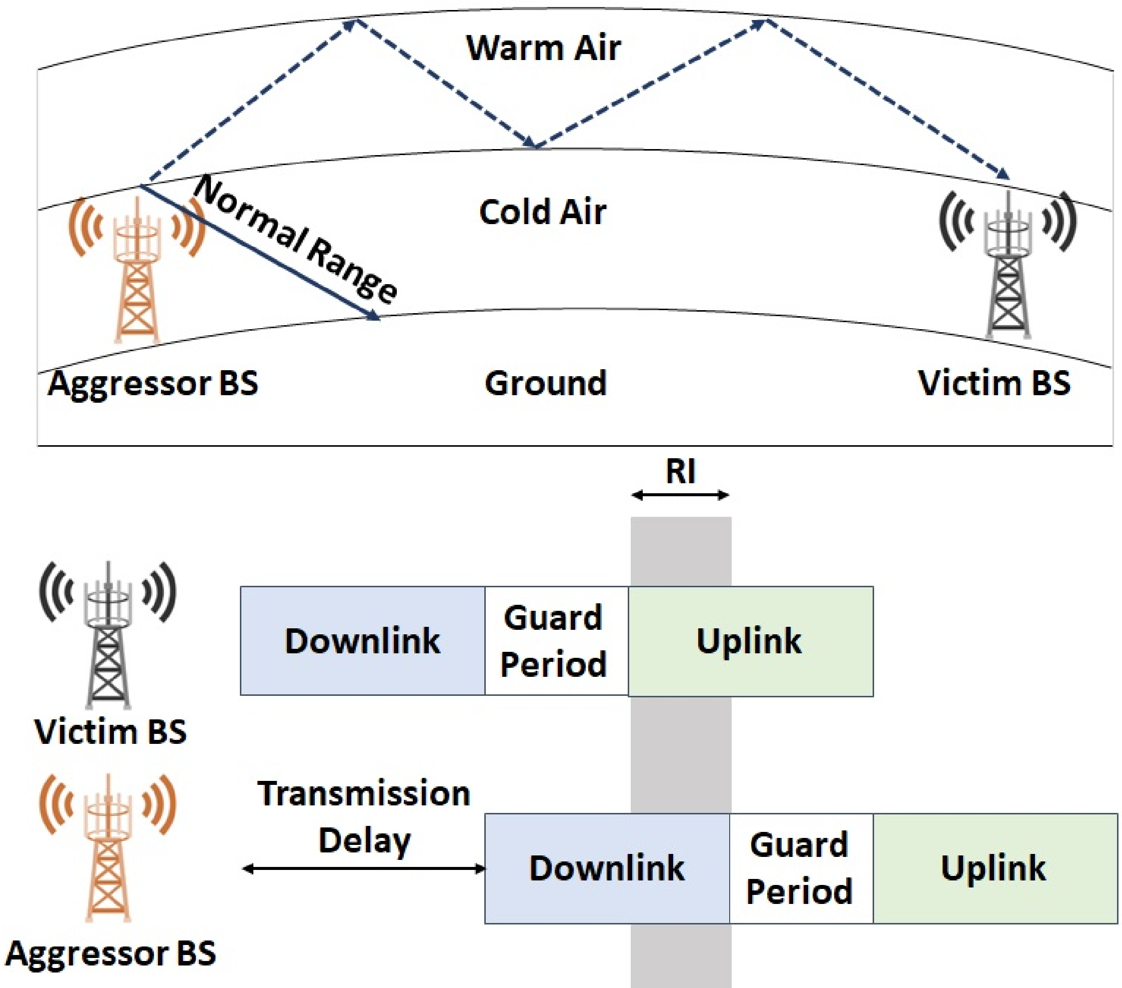



**Fig. 6.** Remote interference.

(SDMA), which allows multiple users to share the same time and frequency resources in the same cell, and the deployment of In-Band FD transceivers. Intra-cell interference can be classified into several subtypes, including Self Interference (SI), Multi-User Interference (MUI), and Inter-Numerology Interference (INI).

#### 2.1.2.1 Self Interference (SI)

SI, also called intra-system interference, is primarily a concern in FD communication systems, where a device transmits and receives signals simultaneously on the same frequency. This can lead to interference between the transmitted and received signals, significantly degrading communication performance. Mitigating self-interference requires Successive Interference Cancellation (SIC) techniques, which employ advanced signal processing to filter out the transmitted signal at the receiver. FD communication is expected to play a

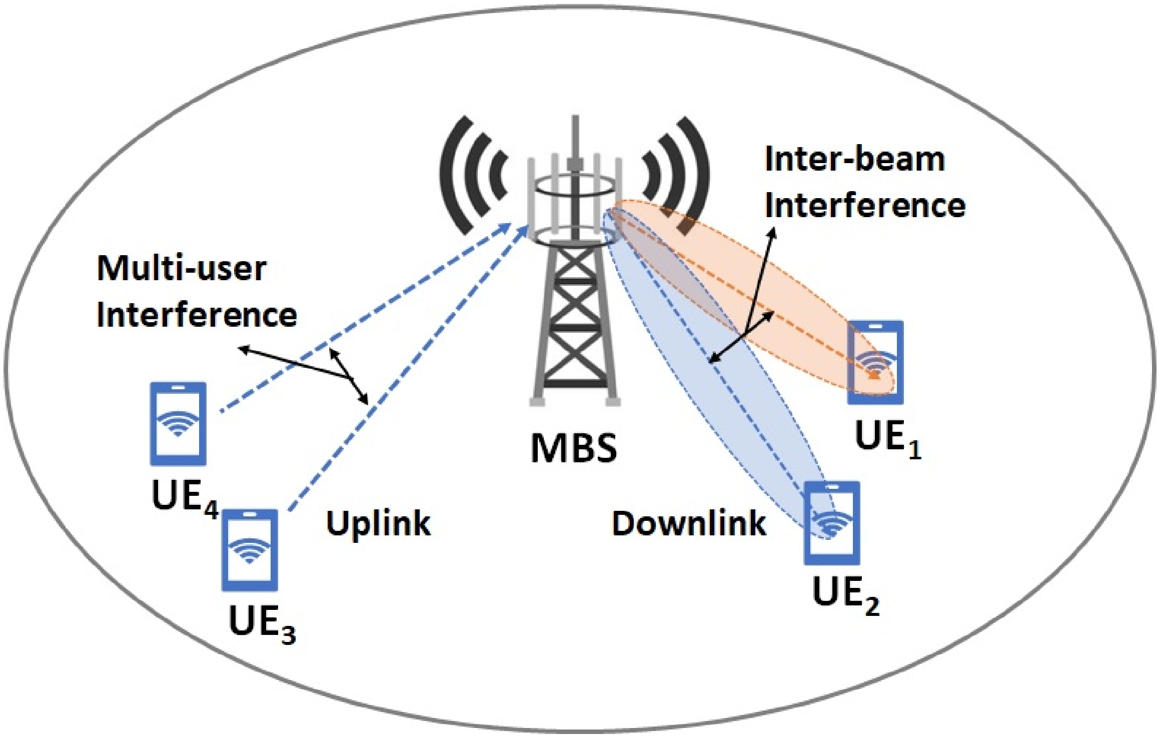



**Fig. 7.** Inter-beam and multi-user interference.

key role in future 6G networks, where efficient SI mitigation will be crucial to unlocking the potential for simultaneous transmission and reception on the same channel [28].

#### 2.1.2.2 Multi-User Interference (MUI)

MUI, as shown in Fig. 7, arises in systems using massive MIMO and spatial multiplexing, where multiple users are served simultaneously using the same time and frequency resources but different spatial beams. MUI occurs when the signals intended for different users interfere with each other, particularly when the users are spatially close. To mitigate MUI, advanced beamforming techniques are employed to ensure that each user's signal is spatially separated from others. In 5G networks, user scheduling algorithms are used to dynamically allocate resources and ensure that users who are likely to interfere with one another are served on different beams or at different times.

- **Inter-beam interference**, as shown in Fig. 7, is a major issue in mmWave and sub-THz frequency bands, where narrow, highly directional beams are used to transmit data. In dense urban environments, where many users are served simultaneously, the interference between closely spaced beams can reduce the effectiveness of beamforming [29, 30]. Dynamic beam management and beam alignment techniques are critical to minimizing inter-beam interference. Beam alignment ensures that the beams are accurately directed toward the intended users, while dynamic beam management adjusts the beams in real time to minimize overlap and interference between adjacent beams.

- **Intra-beam interference** occurs when multiple users share the same directional beam within a cell, causing interference among those served by the same beam. This is particularly common in 5G systems that use mmWave frequencies and beamforming techniques. In massive MIMO and beamforming-based systems, users are spatially multiplexed within the same beam. However, when their data streams are not fully orthogonal, the spatial overlap results in interference between their signals, especially when the users are located close to each other within the beam. This interference reduces the quality of service for users, leading to lower data rates, increased error rates, and a decreased SINR. Moreover, intra-beam interference diminishes the system's ability to spatially multiplex users effectively, limiting the expected capacity gains from beamforming. To mitigate intra-beam interference, advanced beamforming techniques, such as adaptive beamforming and narrow-beam control, can be used to precisely target beams and minimize the number of users per beam. Effective user scheduling algorithms also play a key role by preventing users with similar spatial signatures from being served by the same beam, thereby reducing interference. Adjusting transmission power for users within the beam, particularly for those at the cell edge, helps mitigate interference, as does real-time beam refinement, which dynamically reassigns users to better-aligned beams to optimize performance.

#### 2.1.2.3 Inter-Numerology Interference (INI)

INI occurs when different numerologies—combinations of subcarrier spacing, cyclic prefix lengths, and other transmission parameters—are used simultaneously within the same frequency band in 5G networks. This interference arises due to the non-orthogonality of the numerologies. In 5G NR, multiple numerologies are introduced to support diverse services such as enhanced Mobile Broadband (eMBB), URLLC, and mMTC, which have varying latency and bandwidth requirements. Since these numerologies, with different subcarrier spacings, are multiplexed within the same bandwidth, their overlapping subcarriers can interfere with each other. This interference degrades signal quality, especially for services like URLLC that require high reliability or low latency, reducing the SINR and leading to lower data throughput, higher error rates, and overall service degradation [31–33].

To mitigate INI, several techniques are employed. Introducing guard bands between numerologies can reduce interference by creating buffer zones where no transmission occurs, though this approach reduces spectral efficiency. Advanced filtering techniques or windowing at the transmitter and receiver can also minimize interference by preventing signal leakage across numerologies. Lastly, dynamic resource allocation helps by scheduling different numerologies in separate parts of the spectrum, thus preventing interference caused by their proximity.

Beyond traditional interference scenarios, modern cellular networks must also address **interference from uncoordinated and adversarial sources**. In public safety networks, for example, interference from uncoordinated sources, such as neighboring networks operating on the same frequencies or external devices disrupting the spectrum, can severely degrade communication. Malicious actors may also deliberately cause interference through jamming or spoofing attacks, which aim to disrupt network operations. To counteract these threats, advanced spectrum monitoring, jamming detection, and security protocols must be employed to detect and mitigate interference from uncoordinated or adversarial sources. We discuss such interference scenarios in detail in Section 4.

In conclusion, while both 4G and 5G networks face similar types of interference, the complexity and severity are significantly greater in 5G due to innovations such as small cells, beamforming, and NOMA. Interference classification in 5G covers a wide range of scenarios, from traditional inter-cell and intra-cell interference to more advanced and emerging challenges posed by modern network architectures. Effective interference management will rely on a combination of techniques, including advanced beamforming, dynamic spectrum allocation, and real-time interference monitoring powered by AI/ML algorithms. As networks evolve towards 6G, interference management strategies will need to adapt to higher frequency bands, more complex deployments, and a wider range of interference sources, ensuring that the growing demands for capacity, reliability, and low latency are met.

### 2.2. Proposed Methodologies by 3GPP for Interference Management

As 5G and beyond networks become more complex, managing interference has become critical. 3GPP has proposed various methodologies, signaling mechanisms, and advanced procedures to address interference in these networks. This section outlines the key interference management approaches proposed by 3GPP, including techniques for pilot contamination, control channel interference, CLI, and RI, along with the signaling and measurement enhancements introduced in 5G NR.

#### 2.2.1. 5G NR Signaling for Interference Management

Signaling plays a crucial role in managing interference within 5G NR networks. To enhance interference management, 3GPP has introduced various types of Reference Signals (RS), which are exchanged between Next Generation Node B (gNB)s and User Equipment (UE)s. These signals are fundamental for functions such as DL/UL channel sounding, beam management, synchronization, and channel demodulation. Unlike earlier cellular technologies, where always-on, cell-specific synchronization and RS were continuously transmitted across the spectrum to facilitate precise channel estimation, 5G NR has adopted a more efficient approach. In 5G, only a minimal amount of cell-specific signals is broadcast, and the sole always-on signal is the Synchronization Signal Block (SSB). Key synchronization and RS in 5G NR include:

- **Channel State Information Reference Signal (CSI-RS):** CSI-RS is a flexible, configurable signal used for DL Channel State Information (CSI) acquisition. It provides interference estimation for UEs and supports advanced beamforming, particularly in Massive MIMO systems. CSI-RS is more efficient than LTE's Cell-specific Reference Signal (CRS), which was introduced in LTE Release 8, as it uses less overhead and can be configured per UE or beam. CSI-RS can be categorized as Zero Power (ZP) or Non Zero Power (NZP) for optimized interference management.
- **Sounding Reference Signals (SRS):** SRS is transmitted by UEs for UL channel quality estimation. It plays a similar role to CSI-RS but for the UL, helping gNBs optimize resource allocation. In TDD networks, SRS enables both UL and DL scheduling by leveraging channel reciprocity.
- **DeModulation Reference Signal (DMRS):** DMRS is used for decoding UL and DL channels, reducing interference during data transmission by providing channel-specific information. It replaces the always-on CRS used in LTE, minimizing unnecessary overhead.
- **SSB:** SSB, used for initial connection and beam management, is a periodic signal that allows UEs to measure DL channel quality. It assists in selecting optimal beams and helps mitigate interference in dynamic beamforming scenarios [34].

Typically, to measure interference from neighboring BSs, a UE can either directly measure the RS power from the interfering signal or utilize ZP-CSI-RS, which are specially configured resource elements for Channel State Information Interference Management (CSI-IM) estimation [35]. In this approach, the network configures CSI-IM to puncture the Physical Downlink Shared Channel (PDSCH) of the serving cell, creating a transmission gap that coincides with the data transmission of the neighboring cell. This enables the UE to perform interference measurements and provide feedback to the gNB.

These RSs enable UEs to measure interference from neighboring cells and report the results to the gNBs. This feedback is essential for allowing gNBs to dynamically adjust scheduling and resource allocation to mitigate interference. However, in dense network deployments, non-orthogonal RS are often used, which can result in pilot contamination—a major source of interference, particularly in multi-cell systems [36]. Pilot contamination occurs when pilot signals from different cells overlap, leading to poor channel estimation and degraded network performance. This issue is explored in more detail later in this section.

### 2.2.2. 5G NR Measurements and Reporting

In 5G NR, users and gNBs perform channel quality measurements to manage resources and mitigate interference effectively. UEs typically measure the quality of DL signals like CSI-RS and SSB, while gNBs measure UL signals such as SRS. UEs may also measure UL SRS from neighboring UEs. Key measurement indicators include SS-Reference Signal Received Power

(RSRP) , SS-SINR, and NR-Received Signal Strength Indicator (RSSI), which help assess the signal and interference conditions across different channels.

These measurements are then reported back to the gNB, which uses this feedback to optimize resource scheduling and interference management. Reporting can occur periodically, aperiodically, or semi-persistently, depending on the network configuration. The feedback typically includes Channel Quality Indicator (CQI), Precoding Matrix Indicators (PMI), and other CSI-related metrics that help calculate precoding matrices for beamforming and scheduling [37]. In TDD systems, channel reciprocity allows gNBs to use UL measurements to optimize DL resources, although this process requires substantial processing power.

Despite the utility of these techniques, challenges such as channel estimation errors and feedback delays in dynamic environments persist. Further research into adaptive beamforming methods is ongoing to address these issues and improve real-time interference management in 5G NR systems.

### 2.2.3. CLI Management - Signaling and Measurements

CLI, as shown in Fig. 5, poses significant challenges as UL and DL transmissions occur on the same frequency band but at different times, in dynamic TDD networks, particularly in TDD-LTE systems. To address this, 3GPP introduced multiple methodologies, beginning with Release 12, which proposed approaches for Enhanced Interference Mitigation and Traffic Adaptation (eIMTA) [38]. These strategies include power control, cell clustering, dynamic UL/DL configurations, interference cancellation, and optimized resource allocation and scheduling schemes.

As 5G networks evolved, Release 16 introduced further enhancements for managing CLI, particularly focusing on flexible resource allocation and improved signaling for interference mitigation. The primary advancements introduced in Release 16 [39] include:

- **Special Measurements and Reports at the UE Level:** UEs are now capable of measuring UL SRS from other nearby devices, providing crucial information about potential interference between UEs in neighboring cells. By extending the RSRP measurement and reporting capabilities, the network gains valuable insight into how different cells may interfere with each other in UL and DL operations.
- **Inter-gNB Signaling for Inter-cell Coordination:** Enhanced signaling between neighboring gNBs allows for improved coordination in resource allocation to mitigate interference. Resources can be categorized as either fixed (dedicated for either UL or DL) or flexible (usable for both UL and DL transmissions). Through inter-gNB signaling, a gNB can share its fixed and flexible resource allocation with neighboring gNBs. This coordination enables gNBs to optimize scheduling strategies, ensuring that critical DL transmissions are scheduled on interference-free fixed resources, while flexible resources are used for less critical transmissions that can tolerate higher interference levels.

These enhancements in signaling and measurement capabilities for CLI help 5G networks achieve more efficient interference management, allowing dynamic TDD systems to handle CLI effectively while improving overall network performance.

### 2.2.4. RI Management - Signaling and Measurements

RI, as shown in Fig. 6, occurs due to large propagation delays caused by atmospheric ducting, where signals travel over extended distances with minimal attenuation. This type of interference can severely degrade network performance, including reduced coverage and connection success rates. While no standardized solutions existed for managing RI in LTE, Remote Interference Management (RIM) became a necessary feature in commercial LTE TDD networks to ensure reliability [40].

Recognizing the increased severity of RI in large-scale 5G TDD deployments, particularly across borders, 3GPP introduced tools for automatic RIM in Release 16 [39, 41]. These tools are designed to minimize manual intervention and improve network robustness. Two new types of RIM-RS were specified to support automatic detection and mitigation of RI:

- **RIM-RS Type 1:** Sent by the victim gNB to notify aggressor gNBs of detected interference, providing information such as the identity of the interfering gNB, the number of symbols affected, and whether mitigation measures have been applied.
- **RIM-RS Type 2:** Sent by the aggressor gNB after applying the RIM procedure to inform the victim gNB that interference persists.

3GPP proposed three different frameworks—centralized and distributed—for applying RIM, which differ in how gNBs communicate and where decisions regarding interference management are made. However, the specific schemes to mitigate remote interference have not yet been standardized, leaving room for further development in this area.

### 2.2.5. Pilot Contamination and Control Channel Interference

Pilot contamination occurs when the same UL pilot sequence is reused across neighboring cells for efficient resource management in massive MIMO networks [42]. While frequency reuse helps maximize spectrum efficiency, it also introduces significant ICI, particularly in massive MIMO systems using TDD. Pilot contamination reduces channel estimation accuracy, which in turn affects the achievable data rates and overall spectrum efficiency. Although earlier studies focused on non-orthogonal signals as the primary source of pilot contamination, recent research has identified other factors, such as hardware impairments and distortions [43]. To address pilot contamination, robust interference coordination algorithms and techniques for efficient pilot reuse are required.

CCI, on the other hand, is a significant challenge in HetNets where small cells are deployed alongside macro cells. Control channels, such as the Physical Uplink Control Channel (PUCCH), carry vital signaling information like CQI and Hybrid Automatic Repeat Request (HARQ) feedback. Control channel interference can impact signal synchronization and cell searching. To minimize this interference, 3GPP has proposed power control mechanisms to keep macro base station (MBS) transmission power below a certain threshold [44]. Additionally, in networks where femtocells operate, 3GPP recommended configuring femtocells in closed access mode, which limits interference by restricting services to authorized users only [45]. These measures are essential to improving control channel reliability and mitigating interference in dense deployments.

#### 2.2.6. Base Station Coordination and Identification

The coordination between all MBSs and their associated users is critical to mitigating ICI. Mutual coordination among MBSs and neighboring cells is achieved via the backhaul X2 interface, which facilitates communication between BSs. However, effective identification and transmission of interfering BSs over the air remain key challenges. Advances in reference signals and variations in low transmission power can mitigate interference by optimizing signal control [46].

In dense mmWave networks, research has explored various methods to reduce inter-BS interference. One proposed solution involves choosing a downstream transmission coordination scheme based on the SINR level, helping to schedule packet delivery more efficiently [47]. Some researchers have investigated beam coordination processes between base stations to improve network capacity by synchronizing transmission beams across multiple base stations [44]. Another technique, spectrum pooling, has been explored using a centralized beam coordination framework, which pools frequency resources to avoid overlap and interference [48]. While these methods have demonstrated potential for efficient channel information transfer, their effectiveness largely depends on the latency involved in exchanging information between base stations, highlighting the need for further research to optimize real-time communication and coordination.

#### 2.2.7. Beamforming and Narrow Beam Link Acquisition

In mmWave Massive MIMO systems, beamforming and beamsteering are used to direct narrow beams toward users, reducing interference [49]. However, inter-beam interference remains a challenge, particularly in high-mobility environments like D2D communication. Techniques such as tapering methods and zero-forcing beamforming have been proposed to reduce inter-beam interference by suppressing interference from sidelobes of the antenna array [50]. These solutions are critical for maintaining the performance of Massive MIMO systems in dense and mobile environments.

In conclusion, the methodologies developed by 3GPP for interference management in 5G and beyond networks address the growing complexity of modern wireless systems. Through advanced signaling mechanisms, pilot contamination mitigation, and interference management, 3GPP's proposed solutions play a crucial role in optimizing network performance. These innovations are essential for maintaining efficient and interference-free operation as networks evolve toward higher frequencies, denser deployments, and more diverse use cases.

## 3. Open RAN (O-RAN)

This section discusses the state of O-RAN at the time of this writing. This includes an overview of O-RAN and its architecture in Section 3.1, a detailed description of Use Case 26 in Section 3.2, and, finally, a description of O-RAN's current capabilities. The overview in Section 3.1 will focus on O-RAN as a whole, while Section 3.2 and Section 3.3 will focus on the work of Working Group 1 (WG1) and Working Group 3 (WG3) of the O-RAN Alliance, respectively, as their work is most relevant to our topic.

### 3.1. Overview of O-RAN

The purpose of O-RAN is to define a standardized architecture that is open, smart, virtualized, and disaggregated in mobile networks. This makes it possible for network operators to easily integrate different hardware and software solutions from multiple vendors while ensuring interoperability amongst all of the various components. Such an architecture is also intended to lower the barrier of entry for vendors and third-party application developers, which, in turn, has the potential to increase the availability of new and improved hardware and software, which should increase the rate at which mobile network technologies advance. The remainder of this section provides an overview of the O-RAN architecture.

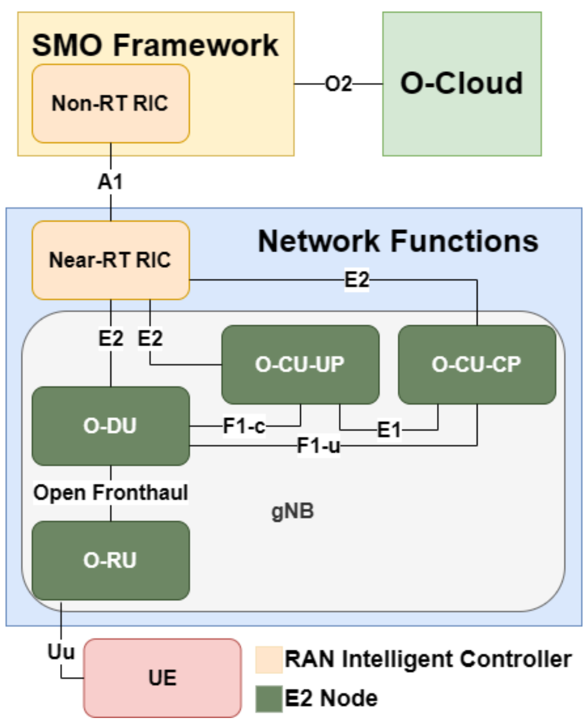



**Fig. 8.** A simplified diagram of the O-RAN architecture that depicts a subset of O-RAN components and interfaces.

The O-RAN architecture can be organized into three functional bodies, as depicted in Fig. 8: the Service Management and Orchestration (SMO) Framework, Network Functions, and the O-RAN Cloud (O-Cloud). The SMO Framework is responsible for managing the RAN domain which is one of several domains, such as the Core Network (CN), that needs to be maintained in a mobile network. Within the SMO, there is a RIC, the Non-Real-Time RIC (Non-RT RIC), that is responsible for managing RAN optimizations, primarily by maintaining policies for and analyzing data provided by RAN entities. The O-Cloud is accessible to the SMO via the O2 interface so that it can provide the SMO with cloud services. For instance, the O-Cloud can be used to host disaggregated and virtualized instances of entities from the Network Functions body, such as the Near-Real-Time RIC (Near-RT RIC). The Network Functions body is responsible for enforcing and executing tasks related to the policies that are created and disseminated by the Non-RT RIC. This group consists of a Near-RT RIC, which communicates with the Non-RT RIC through the A1 interface, and E2 nodes. An E2 node is an entity in the RAN, such as a O-RAN Distributed Unit (O-DU), with a connection to a Near-RT RIC via the E2 interface. Through this interface, the E2 node may report information to and receive commands from the Near-RT RIC.

Both the Non-RT RIC and Near-RT RIC are intelligent controllers, however, they have two very distinct roles in the O-RAN architecture. The Non-RT RIC is responsible for managing the network at a macro-level, meaning that it makes long-term decisions based on events across the entire network and focuses on network performance as a whole. The Near-RT RIC operates at the micro-level when compared to the Non-RT RIC as it is responsible for enforcing the policies that it receives from the Non-RT RIC by issuing commands to E2 nodes in a portion of the RAN that it is managing to achieve short-term goals. Furthermore, a Non-RT RIC may manage many Near-RT RICs while a Near-RT RIC may manage many E2 nodes. It is worth mentioning that it is also possible for the Non-RT RIC to manage E2 nodes in the absence of a Near-RT RIC, as the Near-RT RIC is an optional component in the O-RAN architecture. In such a deployment, E2 nodes would communicate with the Non-RT RIC via the O1 interface which is used to connect E2 nodes with the SMO.

There exists many internal and external functions to support the roles of both the Non-RT RIC and the Near-RT RIC. To achieve the intelligence required by each of these components, their exists rApps and xApps. Both of these components are fundamentally the same in that they are software instances responsible for carrying out automation in the network. The difference between xApps and rApps is that xApps are software specifically designed to run in the domain of the Near-RT RIC and rApps are specifically designed to run in the domain of the Non-RT RIC. Within each of these domains “control loops” exist that essentially define a workflow that accomplishes something useful. Non-RT control loops are expected to execute in a time frame greater than or equal to 1 s, while Near-RT control loops are expected to execute in less than 1 s but greater than 10 ms. This means that xApps will collect, analyze, and react to data quickly for more responsive automation, while rApps will analyze a lot of data at a slower rate and issue commands/policies for more comprehensive adaptations.

For communication to take place between a Near-RT RIC and an E2 node over the E2 interface, there exists an E2 Application Protocol (E2AP) and several E2 SMs (E2SMs) [8]. The E2AP defines the services, procedures, and basic constructs necessary for the Near-RT RIC and E2 nodes to communicate. For instance, the E2AP defines the E2 setup procedure used by an E2 node to send an E2 SETUP REQUEST message to its designated Near-RT RIC to establish an E2 connection. The request message includes a list of RAN functions that are supported by the E2 node that the Near-RT RIC can utilize. After a setup request is received by the Near-RT RIC and it completes the establishment of the connection, the Near-RT RIC can now use RIC Subscriptions to request the E2 node to report a particular metric or to initiate a specific procedure. To handle the definition of what specific metrics and procedures that an E2 node may support, E2SMs exist that define the Information Elements (IEs) that can be embedded in the control and report messages. For instance, it is the KPM E2SM that defines several IEs related to RAN performance that can be reported by an E2 node to the Near-RT RIC. This includes metrics related to transmitted data volume, packet loss, and signal quality. The RC E2SM defines several IEs that can be included in a control message sent from the Near-RT RIC to an E2 node to request an E2 node to carry out a specific action. This includes controls related to radio resource allocation, RAN access, and radio bearer configurations.

### 3.2. Use Case 26: Interference Detection and Optimization

In the O-RAN Alliance, one of WG1's many focuses is the development of use cases, for which they have a dedicated task group. This task group consists of many different players that includes representatives of various network operators, manufactures, vendors, government agencies, and other companies in industry. As all of these different entities have an interest in the development, deployment, and success of O-RAN, WG1 is where they come together to develop use cases that define O-RAN's applicability, requirements, and scope. These use cases are published in [17], which describes the motivation, resources, workflow, data, and goal for each agreed upon use case. Each use case also identifies an issue or limitation within a conventional mobile network, and re-envisions how it can be addressed and improved on by using O-RAN. This also includes completely new ideas with solutions that are only made possible with the O-RAN paradigm.

In [17], Use Case 26 proposes a new solution to an old problem — inter- and intra-cell interference. Due to the nature of mobile networks, a long-standing problem is the scarcity of radio resources that must be reused to support feasible deployments. In both heterogeneous and ultra-dense networks, ICI becomes a more complex problem as the likelihood of co-frequency overlap increases. It is made clear in [17] that while ICIC receives the most attention when it comes to addressing this issue, ICIC also has many limitations. This includes limitations such as the inability to reconfigure resources in real time, which can result in poor resource utilization. Another limitation is that ICIC depends on an ideal deployment, thus, when the deployment becomes more complex the effectiveness of an ICIC approach decreases. The last limitation that we will mention here is that the resource granularity of ICIC algorithms is coarse since they operate at the cell-level and not at the UE- or UE group-level, which limits its flexibility.

When considering the potential of an O-RAN solution to address the interference problem mentioned above, it is envisioned that real-time interference detection and optimization algorithms are possible at the cell, UE, and UE group levels. This includes enhanced mechanisms to detect interference, the ability to construct interference graphs, and autonomous coordination of radio resources to mitigate interference. Also, depending on the rate at which the network is expected to adapt to interference, Use Case 26 proposes both a "Fast Loop Optimization" and a "Slow Loop Optimization.".

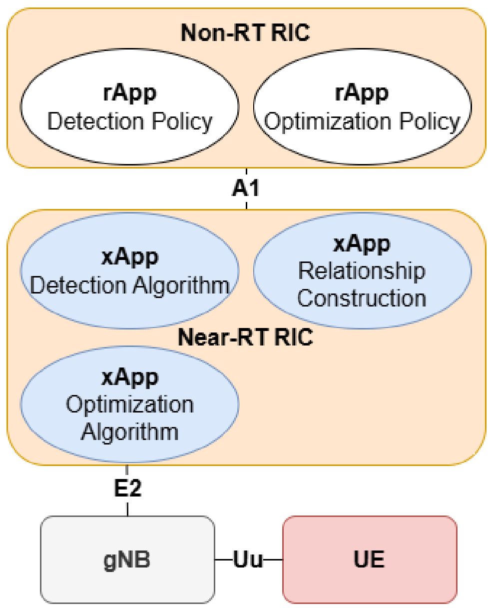



**Fig. 9.** A diagram of the main O-RAN components, interfaces, and responsibilities for the fast loop solution.

The fast loop optimization depends on the coordinated effort of the SMO, the Near-RT RIC, and E2 nodes. The components, interfaces, and relevant component responsibilities are shown in Fig. 9. With this setup, it is expected that the Non-RT RIC will be responsible for generating the interference policies (both for detection and optimization), generate QoS metrics and disseminate that information to the Near-RT RIC, and collect interference detection and optimization performance metrics from the Near-RT RIC. The Near-RT RIC is responsible for passing interference measurement data from E2 nodes to the Non-RT RIC, interpreting policies that it receives from the Non-RT RIC, and enforcing those same policies by issuing commands to the E2 nodes. E2 nodes must be able to report network state and UE measurement data to the Near-RT RIC, and support executing commands issued by the Near-RT RIC to carry out the requested actions. Fig. 10 depicts an example workflow for the fast loop optimization.

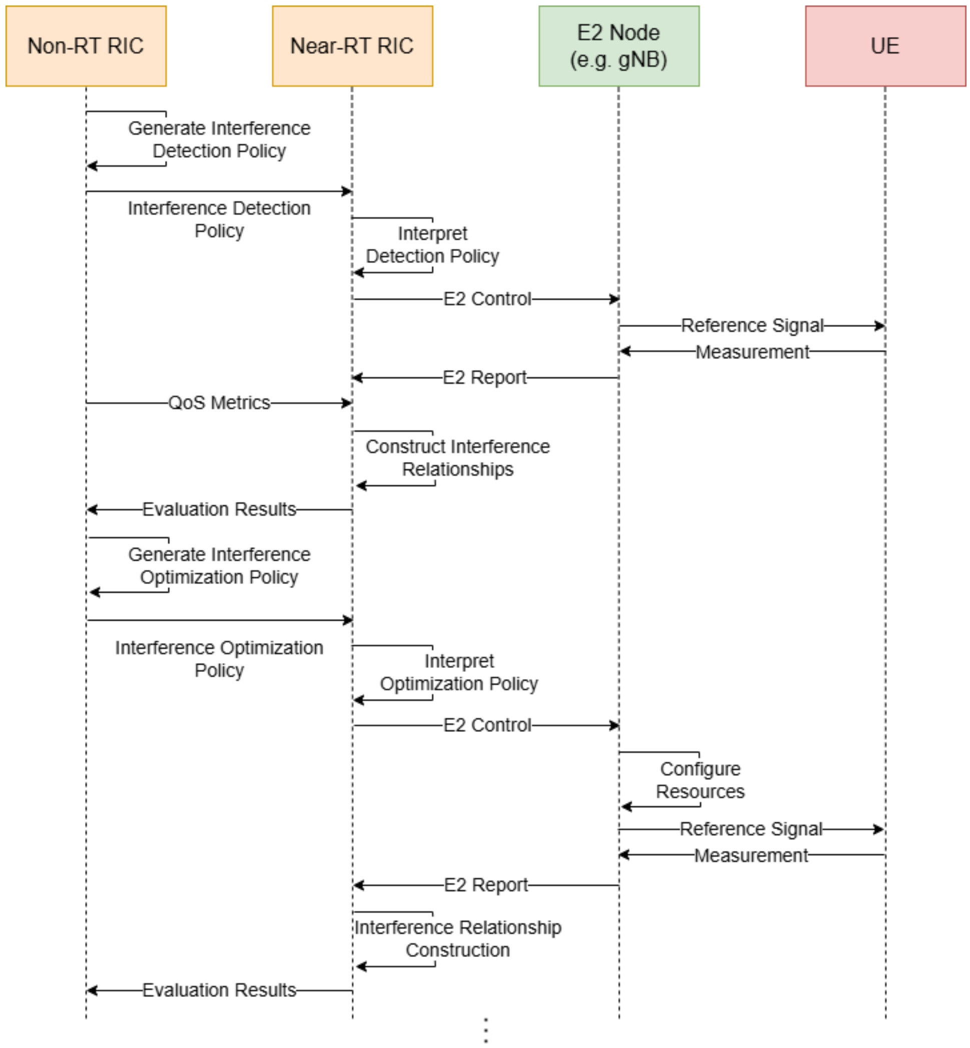



**Fig. 10.** A flow diagram that depicts the O-RAN workflow to perform interference detection and optimizations using the fast loop optimization.

The slow loop optimization is similar to the fast loop, however, there is no Near-RT RIC. Fig. 11 depicts the components, interfaces, and relevant component responsibilities for this solution. In the absence of a Near-RT RIC, the expectation is that the responsibilities of the Near-RT RIC will fall to the Non-RT RIC. This means that the rate at which the network can detect and optimize interference will be slower, the Non-RT RIC will not only create but also enforce its own policies, and E2 nodes will have to interact with the Non-RT RIC via the O1 interface.

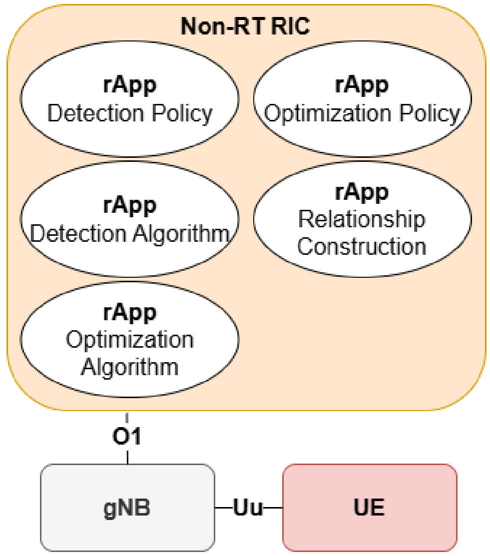



**Fig. 11.** A diagram of the main O-RAN components, interfaces, and responsibilities for the slow loop solution.

As for data requirements with respect to Use Case 26, there are only a handful of metrics that are mentioned in [17]. For network-level measurements it is stated that a UE should report metrics such as CQI, SINR, Modulation and Coding Scheme (MCS), RSRP, Physical Resource Block (PRB) usage, and throughput, while gNB cells will need to report metrics such as PRB usage and throughput. The SMO is also expected to generate metrics related to 5G QoS Identifier (5QI), throughput, latency, packet loss, and Block Error Rate (BLER). The expectation is that any O-RAN solution will use some, all, or other related metrics to achieve this use case's end goal of detecting, predicting, and optimizing interference.

### 3.3. Current O-RAN Capabilities

In this section, we will discuss the current capabilities of O-RAN that are relevant to Use Case 26 at the time of this writing. This entails identifying the data, functions, and messages available in the specifications to realize an interference detection and optimization solution. This will focus primarily on the work of Working Group 2 (WG2) and WG3, as WG2 is responsible for creating and maintaining standards for the Non-RT RIC and A1 interface, while WG3 is responsible for the Near-RT RIC and E2 interface standards.

The efforts of WG2 has resulted in many O-RAN specifications, which includes the Non-RT RIC architecture, the A1 interface, and the R1 interface. In [51], a general overview of the Non-RT RIC is provided, which touches on the various components, interfaces, functions, and services of the Non-RT RIC. In [52], a REpresentational State Transfer (REST) Application Programming Interface (API) is used to realize the A1 Application Protocol (AP) to support policy management. This means that the current A1 interface supports an AP that makes it possible for the Non-RT RIC and Near-RT RIC to exchange information regarding policy. This includes the services, operations, resource indicators, and API to create, update, delete, and query policies. In [53], currently supported data models that can be exchanged over the A1 interface are defined. Moreover, [53] defines the objects, data types, and identifiers that can be transported over the A1 interface via the A1 AP. In its current state, [53] defines policy objectives for QoS, Quality of Experience (QoE), UE-level, slice-level, load balancing, and energy saving targets. In addition to policy objectives, [53] also defines policy resources related to traffic steering optimizations, Slice Level Agreement (SLA) assurance, load balancing, and energy savings. As an example, this means that it is possible to define and transport a policy between a Non-RT RIC and Near-RT RIC over the A1 interface that communicates a QoS target for a given UE using a particular set of resources.

The purpose of the R1 interface is to provide communication between the Non-RT RIC framework and rApps for registration, discovery, authentication, and authorization. By opting to use an interface between Non-RT RICs and rApps instead of a traditional API, the O-RAN alliance seeks to increase flexibility, portability, and interoperability between SMO and rApp implementations from different vendors. All in all, in the current specifications, the Non-RT RIC supports hosting rApps that are capable of analyzing data and creating policies. For further information on the R1 interface, WG2 maintains the specifications [54–56] that define the general principles and aspects of the R1 interface, as well as the transport protocol and data models that are currently supported.

It is WG3 that is responsible for specifying standards related to the Near-RT RIC, the E2 interface, and the Y1 interface. This encompasses the Near-RT RIC architecture, it's API, xApp management, E2 SMs, and access to data for RAN analytics.

In [57], the E2 AP is specified. This AP defines the procedures and corresponding message exchanges that are necessary for the Near-RT RIC and E2 nodes to communicate. This includes E2 setup, update, and removal procedures that allow E2 nodes to open, modify, and close E2 connections with the Near-RT RIC. The setup procedure is a precursor for Near-RT RICs and E2 nodes to interoperate as they must exchange available RAN functionalities, supported E2 SMs, and configurable E2 node components. The procedure defined to open an E2 connection makes use of the "E2 SETUP REQUEST," "E2 SETUP RESPONSE," and "E2 SETUP FAILURE" messages. Once the E2 connection is established, the E2 AP also defines the procedures for subscription management that allows the Near-RT RIC to request periodic reports from an E2 node, which the Near-RT RIC can use to monitor performance in the RAN. The subscription request procedure makes use of the"RIC SUBSCRIPTION REQUEST," "RIC SUBSCRIPTION RESPONSE," and "RIC SUBSCRIPTION FAILURE" messages. In addition to RAN monitoring and once the E2 connection is established, [57] also defines the RIC control and query procedures. The control procedure is what makes it possible for the Near-RT RIC to initiate a specific RAN action by an E2 node. This procedure makes use of the "RIC CONTROL REQUEST," "RIC CONTROL ACKNOWLEDGE," and "RIC CONTROL FAILURE" messages. The query procedure is what enables the Near-RT RIC to request specific information related to the RAN or a UE from an E2 node. This procedure makes use of the “RIC QUERY REQUEST,” “RIC QUERY RESPONSE,” and “RIC QUERY FAILURE” messages. [57] also defines the ASN.1 message formats required for serialization and de-serialization of E2 AP messages. In summary, the current O-RAN E2 AP makes it possible to set up E2 connections, access to RAN data, and a means to issue RAN controls.

In addition to the E2 AP, WG3 also specifies several E2 SMs. These SMs are used in addition to and on top of the E2 AP to monitor a specific RAN metric or to invoke a particular RAN action. Thus, for an E2 SM, the specifications define the services that it realizes (e.g., control and report), the triggers available to detect and report information (e.g., periodic or event-based), and the E2 AP message IEs needed to realize a service. In essence, they determine what can be achieved by a Near-RT RIC when it is is used to manage the RAN. The current specifications include the Cell Configuration and Control (CCC) SM [13], KPM SM [12], and RC SM [14]. In the following paragraphs that describe the current capabilities of the various E2 SMs the focus will be on the elements that we believe are most relevant to Use Case 26.

It is worth mentioning that each E2 SM supports various “styles.” These styles are primarily used to distinguish between variations of granularity, conditions, and functions that are included in the messages. For instance, in the CCC SM, report and control functions can be implemented using Style 1 or Style 2. Style 1 reports and controls apply to the gNB as a whole (node-level), while Style 2 applies to the individual cells that make up a gNB (cell-level). Therefore, the styles that a Near-RT RIC or E2 node supports will directly affect what can be achieved with a particular SM, especially when it comes to the level of control that is available and the granularity of the data that is reported.

In its current state, the CCC SM provides access to E2 node / cell-level configuration information through the report service and allows an E2 node / cell to be configured via the control service. At the E2 node level, the current specifications define IEs to report component information regarding the O-DU, O-RAN Central Unit - Control Plan (O-CU-CP), and O-RAN Central Unit - User Plane (O-CU-UP) that make up the gNB. Controls for the O-CU-CP exists to configure the available neighbor list for handover operations as well as Resource Radio Management (RRM) policy control and reporting. At the cell-level, the O-DUs can report UL and DL frequencies, SSB parameters, available Bandwidth Parts (BWPs), and partition lists. For the O-DU, only the partition list, which is used to mitigate interference for SLA assurance, can be controlled in the current specification. The current specifications also support BWPs and RRM policy configurations to be both reported and controlled at the cell-level.

The purpose of the KPM SM is to provide access to RAN performance measurements over the E2 interface. It only defines IEs in support of a report service and realizes five different reporting styles. With this SM, the Near-RT RIC can subscribe to the following O-RAN-specific reports from an E2 node. Transmitted data volume reports for both the UL and DL that describe how much data is transmitted in either the UL or DL at the Radio Link Control

(RLC) layer in a given amount of time. Distribution of transmitted data volume to incoming data volume reports for both the UL and DL that describe the ratio of packets successfully transmitted versus those that have been queued for transmission at the RLC layer in a given amount of time. Packet drop rate reports for both the DL and UL that describe the ratio of packets that were dropped due to high traffic loads. DL synchronization RSRP and SINR reports that describe RSRP and SINR measurements reported by a UE to an E2 node. In addition to the O-RAN-specific metrics, the KPM SM specification also indicates that the SM can be used for measurements defined by 3GPP in [58] and [59]. As for the different KPMs that can be measured and reported, the five styles are described in Table 1. Thus, the current KPM SM supports the transport of traffic and signal measurement reports from the gNB-level down to the UE-level, and can provide them periodically or based on some event.

| Style | Description |
|---|---|
| 1 | 3GPP defined measurements and O-RAN measurements at the gNB- / cell-level |
| 2 | Measurements at the UE-level and are specific to a single UE |
| 3 | A particular measurement for a group of UE that meet a particular condition |
| 4 | UE-level measurements for a group of UE that match multiple conditions |
| 5 | Measurements for a particular set of UE that are specifically identified |
| 255 | A single composite report of multiple reports for a particular style |

**Table 1.** O-RAN KPM E2 SM Report Service Styles

The RC SM provides the mechanisms necessary to control the RAN. In its current state, the RC SM implements the report, insert, control, policy, and query services which all facilitate manipulating the RAN. The report service is used to provide control and UE information for context, and supports four different as described in 2.

The insert service is in place to provide a way for E2 nodes to suspend a RAN process and request information from the Near-RT RIC on how to proceed. The insert service supports eight different styles, each pertaining to a different RAN related control. The styles and their respective descriptions are listed in Table 3.

The control service makes it possible to initiate and resume suspended RAN actions. The styles that this service supports includes the same eight styles mentioned for the insert service as each insert request must have a control request counterpart. Moreover, when the insert service is used to make a request to the Near-RT RIC, the process for which the insert request was initiated for is suspended until a response (i.e. control request) is received from the Near-RT RIC on how to proceed. However, since the control service can

| Style | Description |
|---|---|
| 1 | Complete copy of a network interfaces or Radio Resource Control (RRC) messages |
| 2 | Outcomes of a function that has been invoked |
| 3 | gNB configuration and neighbor relation changes |
| 4 | UE ID and state changes |
| 5 | Measurements for a particular set of UE that are specifically identified |

**Table 2.** O-RAN RC E2 SM Report Service Styles

| Style | Description |
|---|---|
| 1 | Radio bearer modification requests (e.g., QoS related parameters) |
| 2 | Radio resource allocation change requests (e.g., PRB scheduling) |
| 3 | Connected mobility control requests, primarily related to handover |
| 4 | Access control requests related to RRC admissions, rejections, and releases |
| 5 | Initiating, modifying and releasing secondary cells for dual connectivity |
| 6 | Initiating, modifying and releasing secondary cells for carrier aggregation |
| 7 | Configuration of cell re-selection priorities and timers |
| 255 | Composite insert function controls to support taking multiple actions in parallel |

**Table 3.** O-RAN RC E2 SM Insert Service Styles

be used without the insert service, it also supports additional service styles 8, 9, and 10. Those additional styles are listed in Table 4.

The policy service enables modifying the behavior of control process. In essence, the Near-RT RIC uses a policy to define a set of conditions that, once met, indicate what actions should be taken. The current policy service supports nine styles, very similar to those supported in the control service. Each style and their respective descriptions can be found in Table 5 for the policy service in the RC E2 SM.

Lastly, the query service supports requesting specific RAN and UE information needed to carry out RAN actions. Currently, the query service only supports two style types: style 1 and style 2. Style 1 is used for requesting and providing E2 node information, while style 2 is used for requesting and providing UE related information. Thus, style 1 can be used to collect cell configuration and neighbor relation information, and style 2 can be used for UE

| Style | Description |
|---|---|
| 1 | Radio bearer modification requests (e.g., QoS related parameters) |
| 2 | Radio resource allocation change requests (e.g., PRB scheduling) |
| 3 | Connected mobility control requests, primarily related to handover |
| 4 | Access control requests related to RRC admissions, rejections, and releases |
| 5 | Initiating, modifying and releasing secondary cells for dual connectivity |
| 6 | Initiating, modifying and releasing secondary cells for carrier aggregation |
| 7 | Configuration of cell re-selection priorities and timers |
| 8 | UE identification assignments |
| 9 | UE measurement reporting and configuration control |
| 10 | Control for UE beamforming settings |
| 255 | Composite insert function controls to support taking multiple actions in parallel |

**Table 4.** O-RAN RC E2 SM Control Service Styles

context related information. As the RC SM is the most elaborate E2 SM to-date, it provides many mechanisms and extensive control of the RAN.

| Style | Description |
|---|---|
| 1 | Radio bearer control policies |
| 2 | Radio resource allocation control policies |
| 3 | Mobility policies for connected UE |
| 4 | Radio access control policies |
| 5 | Dual connectivity control policies |
| 6 | Carrier aggregation control policies |
| 7 | Mobility control policies for idle UE |
| 8 | UE measurement and reporting configuration policies |
| 9 | Beamforming control policies |

**Table 5.** O-RAN RC E2 SM Policy Service Styles

## 4. Gap Analysis

In this section, we map various interference management techniques to the use cases defined by O-RAN, highlighting overlapping features. We also cover what we refer to as "non-ideal scenarios", which are situations that could benefit from interference management within the O-RAN framework but are not specifically addressed by the O-RAN Alliance. Section 4.1 explores how the O-RAN use cases align with existing interference management techniques, identifying areas where these techniques are sufficient and where gaps remain. In Section 4.2, we introduce non-ideal scenarios—such as uncoordinated or adversarial interference—that are not currently captured in Use Case 26 but should be considered by the O-RAN alliance for future development. These scenarios highlight the potential for extending O-RAN's capabilities to address a broader range of interference challenges.

### 4.1. O-RAN and Interference Management in Cellular Networks

Given the current state of O-RAN capabilities discussed in Section 3.3 and the review of interference management in Section 2, several key observations emerge. The use cases defined by the O-RAN Alliance in [17] provide a solid architecture and mechanisms for dynamic, fine-grained control of the RAN. However, while these use cases cover a variety of network optimization tasks, only Use Case 26 is specifically designed to address interference detection and mitigation. Despite this, none of the standardized functionalities in O-RAN are solely dedicated to interference detection, and only a few can be indirectly applied to interference mitigation.

Table 6 maps various interference management techniques to existing O-RAN use cases that share overlapping features, even though these use cases are not primarily focused on interference. This shows that, while O-RAN has the potential to implement interference management techniques, the framework is not yet fully optimized for this task. Furthermore, the current SM and IE only offer the groundwork for implementing interference detection and mitigation, but they have not been fully tailored for Use Case 26, which is still evolving.

For each interference type listed in Table 6, the specific mechanisms for interference detection and the relationships between interfering entities are still unclear. It is uncertain how a system will identify which RAN entities are causing interference and which should be targeted for mitigation. However, based on existing specifications, interference detection could potentially be managed by leveraging DL RSRP, DL SINR, and UL RSRP IEs, as defined in the KPM SM. The level of granularity in interference detection will depend on which of the six service models is employed.

Once the interference is detected, mitigation techniques must be considered. For example, co-tier interference requires BSs to coordinate transmissions and limit frequency sharing. The O-BWP attribute in the CCC SM can specify which PRB a cell uses, addressing frequency sharing. Similarly, the O-Newtork Energy Savings (NES) policy attribute can define a slot mask to coordinate transmissions with TDD. Cross-tier interference techniques, such as ABS, allow coordination between macro and small cells, which can also be managed with the O-NES policy attribute.

For ACI, enhanced filtering techniques, wider guard bands, and more precise modulations are recommended. The Grant Configuration control structure in the RC SM can specify MCS tables and transport block sizes during scheduling to mitigate ACI. CCI mitigation, which includes techniques like FFR, DSS, and beamforming, can be managed using the O-BWP attribute in the CCC SM and the beamforming configuration control in the RC SM. However, for SI management, which focuses on filtering techniques, there is no direct correlation with any O-RAN service models, and this might be beyond the scope of O-RAN specifications.

In summary, while O-RAN provides certain metrics and tools that could be applied to interference detection and mitigation, the precise mechanisms for doing so remain undefined. The service models designed to control and configure E2 nodes offer several features that could be adapted for interference management, but their primary focus lies outside of this domain. Additionally, there are specific scenarios, particularly those involving interference from uncoordinated and adversarial sources, that will require further development within O-RAN. These scenarios will be explored in Section 4.2, with future work discussed in Section 5.

| **Type of Interference** | **Cause** | **Impact** | **Interference Mitigation/Management Technique** | **Supporting O-RAN Use Case and Specifications [17]** |
|---|---|---|---|---|
| **Co-tier Interference** | Co-tier interference is prominent in dense deployments, where neighboring cells reuse the same frequency bands. | As more cells are deployed to improve coverage and capacity, interference among cells of the same type (e.g., macro-macro, small-small) becomes a growing concern, degrading network performance. | CoMP techniques allow base stations to coordinate their transmission and reception to reduce co-tier interference. Dynamic frequency reuse can also limit frequency sharing between neighboring cells. | Use case 5: Traffic Steering<br>Use case 11: Dynamic Spectrum Sharing (DSS)<br>Use case 26: Interference Detection and Optimization |

| Type of Interference | Cause | Impact | Interference Mitigation/Management Technique | Supporting O-RAN Use Case and Specifications [17] |
|---|---|---|---|---|
| **Cross-tier Interference** | Since small cells often operate within the coverage area of macro cells and reuse the same spectrum, they are vulnerable to interference from macro cells, particularly at cell edges. | This form of interference is particularly harmful in areas where small cells operate at lower transmission powers compared to macro cells. | eICIC, including techniques like ABS, allows macro cells to mute transmissions in specific subframes, giving small cells an opportunity to transmit without interference. | Use case 26: Interference Detection and Optimization |
| **Adjacent Channel Interference (ACI)** | In systems using OFDM, such as 4G LTE and 5G NR, out-of-band emissions can lead to ACI, especially when signals are closely spaced in frequency. | ACI can degrade the SINR for users in neighboring frequency channels, reducing the overall network throughput. | ACI is addressed by allocating adjacent channels to cells in different geographical regions, employing better filtering techniques, wider guard bands, and more precise signal modulation to reduce the impact of out-of-band emissions. | Use case 26: Interference Detection and Optimization |

| Type of Interference | Cause | Impact | Interference Mitigation/Management Technique | Supporting O-RAN Use Case and Specifications [17] |
|---|---|---|---|---|
| **Co-Channel Interference (CCI)** | In 5G, the reuse of the same frequencies across multiple cells to maximize spectral efficiency exacerbates CCI. | CCI is particularly problematic for cell-edge users, where signal power is weaker, and interference from neighboring cells is more prominent. | Techniques such as FFR, DSS, and advanced beamforming with massive MIMO can help reduce the overlap of frequency use between neighboring cells. | Use case 6: Massive MIMO Beamforming Optimization<br>Use case 11: Dynamic Spectrum Sharing (DSS)<br>Use case 22: MU-MIMO Optimization<br>Use case 26: Interference Detection and Optimization |
| **Intra-mode Interference (Downlink (DL) and Uplink (UL) Interference)** | Intra-mode interference occurs when neighboring cells operate in the same transmission mode (DL-to-DL or UL-to-UL), often in FDD or synchronized TDD systems. It is common in dense networks with small cells and high user density. | It lowers the SINR, reducing data throughput, increasing latency, and impacting users, especially at cell edges. It degrades network performance by making it harder for base stations to correctly decode signals from users. | Techniques such as beamforming, CoMP, power control, dynamic resource allocation and FFR are employed to minimize overlapping transmissions and reduce interference, particularly in dense network environments. | Use case 5: Traffic Steering<br>Use case 11: Dynamic Spectrum Sharing (DSS)<br>Use case 22: MU-MIMO Optimization<br>Use case 26: Interference Detection and Optimization |

| Type of Interference | Cause | Impact | Interference Mitigation/Management Technique | Supporting O-RAN Use Case and Specifications [17] |
|---|---|---|---|---|
| **Inter-mode Interference (Cross-Link Interference (CLI) and Remote Interference (RI))** | Occurs in TDD systems, where the same frequency is used for both UL and DL but at different times. When neighboring cells are not perfectly synchronized, CLI arises, where an UL transmission in one cell interferes with the DL in another. RI occurs in TDD systems due to atmospheric conditions, where DL signals from distant BSs interfere with UL reception at other BSs, particularly during rare events like atmospheric ducting. | Degrades the SINR, affecting both UL data and DL quality, leading to increased call drops, handover failures, and reduced throughput. RI, especially, can disrupt UL reception for a large number of BSs simultaneously, significantly impacting network performance. | Dynamic TDD adjusts UL/DL patterns to minimize CLI, while inter-cell synchronization ensures better coordination between neighboring cells. For RI, guard periods between UL and DL transmissions, along with spectrum monitoring and frequency planning, can help mitigate interference, especially in regions prone to atmospheric ducting events. | Use case 9: RAN Slice SLA Assurance<br>Use case 11: Dynamic Spectrum Sharing (DSS)<br>Use case 26: Interference Detection and Optimization |
| **Self Interference (SI)** | In FD systems, a device transmits and receives on the same frequency at the same time, causing interference between outgoing and incoming signals. | Without effective cancellation, SI can severely degrade the performance of FD systems. | SIC techniques are used to filter out the transmitted signal at the receiver to improve performance in FD communication. | None |

| Type of Interference | Cause | Impact | Interference Mitigation/Management Technique | Supporting O-RAN Use Case and Specifications [17] |
|---|---|---|---|---|
| **Multi-User Interference (MUI)** | When multiple users share the same time and frequency resources, interference arises from the overlap of signals. | MUI reduces the overall signal quality for users, particularly when users are closely spaced in the spatial domain. | Advanced beamforming and user scheduling techniques help reduce MUI by dynamically adjusting the spatial separation of users and carefully allocating resources. | Use case 6: Massive MIMO Beamforming Optimization<br>Use case 9: RAN Slice SLA Assurance<br>Use case 11: Dynamic Spectrum Sharing (DSS)<br>Use case 22: MU-MIMO Optimization<br>Use case 26: Interference Detection and Optimization |
| **Inter-Numerology Interference (INI)** | 5G supports various services like eMBB, URLLC, and mMTC, each requiring different numerologies. When multiple numerologies are multiplexed in the same band, their non-orthogonal subcarriers can overlap, leading to interference. | This interference degrades signal quality, reducing SINR, data throughput, and increasing error rates, particularly affecting high-reliability services like URLLC. | Techniques include introducing guard bands to create buffer zones, using advanced filtering/windowing to minimize signal leakage, and dynamically scheduling numerologies across different parts of the spectrum to avoid interference. | Use case 26: Interference Detection and Optimization |

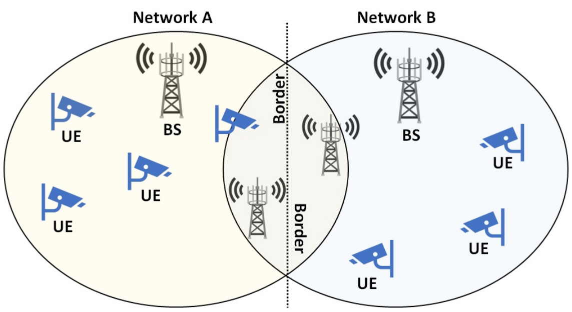
| Type of Interference | Cause | Impact | Interference Mitigation/Management Technique | Supporting O-RAN Use Case and Specifications [17] |
|---|---|---|---|---|
| **Inter-beam Interference** | As the number of beams increases, particularly in dense environments, interference between closely spaced beams can degrade signal quality. | Inter-beam interference reduces the effectiveness of mmWave systems, particularly in urban and high-density areas where many users are served simultaneously. | Dynamic beam management and precise beam alignment techniques are necessary to minimize interference between closely spaced beams. | Use case 6: Massive MIMO Beamforming Optimization<br>Use case 22: MU-MIMO Optimization |
| **Intra-beam interference** | In massive MIMO systems, multiple users are spatially multiplexed within the same beam. If their signals aren't fully orthogonal, interference arises, especially when users are close within the same beam. | This interference reduces service quality, leading to lower data rates, higher error rates, and decreased SINR, limiting the system's ability to spatially multiplex users effectively. | Techniques include advanced beamforming to precisely target beams, user scheduling to separate users with similar spatial signatures, power control to reduce interference, and real-time beam refinement to reassign users to less crowded beams. | Use case 6: Massive MIMO Beamforming Optimization<br>Use case 22: MU-MIMO Optimization<br>Use case 26: Interference Detection and Optimization |

**Table 6.** Summary of interference classification and management in 5G and beyond networks with supporting O-RAN use case and specifications.

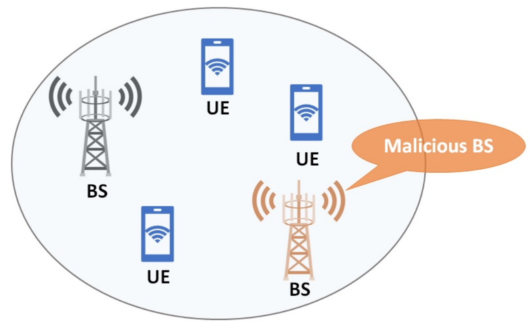
### 4.2. Additional Scenarios of Interest

Unlike the ideal scenario described in Use Case 26, where interference management is conducted in a controlled, coordinated setting, real-world networks often face interference from external or adversarial entities that are beyond the network's control. These situations, categorized as ”non-ideal scenarios,” require a more robust approach to interference detection and mitigation.

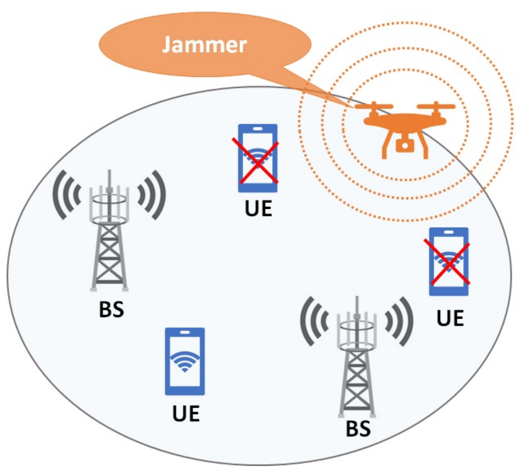
In Scenario A, we consider unintentional, external interference. This scenario could occur when multiple cellular networks have overlapping coverage areas and share part or all of the same spectrum, leading to interference. For instance, at the border of two neighboring countries without a spectrum-sharing agreement, interference may arise between the networks, as illustrated in Fig. 12a. Here, two networks, $\text{Network}_A$ and $\text{Network}_B$, both deploy BSs and UEs, such as wireless cameras for border surveillance. Both UL and DL transmissions could be affected, depending on the spectrum allocated and the scheduling of resources.




**(a)** Two neighboring mobile networks are deployed at the border with overlapping coverage areas.




**(b)** A rogue BS begins causing interference and reporting false data to disrupt service from within the network.




**(c)** A drone external to the network disrupts service by jamming UL and DL signals.

**Fig. 12.** Scenarios illustrating interference from uncoordinated and adversarial sources.

In Scenario B, we deal with intentional, internal interference. In this case, an internal entity that was once trusted by the network is compromised and behaves maliciously. As shown in Fig. 12b, an internal BS could be taken over by an external actor, unbeknownst to the network operator. This compromised BS could disrupt services in the UL and DL by reporting false information or deliberately interfering with network operations.

Scenario C focuses on intentional, external interference, where a malicious actor disrupts network services from outside the network. For example, as depicted in Fig. 12c, a drone may hover near the RAN, jamming UL and/or DL communications for a targeted UE. A more sophisticated attacker could adapt to changes in the network's spectrum, further complicating interference mitigation efforts.

In Scenario D, the risks associated with the reliance on AI/ML solutions for interference detection and optimization are considered. These risks include data poisoning, inference attacks, and evasion attacks. As highlighted in [16], such attacks can degrade the performance of AI/ML-based interference management systems by manipulating the data used for training and decision-making, ultimately compromising the network's ability to detect and mitigate interference effectively.

## 5. Future Research Work

The rapid evolution of 5G and the transition toward 6G networks present increasingly complex challenges in interference management, particularly in the context of O-RAN. While O-RAN has made significant strides in managing coordinated interference, future research must address several key areas to ensure the network's robustness and adaptability in the face of more dynamic, unpredictable, and malicious interference scenarios. Below describes some of the most critical research areas for the future, which are depicted in Fig. 13:

- **Uncoordinated External Interference Management:** A significant gap in current O-RAN solutions is the handling of uncoordinated external interference, such as interference from neighboring networks operating independently, rogue transmitters, or environmental factors that may cause signal degradation. Future research should focus on developing real-time interference detection systems that can identify, classify, and mitigate uncoordinated interference. One potential area of research is the use of AI/ML models that can learn from the environment, predict interference patterns, and adapt dynamically to mitigate the impact on network performance. By leveraging real-time data analytics, networks can be equipped with the ability to automatically adjust spectrum usage, power levels, or beamforming patterns when encountering external interference.
- **Adversarial Interference and Jamming Detection:** As networks become more integral to critical infrastructure and public safety systems, adversarial interference poses an increasing threat. Jamming attacks or malicious actors deliberately disrupting network operations are particularly concerning in military, public safety, and financial sectors. Future research should focus on the development of advanced security protocols to detect and mitigate these types of interference. Techniques such as AI-based jamming detection, spread spectrum technologies, and frequency hopping could be enhanced to provide more resilient solutions. Additionally, building secure frameworks that can rapidly isolate compromised network segments and maintain service continuity during an attack is vital for ensuring O-RAN's robustness.
- **Spectrum Sharing in Highly Dense Environments:** With the growing deployment of UDN and HetNets, where small cells are deployed in close proximity, spectrum sharing becomes a critical challenge. The increasing demand for limited spectrum resources necessitates the development of more intelligent DSS algorithms. Future research should investigate how O-RAN's open interfaces and AI/ML capabilities can enable networks to adaptively allocate spectrum in real-time based on network demand, user density, and interference levels. By developing AI-based systems that can continuously optimize spectrum usage, O-RAN networks can enhance spectral efficiency and reduce the potential for interference in highly congested areas, such as urban centers or stadiums.

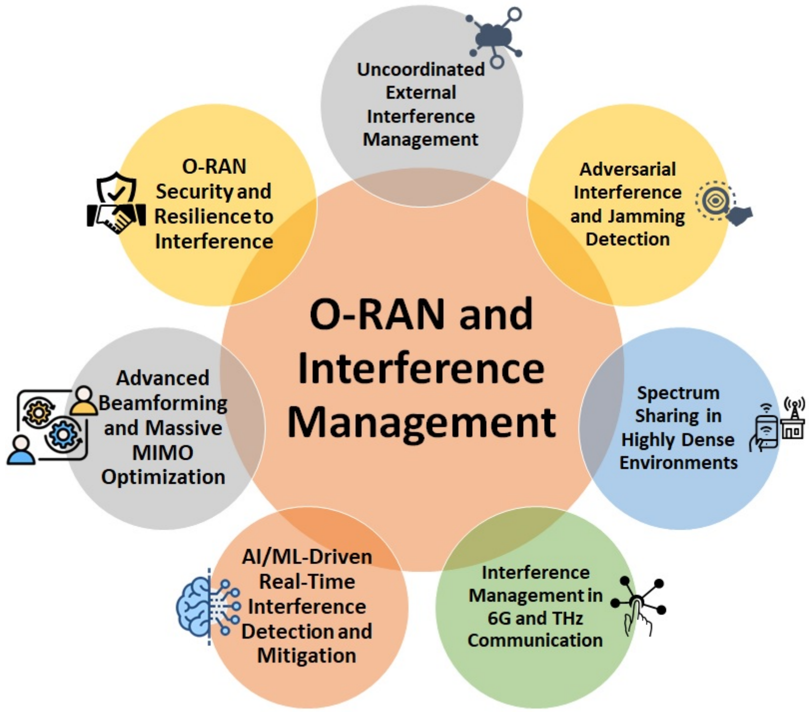



**Fig. 13.** O-RAN and interference management: future research areas.

- **Interference Management in 6G and THz Communication:** As research into 6G progresses, the use of THz frequencies introduces new challenges in interference management. These frequencies are highly susceptible to environmental factors, such as atmospheric absorption and blockages, making interference management more complex than in 5G. Future research should focus on propagation modeling in these frequencies, enabling the development of interference mitigation techniques tailored to the unique properties of these higher frequency bands. Moreover, new methods for handling multi-path interference, as well as techniques for spatial filtering and beamforming, will be crucial in ensuring efficient communication in 6G environments, where small cells and ultra-dense networks are expected to be even more prevalent.

- **AI/ML-Driven Real-Time Interference Detection and Mitigation:** The integration of AI and ML into interference management holds significant potential for improving O-RAN's ability to adapt to changing network conditions in real-time. Future research should focus on developing more sophisticated AI models capable of predicting interference patterns based on real-time network data. These models could enable proactive resource allocation, helping to reduce interference before it impacts the network. Additionally, ML algorithms could be trained to recognize different types of interference (e.g., co-channel, inter-numerology, cross-link) and recommend appropriate mitigation actions. As 5G and 6G networks become more complex, AI-driven automation will be essential for maintaining optimal performance and minimizing the manual intervention required for interference management.

- **Advanced Beamforming and Massive MIMO Optimization**: Massive MIMO and beamforming are key technologies in 5G and beyond for enhancing spectral efficiency and minimizing interference. However, optimizing these technologies in real-time for changing interference conditions remains a challenge. Future research should explore the use of adaptive beamforming techniques that can dynamically adjust beam patterns to avoid interference in highly congested environments. Similarly, massive MIMO optimization algorithms that leverage AI/ML for real-time beam management could improve interference rejection and ensure high-quality service for users, even in complex network topologies with dense deployments of small cells and devices.

- **O-RAN Security and Resilience to Interference:** With the increasing reliance on O-RAN in mission-critical networks, security against interference, particularly deliberate jamming and spoofing attacks, is paramount. Future research should address the development of secure communication protocols that not only detect but also withstand and recover from malicious interference. This may include creating resilient routing mechanisms, implementing encryption techniques to secure control signals, and employing multi-path transmission to ensure that data can still be delivered even under attack. Additionally, self-healing networks that can automatically detect interference or outages and reconfigure resources to maintain service will be vital in ensuring the robustness of O-RAN in the face of interference threats.

In conclusion, these future research areas highlight the critical need to develop more adaptive, intelligent, and secure interference management techniques as we move into the 5G Advanced and 6G eras. By addressing these challenges, O-RAN can ensure the scalability, flexibility, and reliability required to meet the growing demands of next-generation mobile networks.

## 6. Conclusion

This paper presented a comprehensive review of interference management within the O-RAN framework. It covered the general principles of interference management alongside methodologies developed by 3GPP. A detailed examination of the O-RAN architecture was provided, including an in-depth analysis of Use Case 26, which outlines the requirements for interference management in O-RAN. The current state of standards related to this use case was also discussed. Through a gap analysis, we demonstrated that, while several use cases offer mechanisms for managing interference, none directly address the detection and mitigation of uncoordinated external interference or deliberate disruptions caused by internal or external actors. These are critical gaps in ensuring network security and reliability. Therefore, further research and development are needed to enhance and test O-RAN's capabilities in managing adversarial and uncoordinated interference, particularly in scenarios where network stability is compromised by malicious or unexpected sources.

## References

[1] Parkvall S, Dahlman E, Furuskar A, Frenne M (2017) NR: The New 5G Radio Access Technology. *IEEE Communications Standards Magazine* 1(4):24–30.
[2] Qamar F, Hindia MN, Dimyati K, Noordin KA, Amiri IS (2019) Interference management issues for the future 5G network: a review. *Telecommunication Systems* 71:627–643.
[3] Zhou Y, Liu L, Du H, Tian L, Wang X, Shi J (2014) An overview on intercell interference management in mobile cellular networks: From 2G to 5G. *2014 IEEE International Conference on Communication Systems* (IEEE), pp 217–221.
[4] Lindbom L, Love R, Krishnamurthy S, Yao C, Miki N, Chandrasekhar V (2011) Enhanced inter-cell interference coordination for heterogeneous networks in lte-advanced: A survey. *arXiv preprint arXiv:11121344* .
[5] Saad W, Bennis M, Chen M (2019) A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE network* 34(3):134–142.
[6] O-RAN Working Group 1 (2024) O-RAN Architecture Description 12.0 (Open RAN (O-RAN) Alliance), Technical specification.
[7] O-RAN Working Group 2 (2024) O-RAN A1 interface: Use Cases and Requirements 1.03 (Open RAN (O-RAN) Alliance), Technical specification.
[8] O-RAN Working Group 3 (2024) O-RAN E2 General Aspects and Principles (E2GAP) 5.0 (Open RAN (O-RAN) Alliance), Technical specification.
[9] O-RAN Working Group 3 (2024) O-RAN Near-RT RIC Architecture 6.0 (Open RAN (O-RAN) Alliance), Technical specification.
[10] O-RAN Working Group 2 (2024) O-RAN Non-RT RIC & A1 interface: Use Cases and Requirements 10.0 (Open RAN (O-RAN) Alliance), Technical specification.
[11] O-RAN Working Group 3 (2024) O-RAN E2 Service Model (E2SM) 5.0 (Open RAN (O-RAN) Alliance), Technical specification.
[12] O-RAN Working Group 3 (2024) O-RAN E2 Service Model (E2SM) KPM 5.0 (Open RAN (O-RAN) Alliance), Technical specification.
[13] O-RAN Working Group 3 (2024) O-RAN E2 Service Model (E2SM) Cell Configuration and Control 4.0 (Open RAN (O-RAN) Alliance), Technical specification.
[14] O-RAN Working Group 3 (2024) O-RAN E2 Service Model (E2SM), RAN Control 6.0 (Open RAN (O-RAN) Alliance), Technical specification.
[15] O-RAN Working Group 11 (2024) O-RAN Security Requirements and Controls Specification 9.0 (Open RAN (O-RAN) Alliance), Technical specification.
[16] O-RAN Working Group 11 (2024) O-RAN Study on Security for AI/ML 1.0 (Open RAN (O-RAN) Alliance), Technical specification.
[17] O-RAN Working Group 1 (2024) Use Cases Detailed Specification 14.0 (Open RAN (O-RAN) Alliance), Technical specification.
[18] Pauli V, Naranjo JD, Seidel E (2010) Heterogeneous lte networks and inter-cell interference coordination. *Nomor Research GmBH* :1–9.
[19] Trabelsi N, Fourati LC, Chen CS (2023) Interference management in 5G and beyond networks: A comprehensive survey. *Computer Networks* :110159.

[20] Saquib N, Hossain E, Le LB, Kim DI (2012) Interference management in ofdma femtocell networks: Issues and approaches. *IEEE Wireless Communications* 19(3):86–95.

[21] Conceição F, Gomes M, Silva V, Dinis R, Silva A, Castanheira D (2020) A survey of candidate waveforms for beyond 5g systems. *Electronics* 10(1):21.

[22] Caro JB, Ansari J, Sayyed AR, de Bruin P, Sachs J, König N, Schmitt RH (2023) Empirical study on 5g nr adjacent channel coexistence. *2023 IEEE Wireless Communications and Networking Conference (WCNC)* (IEEE), pp 1–6.

[23] Yang X, Petropulu AP (2003) Co-channel interference modeling and analysis in a poisson field of interferers in wireless communications. *IEEE Transactions on signal processing* 51(1):64–76.

[24] Kim R, Kim Y, Yu NY, Kim SJ, Lim H (2019) Online learning-based downlink transmission coordination in ultra-dense millimeter wave heterogeneous networks. *IEEE Transactions on Wireless Communications* 18(4):2200–2214.

[25] Kim H, Kim J, Hong D (2020) Dynamic tdd systems for 5g and beyond: A survey of cross-link interference mitigation. *IEEE Communications Surveys & Tutorials* 22(4):2315–2348.

[26] (2019) Study on Remote Interference Management for NR (Release 16) (3GPP Technical Specification Group Radio Access Network), Technical Report (TR) 38.866.

[27] Zhang H, Zhou T, Xu T, Hu H (2023) Remote interference discrimination testbed employing ai ensemble algorithms for 6g tdd networks. *Sensors* 23(4):2264.

[28] Motz C, Paireder T, Pretl H, Huemer M (2021) A survey on self-interference cancellation in mobile lte-a/5g fdd transceivers. *IEEE Transactions on Circuits and Systems II: Express Briefs* 68(3):823–829.

[29] Kim E, Kwak J, Chong S (2020) Exception of dominant interfering beam: Low complex beam scheduling in mmwave networks. *2020 IEEE Wireless Communications and Networking Conference (WCNC)* (IEEE), pp 1–6.

[30] Afeef L, Arslan H (2022) Beam squint effect in multi-beam mmwave massive mimo systems. *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)* (IEEE), pp 1–5.

[31] Zaidi AA, Baldemair R, Tullberg H, Bjorkegren H, Sundstrom L, Medbo J, Kilinc C, Da Silva I (2016) Waveform and numerology to support 5g services and requirements. *IEEE Communications Magazine* 54(11):90–98.

[32] Zhang X, Zhang L, Xiao P, Ma D, Wei J, Xin Y (2018) Mixed numerologies interference analysis and inter-numerology interference cancellation for windowed ofdm systems. *IEEE Transactions on Vehicular Technology* 67(8):7047–7061.

[33] Marijanović L, Schwarz S, Rupp M (2020) Multiplexing services in 5g and beyond: Optimal resource allocation based on mixed numerology and mini-slots. *IEEE Access* 8:209537–209555.

[34] Lin Z, Li J, Zheng Y, Irukulapati NV, Wang H, Sahlin H (2018) Ss/pbch block design in 5g new radio (nr). *2018 IEEE Globecom Workshops (GC Wkshps)* (IEEE), pp 1–6.

[35] Elgendi H, Mäenpää M, Levanen T, Ihalainen T, Nielsen S, Valkama M (2019) Interference measurement methods in 5g nr: Principles and performance. *2019 16th International Symposium on Wireless Communication Systems (ISWCS)* (IEEE), pp 233–238.

[36] Boulouird M, Riadi A, Hassani MM (2017) Pilot contamination in multi-cell massive-mimo systems in 5g wireless communications. *2017 international conference on electrical and information technologies (ICEIT)* (IEEE), pp 1–4.

[37] Qin Z, Yin H (2023) A review of codebooks for csi feedback in 5g new radio and beyond. *arXiv preprint arXiv:230209222* .

[38] 3GPP Technical Specification Group Radio Access Network (2020) TS 36.211: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation; Rel.16, sixteenth ed. (3GPP), Technical specification.

[39] 3GPP Technical Specification Group Radio Access Network (2019) TR 38.828: Cross Link Interference (CLI) Handling and Remote Interference Management (RIM) for NR; (Release 16), sixteenth ed. (3GPP), Technical specification.

[40] Liu F, Pan J, Zhou X, Li GY (2021) Atmospheric ducting effect in wireless communications: Challenges and opportunities. *Journal of Communications and Information Networks* 6(2):101–109.

[41] 3GPP Technical Specification Group Radio Access Network (2019) TR 38.866: Study on Remote Interference Management for NR (Release 16), sixteenth ed. (3GPP), Technical specification.

[42] Elijah O, Leow CY, Rahman TA, Nunoo S, Iliya SZ (2015) A comprehensive survey of pilot contamination in massive mimo—5g system. *IEEE Communications Surveys & Tutorials* 18(2):905–923.

[43] Ioushua SS, Eldar YC (2020) Pilot sequence design for mitigating pilot contamination with reduced rf chains. *IEEE Transactions on Communications* 68(6):3536–3549.

[44] Ng BL, Chandrasekhar V, Nam YH, Kim J (2018) Beam management of downlink data channel and downlink control channel for 5g next radio systems. US Patent 10,148,337.

[45] Bharucha Z, Auer G, Abe T (2011) Downlink femto-to-macro control channel interference for lte. *2011 IEEE Wireless Communications and Networking Conference* (IEEE), pp 1259–1264.

[46] Cariou L, Stacey R (2018) Report for inter-bss interference avoidance. US Patent App. 15/384,934.

[47] Kim R, Kim Y, Lim H (2017) Inter-bs interference-aware transmission coordination for millimeter wave networks. *IEEE Wireless Communications Letters* 6(3):350–353.

[48] Boccardi F, Shokri-Ghadikolaei H, Fodor G, Erkip E, Fischione C, Kountouris M, Popovski P, Zorzi M (2016) Spectrum pooling in mmwave networks: Opportunities, challenges, and enablers. *IEEE Communications Magazine* 54(11):33–39.

[49] Foegelle MD (2019) New and continuing measurement challenges for 5g mmwave and beamforming technologies. *2019 13th European Conference on Antennas and Propagation (EuCAP)* (IEEE), pp 1–5.

[50] Mailloux RJ (2017) *Phased array antenna handbook* (Artech house).

[51] O-RAN Working Group 2 (2021) O-RAN Non-RT RIC: Functional Architecture 1.01 (Open RAN (O-RAN) Alliance), Technical specification.
[52] O-RAN Working Group 2 (2024) O-RAN A1 interface: Application Protocol 4.02 (Open RAN (O-RAN) Alliance), Technical specification.
[53] O-RAN Working Group 2 (2024) A1 interface: Type Definitions (Open RAN (O-RAN) Alliance), Technical specification.
[54] O-RAN Working Group 2 (2024) O-RAN R1 interface: General Aspects and Principles 8.0 (Open RAN (O-RAN) Alliance), Technical specification.
[55] O-RAN Working Group 2 (2024) O-RAN R1 interface: Application Protocols for R1 Services 5.0 (Open RAN (O-RAN) Alliance), Technical specification.
[56] O-RAN Working Group 2 (2024) O-RAN Type Definitions for R1 Services 2.0 (Open RAN (O-RAN) Alliance), Technical specification.
[57] O-RAN Working Group 3 (2024) O-RAN E2 Application Protocol (E2AP) 5.0 (Open RAN (O-RAN) Alliance), Technical specification.
[58] 3GPP (2024) TS 28.55: Management and orchestration; 5G performance measurements (3GPP), Technical specification.
[59] 3GPP (2024) TS 32.425: Telecommunication management; Performance Management Performance managements (3GPP), Technical specification.