Review

Not peer-reviewed version

A Comprehensive Survey on 5G RedCap: Technologies, Security Vulnerabilities, and Attack Vectors

Pavan Raja I , Kurunandan Jain * , Hari N.N , Sethu Subramanian N , Prabhakar Krishnan

Posted Date: 24 December 2025

doi: 10.20944/preprints202512.2156.v1

Keywords: 5G; Reduced Capability (RedCap); eRedCap; Internet of Things (IoT); 3GPP Release 17; 3GPP Release 18; cellular IoT; Low-Power Wide-Area (LPWA)

 doi:10.20944/preprints202512.2156.v1

Article

A Comprehensive Survey on 5G RedCap: Technologies, Security Vulnerabilities, and Attack Vectors

Pavan Raja I, Kurunandan Jain *, Hari N N, Sethu Subramanian N and Prabhakar Krishnan

Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam, Kerala, India
* Correspondence: kurunandanj@am.amrita.edu

Abstract

The 5th Generation New Radio (5G NR) evolution has mainly been focused on three pillars: enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC). While eMBB and URLLC focus on high-performance applications and mMTC cater for low-power and low-throughput massive IoT, a considerable void has appeared in price performance ratio for mid-level IoT use cases. Examples of such use cases include industrial sensors, wearables, and video surveillance, all of which call for more than conventional mMTC technologies such as NB-IoT and LTE-M can offer but do not need the full and usually expensive complexity of eMBB/URLLC devices. To bridge this gap, Release 17 introduced Reduced Capability (RedCap) NR, with Release 18 further enhancing it. This survey systematically reviews 5G RedCap technology. It initially gives an account of the cellular IoT landscape, setting the agenda of the unique niche RedCap fills. A thorough technical dive into Release 17 and 18 core specifications then follows, highlighting the key methods of reducing complexity: bandwidth reduction, reduced antenna configurations, half-duplex FDD operation, and power-saving e nhancements. This paper further explores the architectural impacts on the 5G network, such as BWP operation, and initial access procedures. Then detailed analyses that relate RedCap features to specific application requirements for industrial IoT, wearables, and smart cities are offered. Performance data from academia and industry reports are consolidated in this survey to give a quantitative comparison of RedCap against other cellular technologies in specific K PIs. Finally, deployment challenges are outlined, a bibliometric analysis of the current research landscape is undertaken, and concrete future directions are proposed to pave the way for further development of this important 5G IoT technology.

Keywords: 5G; Reduced Capability (RedCap); eRedCap; Internet of Things (IoT); 3GPP Release 17; 3GPP Release 18; cellular IoT; Low-Power Wide-Area (LPWA)

1. Introduction

From a high-level perspective, 5G was envisioned to not just connect people but with farther-reaching applications to connect a fathomless, huge, and heterogenous landscape of machines, devices, and sensors-infrastructuring the IoT era [1,2]. The initial 5G NR standard was based on the three service types featured within the UTRA Family of IMT-2020 specification as defined by the ITU and standardized in 3GPP Release 15: eMBB, URLLC, and mMTC.

eMBB primarily delivers data rates of gigabits for applications like HD video streaming and AR/VR experiences. URLLC is for mission-critical applications requiring extremely low latencies and high reliabilities such as industrial automation and autonomous driving [3,4]. On the other end of the spectrum, mMTC, primarily served by technologies like NB-IoT and LTE-M, aims to connect the billions of low-complexity, low-power devices that send very little data, very infrequently—the likes of smart meters and asset tracking [5].

 doi:10.20944/preprints202512.2156.v1

Whereas this triad has been largely successful at covering the extreme ends of the coverage spectrum, with time a large gap has widened in the middle. A large and continuously growing set of IoT use cases, including high-end wearables, industrial wireless sensors, and smart grids, have needs that fall within the unsold middle ground between traditional mMTC and the high-performance pillars of eMBB/URLLC [6]. Such mid-tier applications are too complex for the low data rates and higher latencies supported by NB-IoT/LTE-M, yet they do not require the high performance, with the associated high costs, increased complexity, and huge power consumption, of conventional 5G NR devices designed for eMBB.

For an illustration, consider that a standard 5G NR device is required to support a minimum bandwidth of 100 MHz, while more than likely, it would be equipped with four receive antennas. This over-qualifies many of these IoT applications and makes it economically unviable. Thus, the farther-higher mid-tier market segment demands are signalling elicited for a 5G-native solution [7,8].

Support will be provided now to close that gap in terms of capability and complexity when the 3GPP introduced in Release 17 a new generation of devices under the name of Reduced Capability NR or NR-Light. RedCap has been designed to bridge the compromise by dialing down the complexity of 5G NR but keeping core benefits like low latency and working with 5G Standalone (SA) architecture. It somewhat works on the logic of cutting down device bandwidth, limiting the number of antennas, relaxing modem processing requirements, and adding better power-saving features so that it can somewhat compete with mid-range LTE categories (such as LTE Cat-1/Cat-4) in terms of performance, yet within the evolutionary and future-proof 5G native framework.

The enhancement in complexity reduction and targeting replacement of legacy LTE Cat-1/1bis devices aptly concluded the 5G IoT technology portfolio in the subsequent version 18 of 3GPP that also brought along enhanced RedCap (eRedCap). This, thus, places RedCap at the center stage to be the key enabling technology mass adoption for 5G IoT and the main migration path for services currently running on legacy 2G, 3G, and 4G networks.

1.1. Research Gap and Motivation

While RedCap technology has become standardized and its ecosystem of chipsets, modules, and devices is rapidly maturing, academic literature has not yet offered a holistic and comprehensive synthesis of the technical specifications, performance characteristics, application domains, and deployment challenges [9]. Previous studies went into selected issues, such as coverage analysis via simulation, power consumption modeling via analytical methods, or maximizing uplink performance [10–12]. Industry white papers from significant stakeholders such as GSMA, Qualcomm, and Ericsson provide invaluable insights into technical specifications and performance targets. However, there seems to be a need for a survey that brings all those pieces together, evaluates the technology from a system-level vantage point, and clearly sets an outlook before the research community and industry stakeholders.

This work fills this glaring gap by systematically reviewing and synthesizing the foundational concepts of RedCap stemming from 3GPP Releases 17 and 18, carrying out a performance analysis grounded in both theoretical specifications and empirical data, and then moving on to sketch the potential metamorphosis of a wide range of IoT applications.

1.2. Contributions

This paper comprehensively surveys 5G RedCap technology from its inception to its potential evolutionary path. The broad contributions are as follows:

- **A Holistic Technical Overview:** A detailed, multi-layered technical deep-dive into RedCap that synthesizes specifications from 3GPP Release 17 and enhancements for eRedCap in Release 18 is, in fact, produced. This also clearly covers main complexity reduction techniques and their implications on device design and network architecture.

 doi:10.20944/preprints202512.2156.v1

- **Novel Taxonomy of Use Cases and Applications:** We propose a detailed taxonomy of RedCap use cases covering the main verticals of Industrial IoT, wearables, video surveillance, and smart cities. An exhaustive table maps specific application requirements to RedCap technological features explicitly, thus providing a clear guide for developers and system integrators.
- **Quantitative Performance Synthesis and Comparison:** Our survey is the first-ever comparative performance analysis synthesizing quantitative data from disparate sources, comprising academic simulation works, industry white papers (Qualcomm, Ericsson, et al.), and empirical test results. We build comparative tables and charts to juxtapose RedCap against LTE-M, NB-IoT, and traditional 5G NR for key performance indicators (KPI) such as throughput, latency, battery life, and device cost.
- **Bibliographic Analysis and Future Research Agenda:** We carry out a bibliographic analysis of the surveyed literature for mapping the existing research landscape, identifying the main contributors as well as publication trends. Subsequently, based on a thorough evaluation of the technology's capabilities as well as deployment challenges (such as reliance on 5G SA and spectrum management), we propose an exact, concrete, and actionable future research agenda meant to fill the open-ended questions and guide the subsequent phase of RedCap's evolution.

1.3. Paper Organization

The remainder of this survey is structured to provide a logical and comprehensive exploration of 5G RedCap.

- Section 2 provides essential context by situating RedCap within the broader landscape of cellular IoT technologies, performing a comparative analysis against eMBB, URLLC, LTE-M, and NB-IoT to highlight the mid-tier gap it addresses.
- Section 3 offers a detailed technical deep-dive into the foundational specifications of RedCap as defined in 3GPP Release 17, covering bandwidth, antenna configurations, duplexing modes, and power-saving features.
- Section 4 details the evolution to enhanced RedCap (eRedCap) in 3GPP Release 18, explaining the motivations and technical enhancements targeting lower-tier IoT use cases.
- Section 5 explores the key enabling technologies and the architectural impact of RedCap on the 5G network, including BWP operation, initial access, and RAN resource management.
- Section 6 categorizes key use cases including industrial sensors, wearables, and video surveillance mapping their specific requirements to RedCaps capabilities.
- Section 7 focuses on quantitative performance analysis, synthesizing and comparing performance data for RedCap against other cellular technologies across critical KPIs.
- Section 8 investigates the security landscape, identifying specific vulnerabilities arising from RedCap's protocol design and resource constraints, along with countermeasures.
- Section 9 identifies and discusses the key deployment challenges and proposes specific future research directions for the academic and industrial communities.
- Section 10 provides a bibliographic analysis of the surveyed literature, visualizing publication trends and research themes.
- Section 11 concludes the paper by summarizing the key findings and offering a forward-looking perspective on the transformative potential of 5G RedCap.

2. The Landscape of Cellular IoT Technologies

The rise of IoT has given rise to a vast and heterogeneous family of cellular technologies for supporting a wide variety of device types and their respective application needs [13]. The 5G framework, as envisaged by IMT-2020, is expected, therefore, to act as the sole platform serving multitude diversity through its three service pillars, i.e., eMBB, URLLC, and mMTC. To understand the property that 5G RedCap offers uniquely, one should understand the varied nature and constraints imposed by these pillars and their 4G-NR alike.

 doi:10.20944/preprints202512.2156.v1

2.1. A Comparative Overview

Cellular IoT technologies usually can be classified based on parameters that determine their general performance: data rate, latency, device complexity, cost, and battery life.

- **High-Performance 5G (eMBB and URLLC)**: At the peak of the spectrum, the highest performance category is for eMBB and URLLC applications that serve the most demanding application requirements.
  - *Enhanced Mobile Broadband (eMBB):* This pillar is an evolution of 4G LTE and is designed to provide extremely high data rates, high network capacity, and maximum spectral efficiency. Correspondingly, applications that require multi-Gbps throughput such as 4K/8K video streaming, virtual reality (VR), and fixed wireless access (FWA) are targeted for eMBB. Fast performance comes at the price of complicated implementations, including support for wide bandwidths (up to 100 MHz in FR1, 400 MHz in FR2), advanced MIMO antenna configurations (e.g., 4Rx), and high-order modulation schemes (e.g., 256QAM). These high complexities result in device costs and power consumption levels intolerable for most IoT devices that are battery-powered or price-sensitive.
  - *Ultra-Reliable Low-Latency Communications (URLLC):* This latter pillar is built for mission-critical applications that require utmost data integrity and very short timing for data delivery. URLLC applications demand strong connectivity with less than 1 ms latency and an availability of "five-nines" or 99.999% and higher reliability. Typical applications may include industrial automation, remote surgery, and vehicular communications (V2X). Although ground-breaking, URLLC requires devices that are sophisticated and network features that are highly complex; thus, it is economically and technical-wise impractical for the vast majority of IoT applications.
- **Low-Power Wide-Area (LPWA) Technologies (mMTC)**: The LPWA technologies form the far end of the spectrum for the mMTC pillar. These are meant to maximize the number of simple, low-cost devices connected over large geographical areas, with special emphasis on long battery life.
  - *Narrowband-IoT (NB-IoT):* Standardized in Release 13 by the 3GPP, NB-IoT makes use of extremely narrow bandwidth (200 kHz) to obtain good coverage and deep indoor penetration. It was created for fixed or low-mobility devices sending very tiny packets of data (tens of kbps) dropped at great intervals, such as in smart utility meters, environmental sensors, and agricultural monitors. Its advantages chiefly include an extremely low device cost and a battery life of more than ten years. However, the data rate and latency limitations of NB-IoT prevent it from being used in applications that require more responsive or data-intensive communication.
  - *LTE-M (eMTC):* Also introduced in Release 13, LTE-M officially defines a better performing alternative to NB-IoT. Under operation within 1.4 MHz bandwidth, it supports higher data rates (up to 1 Mbps) with appreciable low latencies and coverage. More importantly, it entertains mobility and voice communication (voice over LTE or VoLTE), which basically opens this technology to implementation scenarios like asset trackers, wearables, and alarm panels.

  In Release 15 onward, both NB-IoT and LTE-M were declared a very much integral part of the 5G mMTC world, able to work in-band with 5G NR and connect to 5G Core (5GC).

2.2. Identifying the Mid-Tier IoT Gap

Plotting these technologies on a multi-axes chart that compares KPIs portrays a lacuna plainly. As shown in Figure 1, eMBB and URLLC lead in data rate and latency but suffer from high complexity and cost and power consumption. The very opposite is the case for NB-IoT and LTE-M, which are being designed to be cost-effective and battery-conservative while facing a heavy bottleneck in throughput

 doi:10.20944/preprints202512.2156.v1

and latency. This huge "middle ground" constitutes applications that are being underadapted by these extremes. For example, higher-date-rate video surveillance, smart grid control, industrial process monitoring, and advanced wearables require:

- More data rate than LTE-M (for example, several Mbps for video feeds).
- A much lower latency than LPWA technologies so as to implement real-time control and monitoring.
- A cost and level of complexity much lower than 5G NR eMBB/URLLC devices.
- Power efficiency that must be higher than eMBB so as to accommodate battery-powered or compact form-factor requirements.

Before RedCap came into the picture, such use cases mainly fell into the cat of legacy LTE technologies, such as LTE Cat-1/1bis and Cat-4 [14].

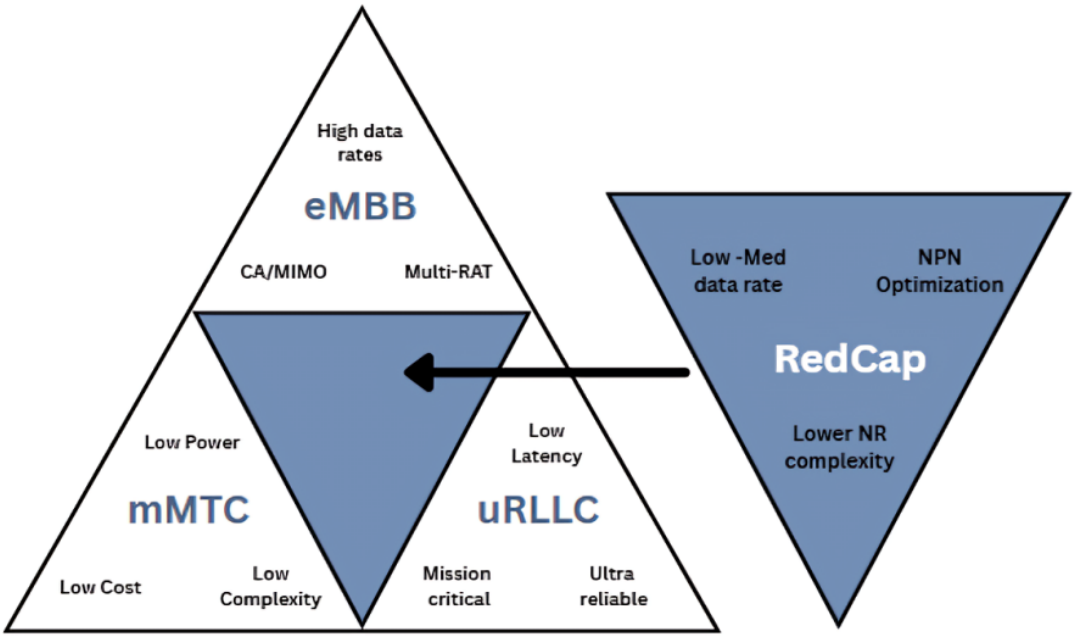

Figure 1. The Cellular IoT Landscape.

LTE Cat-1 supports data rates of up to 10 Mbps downlink and 5 Mbps uplink, whereas LTE Cat-4 has data rates up to 150 Mbps downlink and 50 Mbps uplink. While being somewhat effective, these do not really possess the inherent advantages of the 5G SA architecture, namely network slicing, enhanced positioning, and future-proof evolution path. And on the other hand, relying on older fourth-generation infrastructure poses long-term challenges for operators who would be aggressively refarming spectrum from 4G to 5G.

2.3. RedCap: The Purpose-Built Mid-Tier Solution

5G RedCap was introduced in 3GPP Release 17 precisely to fill this mid-tier gap within the 5G ecosystem. As illustrated in Figure 1, RedCap was intended as a solution for balanced characteristics:

- Data rate-wise, similar to LTE Cat-4, with peak theoretical rates of 150 Mbps downlink and 50 Mbps uplink, sufficient for streaming video and industrial data aggregation [15].
- Latency-wise, orders better than LPWA technologies and comparable to LTE to such an extent that near-real-time control actuations can be executed.
- Complexity and cost-wise, order(s) less than eMBB/URLLC devices, due to lower bandwidth, number of antennas, simplifications, etc., with cost-parity with LTE Cat-4 modules [16,17].

 doi:10.20944/preprints202512.2156.v1

- Power-wise, markedly better than eMBB devices through dedicated power-saving features such as extended DRX (eDRX), and thus fit for battery-powered equipment like wearables and remote sensors.

What RedCap does within the 5G SA architecture is therefore not only to provide a perfect replacement for mid-tier LTE but also to bring in some new 5G native features for these applications such as network slicing and improved positioning. The subsequent introduction of eRedCap in Release 18 extends this strategy to the lower-performance tiers by targeting the replacement of LTE Cat-1 and therefore providing a further cost- and power-optimized solution. In concert, RedCap and eRedCap shall fill in the 5G IoT landscape to allow mobile network operators to cater to IoT use cases covering the whole spectrum with a single forward-looking technology standard.

3. Foundations of 5G RedCap: 3GPP Release 17

5G RedCap's formal introduction in 3GPP Release 17 was, indeed, a landmark step in the evolutionary development of 5G for IoT. The primary goal was to define a new User Equipment (UE) type that systemically reduces complexity, cost, and power consumption in comparison to a baseline 5G NR device, yet with adequate performance for mid-level applications. Through a careful selection of technical specifications that restrict capabilities in five major aspects, namely device bandwidth, number of antennas, modem processing, duplex operation, and power-saving mechanisms, this was realized [18–20]. The section will provide a technical deep dive into these Release 17 RedCap foundational features.

3.1. Bandwidth Reduction

To support very wide channel bandwidths, a standard NR device must be capable of operating with up to 100 MHz of bandwidth in Frequency Range 1 (FR1, sub-7 GHz) and up to 400 MHz in Frequency Range 2 (FR2, mmWave). This means that extremely complex and power-hungry RF front-end and baseband processors are needed. Release 17 RedCap slashes this requirement in an effort to lower device complexity. The specification demands a reduced maximum UE bandwidth of:

- 20 MHz in FR1 (sub-7 GHz bands)
- 100 MHz in FR2 (mmWave bands)

Reducing bandwidth requirements thereby simplified the RF filter design and buffer sizes while lowering baseband processing demands, which equated to direct cost and power savings. The coexistence mechanism for RedCap UE with normal NR devices located on a broader carrier (for instance, 100 MHz) is operated through Bandwidth Part (BWP) whereby this concept is natively supported by 5G NR such that devices monitor only a portion of the total cell bandwidth. In order to simplify device design, Release 17 RedCap UEs are not, by default, required to support Carrier Aggregation (CA) or Dual Connectivity (DC), i.e., they do not operate on two carriers simultaneously.

3.2. Reduced Number of Antennas and MIMO Layers

Another major complexity driver in baseline NR UEs is the mandatory support for multiple receive antennas to enable advanced MIMO schemes. Depending on the frequency band, a baseline NR UE must support at least two or even four receive (Rx) antenna branches. This would increase the device's size, cost, and power consumption—especially in terms of RF chains and processing requirements. RedCap alleviates such requirements by significantly relaxing them. A Release 17 RedCap UE has reduced number of antennas defined as follows:

- **Tx Antennas**: A RedCap UE shall only be required to support a single (1T) transmit antenna, which means that UL MIMO and transmit diversity are not supported.
- **Rx Antennas**: In FR1, a RedCap UE may implement either 1R or 2R. The 1R configuration has the largest reduction in cost and size and may be aimed at small wearables and sensors. The 2R option provides better downlink performance through receive diversity. In FR2, a minimum of 2R is mandatory.

 doi:10.20944/preprints202512.2156.v1

Reduction in antenna count also reduces the number of downlink MIMO layers supported. A 1T1R device can only support one downlink data stream (1 layer), while a 1T2R device can optionally support two downlink layers for higher throughput. This means that, in terms of peak theoretical data rate, the RedCap device is not as good as a 4-layer baseline device, but the performance is good enough for the target use cases of RedCap and facilitates a big reduction in device complexity. It should however be noted that fewer receive antennas translate to suboptimal spectral efficiency from the network perspective, as radio resources will be consumed insufficiently compared to a more capable MIMO device for delivering the same amount of data [21].

3.3. Relaxation of Modem Processing and Capabilities

Other than that, Release 17 defines several relaxations in modem processing and some other high-level capabilities to further simplify and reduce the cost of the RedCap baseband.

- **Modulation Order**: Baseline NR is required to be capable of supporting 256 quadrature amplitude modulation (256-QAM) to achieve the highest data throughput under good signal conditions. This requirement is relaxed for RedCap UEs. For RedCap, the NR specification requires 64QAM as the highest modulation that must be supported; 256QAM is optional in the case of higher-performing RedCap devices. Putting a constraint on the mandatory modulation order basically eases the demodulation and decoding logic within the modem, which in turn helps in cost as well as power savings.
- **Upper Layer Capabilities**: At the higher layer of the protocol stack, complexity is also reduced. For instance, the mandatory user equipment (UE) number of Data Radio Bearers (DRBs) supported shall be reduced from 16 to 8. Also, the length of the sequence number (SN) field for the Packet Data Convergence Protocol (PDCP) and Radio Link Control (RLC) layers can be shortened from 18 bits to 12 bits, reducing memory requirements.

3.4. Half-Duplex FDD (HD-FDD) Operation

In a standard Frequency Division Duplex (FDD) system, UEs can transmit uplink data signals and receive downlink data signals simultaneously at different frequencies. This type of simultaneous operation is called full-duplex (FD-FDD). It requires quite an expensive and bulky element, known as a duplexer, which is otherwise used to isolate the high-power transmitted signal from the sensitive receiver circuitry. Release 17 makes HD-FDD optional for RedCap UEs. In HD-FDD mode, however, simultaneous transmission and reception are prohibited; instead, the UE alternates between uplink transmission and downlink reception in the time domain. With the duplexer eliminated, it can be replaced with simpler and cheaper RF switches, bringing the following significant benefits:

- **Cost and Size Reduction**: The elimination of duplexers means a much smaller bill of materials (BOM) and smaller device footprint, which is the most crucial element for compact devices such as wearables.
- **Easier Multi-Band Support**: Since there is no band-specific duplexer, it becomes easier for manufacturers to create devices supporting multiple frequency bands, thus reducing the number of product variants.

The trade-off HD-FDD offers is that peak throughput may potentially be reduced (approximately halved when compared to FD-FDD) and an increase in latency of the device waiting time until it gets its joint time slot to either transmit or receive. However, for many middle-tier IoT applications, this trade-off would be well worth the cost and size savings.

3.5. New Power-Saving Features

Extending battery life is always under great scrutiny for many IoT scenarios. Although baseline NR already has several mechanisms for power saving, Release 17 brings forth enhancements beneficial to RedCap devices, inspired by tried-and-true LPWA technology [22]:

 doi:10.20944/preprints202512.2156.v1

- **Extended Discontinuous Reception (eDRX)**: The Discontinuous Reception (DRX) mechanism enables a UE to power down its receiver circuitry periodically to save power. Under baseline NR, the maximum DRX cycle in the RRC IDLE state is 2.56 seconds. Release 17 adds eDRX for RedCap, supporting much longer sleep cycles [23]:
  - *RRC IDLE State:* Maximum allowed eDRX cycle has been multiplied to 10,485.76 seconds (around 2.91 hours).
  - *RRC INACTIVE State:* Maximum allowed eDRX cycle of 10.24 seconds.

  The years-of-battery life trade-off means ultra-low average power consumption for devices that only need to be reachable from the network infrequently, such as certain sensor applications, though increased latency downstream does occur while the device is unreachable in its sleep cycle.
- **Relaxed Radio Resource Management (RRM) Monitoring**: For good mobility, a connected UE is usually required to keep performing RRM measurements on the serving and neighboring cells. It is highly energy-consuming. Many RedCap use cases, though, are stationary (for example, industrial sensors) or bear low mobility (e.g., wearables).

Release 17 allows RedCap UEs to perform "relaxed RRM monitoring" by which they can do such neighbor-cell measurements less frequently whenever certain conditions are met, e.g., when being stationary or when not being at the cell edge [24,25]. This reduces the activity period of the receiver, and that will entail huge energy savings without compromising connectivity of low-mobility devices.

Table 1. Summary of Key 5G RedCap Features in 3GPP Release 17.

Feature Category	Release 17 Specification	Primary Benefit
Bandwidth	Max 20 MHz in FR1; 100 MHz in FR2. No Carrier Aggregation (CA) or Dual Connectivity (DC).	Reduced RF front-end complexity, lower power consumption, lower device cost
Antennas / MIMO	1Tx mandatory. 1Rx or 2Rx in FR1; 2Rx in FR2. Max 1 or 2 downlink MIMO layers depending on Rx antennas.	Reduced device size and cost, simpler RF chain. Ideal for compact form factors like wearables.
Modem Processing	64QAM mandatory for downlink; 256QAM optional. Reduced number of DRBs (from 16 to 8).	Lower baseband processing requirements, reduced modem cost, and lower power consumption.
Duplex Operation	Half-Duplex FDD (HD-FDD) supported as an option.	Eliminates need for expensive duplexer, significantly reducing cost and size, simplifying multi-band support.
Power Saving	Extended DRX (eDRX) cycles up to approx. 2.9 hours in RRC IDLE. Relaxed RRM monitoring for stationary/low-mobility devices.	Drastically extended battery life (potentially years for some applications), making RedCap suitable for battery-powered sensors and wearables.

4. The Evolution to Enhanced RedCap (eRedCap): 3GPP Release 18

While Release 17 successfully established RedCap as the 5G solution for mid-tier IoT use cases (approximately on the same scale as LTE Cat-4), the industry-consciousness for an even leaner and cheaper 5G variant remained. Many IoT applications currently served by the lowest categories of LTE mainly LTE Cat-1 and Cat-1bis-would not require the approximate 150 Mbps peak data rates of Rel-17 RedCap. These use cases basically put a premium on cost and power efficiency rather than throughput. To target this side of things and to complete the 5G migration path for all legacy cellular IoT technologies, 3GPP has taken the initiative under Release 18, the first release under the "5G-Advanced" moniker, to work on eRedCap [26]. The primary objective of the eRedCap work item

 doi:10.20944/preprints202512.2156.v1

was to optimize UE complexity and power consumption from Rel-17 up to a peak data rate of 10 Mbps. This evolution is backward compatible with Rel-17 RedCap networks while providing new features to achieve further cost and form-factor reductions, improved battery life, hence putting eRedCap as the direct 5G successor of LTE Cat-1.

4.1. Motivation for eRedCap

The development of eRedCap was driven by a number of motivations, among them:

- **Targeting Legacy LTE Replacement**: A great part of cellular IoT market relies on LTE Cat-1 (DL: 10 Mbps ; UL: 5 Mbps) and Cat-1bis (single antenna variant) for point-of-sale terminals, smart metering, and vehicle telematics applications. eRedCap was hence concretely designed to deliver similar performance in the 5G SA realm for them to have an explicit and future-proof migration path for the widespread deployment of these devices.
- **Further Cost Reduction**: While Rel-17 RedCap brought major cost reductions over baseline NR, eRedCap wants to push cost reductions even further down to a point where it is almost as cheap as LTE Cat-1 modules. Cost is a key for mass market uptake in cost-conscious IoT verticals.
- **Enhanced Power Efficiency**: For many battery-powered IoT devices, longevity is the single-most important parameter. eRedCap bring further optimizations to the power saving mechanisms to accommodate devices that are supposed to be in operation in the field for many years with little maintenance.
- **Enabling New Use Cases**: Drop the thresholds for performance, cost, and power consumption, and this immediately opens up new 5G use cases that were previously not even at the verge of economic or technical feasibility-large scale deployments on smart grids, environmental monitoring.

4.2. Key Technical Enhancements in Release 18

The eRedCap specification in Release 18 builds upon the foundation of Rel-17 RedCap, introducing several targeted enhancements to achieve its goals.

- **Reduced Peak Data Rate and UE Bandwidth**: Reducing peak data rate is the defining characteristic of eRedCap. In other words, classifying eRedCap as a specification targets a peak rate of 10 Mbps in downlink as well as uplink. This reduction is central to the design as it permits a gross simplification in the UE's baseband and RF aspects. Two main types of techniques have been designed to achieve these goals:
  1. Lower Data Rate Capping: The UE can be capped at 10 Mbps peak rate even while Operation within 20 MHz BWP, similar to that of a Rel-17 device.
  2. Optional UE Bandwidth of 5 MHz: Release 18 introduces, for data channels (PDSCH and PUSCH) in FR1, a new optional narrower UE bandwidth of 5 MHz.

  While the UE still needs to be capable of receiving control signals over a 20 MHz channel to ensure backwards compatibility with network broadcasts, its data processing pipeline can get optimized for a much narrower bandwidth allowing further cost and power savings.
- **Relaxed UE Processing Timelines**: To suit simpler and less expensive processors, Release 18 incorporates a relaxation of UE processing timelines for eRedCap devices. For instance, the timers for the UE to process downlink control information and to respond with an uplink transmission can be extended. Relaxation is also provided for random access procedure. PRBs needed for some random access messages may be above that in a 5 MHz bandwidth; consequently an additional slot could be required and the timeline for this procedure was accordingly relaxed for eRedCap UEs.
- **Positioning Enhancements**: While Rel-17 RedCap supports baseline 5G positioning methods, Rel-18 enhances positioning support in RedCap devices adapting for their reduced capabilities. The work in Rel-18 focuses on defining performance requirements and potential improvements. The next releases will be expected to continue to build on this activity, further enhancing M-RTT and

 doi:10.20944/preprints202512.2156.v1

AoD/AoA techniques for RedCap devices to facilitate easier accurate positioning for a much wider range of IoT applications [27]. Sidelink positioning is also a key area for further development and allows direct device-to-device range measurements which may be more pertinent for asset tracking and proximity services.

- **Enhanced Power Saving**: Release 18 further enhances power saving introduced in Rel-17, one of the key features being the extension of the maximum allowed eDRX cycle between two paging occasions for UEs in the RRC INACTIVE state; while Rel-17 limited the maximum allowed eDRX cycle between paging occasions for UEs in the RRC INACTIVE state to 10.24 seconds, Release 18 increases this to the maximum allowed eDRX cycle between paging occasion for UEs in the RRC IDLE state which is approximately 2.91 hours. This enables devices requiring quick reachability (which is a key advantage of RRC INACTIVE) to leverage extraordinarily long sleep cycles, thus providing a better trade-off between responsiveness and battery life.

4.3. Coexistence and Network Identification

Similar to Rel-17 RedCap, eRedCap devices are supposed to coexist with baseline NR and Rel-17 UEs on the same network. To be able to manage such heterogeneity, the network shall be able to distinguish the types of devices present. Release 18 introduces a new Radio Access Technology (RAT) type for eRedCap devices so that Mobile Network Operators (MNOs) can apply specific policies to eRedCap UEs regarding access control, resource allocation, and roaming management, all to ensure that network resources are efficiently and appropriately assigned with respect to each device class. The network may also limit access based on the UE's supported number of receive antennas, thereby creating another layer of finer control.

Table 2. Comparison of 3GPP Rel-17 RedCap and Rel-18 eRedCap.

Parameter	Release 17 RedCap	Release 18 eRedCap
Target LTE Equivalent	LTE Category 4 (150/50 Mbps)	LTE Category 1 (10/5 Mbps)
Peak Data Rate	150 Mbps DL / 50 Mbps UL	10 Mbps DL / 10 Mbps UL
UE Bandwidth (FR1)	20 MHz	20 MHz (control) with optional 5 MHz for data channels
UE Antennas (FR1)	1T/1R or 1T/2R	1T/1R or 1T/2R (Primarily targeting 1T/1R for lowest cost)
eDRX (RRC INACTIVE)	Max cycle of 10.24 seconds	Max cycle extended TO 2.91 hours (matches RRC IDLE)
Processing Timeline	Baseline NR timelines	Relaxed processing timelines for RACH and data scheduling
Positioning	Support for baseline NR positioning methods.	Initial performance requirements defined; paves the way for future enhancements like sidelink positioning.
Network Identification	"NR REDCAP" RAT Type	New, distinct "eRedCap" RAT Type for more granular network policies.

5. Key Enabling Technologies and Architectural Impact

The operation of RedCap 5G devices successfully relies on the 5G Radio Access Network (RAN) and Core Network (5GC) specific mechanisms that support the limited functionalities of the devices [28]. Even though the RedCap UEs are more straightforward compared to the basic NR devices, the network architecture needs to be intelligent and flexible enough to manage these devices efficiently without compromising the quality of other services [29]. This section introduces the key enabling technologies and architectural considerations for integrating RedCap into a Standalone (SA) 5G

 doi:10.20944/preprints202512.2156.v1

network, particularly focusing on Bandwidth Part (BWP) operation, initial access procedures, and RAN resource management.

5.1. Bandwidth Part (BWP) Operation for RedCap

A fundamental design principle of 5G NR is its ability to operate over very wide carrier bandwidths (e.g., 100 MHz in FR1). However, as detailed in Section 3, RedCap UEs are limited to a much narrower maximum bandwidth (20 MHz in FR1 for Rel-17, with a 5 MHz data channel option for Rel-18). The mechanism that reconciles this difference is the Bandwidth Part (BWP). A BWP is a contiguous subset of the total carrier bandwidth that a UE is configured to operate on at a given time. This concept is central to RedCap's ability to coexist with high-performance eMBB devices on the same wide carrier.

- **Initial Access BWP**: Connecting for the first time, a RedCap UE needs to discover a BWP whose width is not greater than 20 MHz. The standard is this: The network provides with the system information (SIB1) the initial BWP or even more than one. In order not to compel all the gadgets to a tight BWP, the Release 17 has offered the option of a particular BWP configured for the network, RedCap-specific initial BWP. The operator usually locates this BWP at the fringe of the carrier in order not to cause fragmentation of frequency resources for the wideband eMBB UEs. And most importantly, this RedCap-specific initial BWP can be configured without its own synchronization signals (SSB). The UE can then pick up timing and synchronization from the main cell's SSB and then tune in to the narrower RedCap BWP.
- **Dedicated BWP in Connected Mode**: When a RedCap UE is in RRC CONNECTED state, the network can, in fact, configure it with one or more BWPs dedicated to its traffic patterns and capabilities. For example, a device can be assigned a very narrow BWP during times of low activity to save power; and as the demand for throughput increases, the device can be switched to a wide BWP (up to its 20 MHz maximum). This is indeed very dynamic BWP adaptation, which contributes significantly to power and spectral efficiency optimization for RedCapdevices.
- **BWP for eRedCap**: For Rel-18 eRedCap devices that are compliant with the 5 MHz data channel option, the BWP concept still remains vital. A working eRedCap device would still require a 20 MHz receiver to read the initial and control channel BWPs, but the process of configuring its BWP for data transmission and reception could be reduced to only 5 MHz which means that the network resources would be in line with the standard of the UE's simplified baseband processing.

5.2. Initial Access and Network Identification

At the very moment of the connection, the network should already classify a UE as a RedCap device in order to assign the proper configurations and policies. If a regular NR device connects to a cell that it cannot manage, then its access will be denied, but a RedCap UE will get a different treatment. Different ways for such early identification have been proposed in Release 17.

- **System Information and Cell Barring**: Initially, a cell will announce its capability to support RedCap devices. SIB1 indicates this through signals. With SIB1, the network can also set up access restrictions for certain devices. For example, a mobile operator might decide to limit access for 1Rx RedCap devices in an area with poor downlink coverage or deny access for HD-FDD devices in an area experiencing heavy traffic to preserve spectral efficiency. A RedCap UE receives the notification and does not even try to connect to a forbidden cell.
- **Random Access Channel (RACH) Procedure**: The primary method used for early identification is the 4-step Random Access Channel (RACH) procedure run via the 4 steps.
  - *Msg1 (PRACH Preamble):* One option for the network is to assign RedCap UEs a different set of PRACH resources (time-frequency opportunities) to use. If a UE sends Msg1 with one of these preambles designated for it, the gNodeB immediately concludes it is a RedCap device. This is the point where identification can happen the earliest.

 doi:10.20944/preprints202512.2156.v1

- *Msg3 (RRC Setup Request):* If there are no separate PRACH resources allocated, then the ultimate user identification occurs at Msg3. A RedCap UE communicates using an LCID (Logical Channel ID) of 35 or 36 in the MAC header of its Msg3 transmission, which is reserved for it. The gNodeB, upon decoding this LCID, recognizes the UE as a RedCap unit and is able to customize the following steps of the connection setup (for example, Msg4 and the RRC Reconfiguration message) to meet the device's requirements.

- **UE Capability Information**: The UE after initial access sends its full capabilities to the network in an RRC UE Capability Information message [30]. This message contains a flag indicating the UE is a RedCap one (supportOfRedCap-r17) and also shows the support features like 2Rx antennas, HD-FDD, or relaxed RRM measurements which are all optional. For eRedCap, a new RAT type is signaled that enables even more granular policy application. The network relies on this information to equip the UE with the best set of parameters for its entire connection duration.

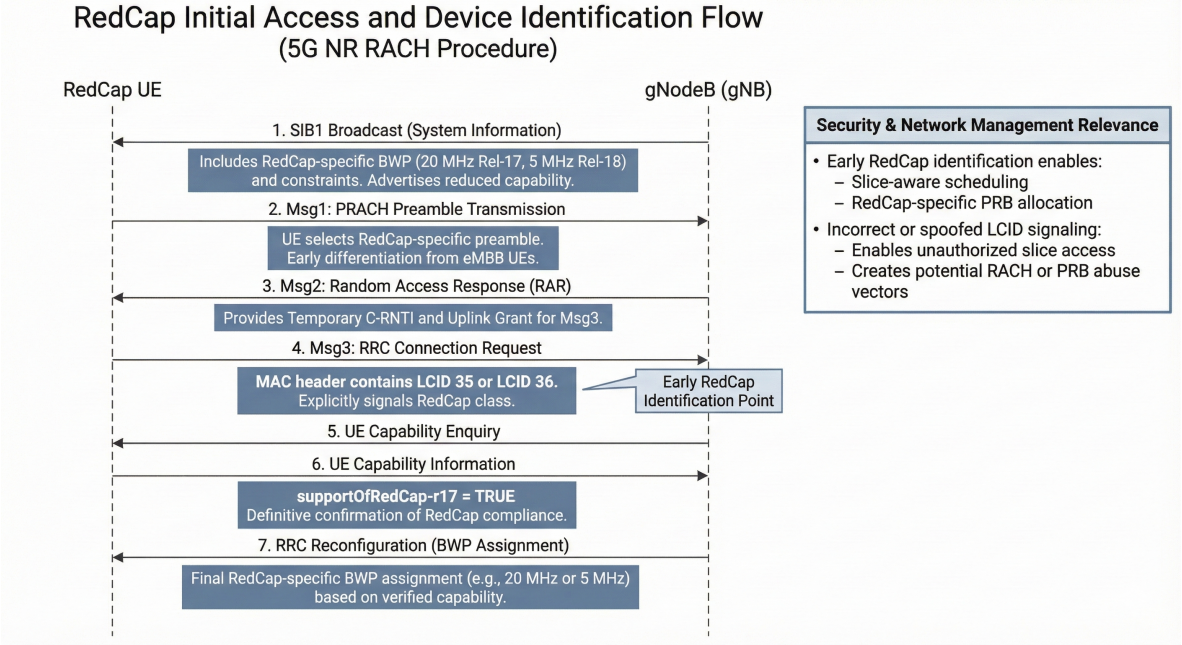

Figure 2. Sequence diagram illustrating the RedCap initial access and identification process during the 5G NR random access procedure. RedCap devices are identified through a combination of broadcast configuration, PRACH preamble selection, MAC-layer LCID signaling, and final capability verification using the supportOfRedCap-r17 flag.

5.3. Impact on RAN Architecture and Resource Management

The massive deployment of RedCap devices has a lot of consequences on the handling of RAN resources and performance of the whole network.

- **Spectral Efficiency Considerations**: One of the major concerns regarding RedCap's application in the area of mobile communications. RedCap devices in general, and especially the 1T1R versions are mainly less efficient in terms of the spectrum than the baseline NR devices with multi-antennas. They need more time-frequency resources (Physical Resource Blocks, or PRBs) for transmitting or receiving the same data. In case the cell has a large number of RedCap UEs with high traffic, the median throughput of all users including eMBB will be reduced. However, system-level simulations indicate that with moderate traffic and a reasonable mix of devices, eMBB performance will be barely affected [31,32]. This means that operators have to be very careful not to create capacity issues in cells that are already heavily loaded due to the presence of RedCap. Thus, capability-specific cell barring became one of the major reasons for the Our deployment strategy so far [33].

 doi:10.20944/preprints202512.2156.v1

- **Scheduling and Resource Allocation**: The gNodeB scheduler needs to know about RedCap and be able to make decisions [34,35]. It has to consider the specific characteristics of RedCap UEs such as:
  - *Narrowband Operation:* The scheduler must limit resource allocations for a RedCap UE to its active BWP.
  - *HD-FDD Constraints:* For UEs operating in HD-FDD mode, the scheduler must make sure that uplink and downlink allocations are not scheduled at the same time, thus controlling conflicts, and prioritizing transmissions based on the rules set beforehand.
- **Relaxed Processing Times**: For eRedCap UEs, the scheduler must take into account a longer processing timeline, hence modifying the timing between a grant (DCI) and the corresponding data transmission (PDSCH/PUSCH).
- **Coexistence with Other Services**: 5G NR was aimed at being a flexible and future-compatible air interface all through its design, which is a primary reason for RedCap's coming into the picture. The network can impeccably schedule RedCap UEs along with eMBB and URLLC traffic using the same time-frequency resources. The flexible slot-based framework and scalable numerology of 5G allow the network to interlace transmissions for different service types. For instance, low-latency URLLC data can take over the ongoing eMBB or RedCap transmissions to meet its very strict deadlines. This built-in flexibility enables service providers to offer RedCap over their existing 5G SA infrastructure with just a software upgrade, thus making the most of the spectrum and paving the way for a gradual integration.

To sum up, the architecture of 5G is strong and flexible enough to support RedCap. Moreover, it is through BWP, dedicated initial access procedures, and intelligent RAN resource management that these lower-complexity devices are accommodated efficiently by the network thereby opening up the mid-tier IoT market without considerably deteriorating high-end 5G services' performance.

6. Use Cases and Applications

The deployment of 5G RedCap is not just a gradual technical progression. Rather, it is a powerful tool that opens up a whole range of IoT applications that were hitherto stuck in the low-rate, high-latency world of LPWA and the high-cost, high-power domain of eMBB. RedCap's combination of high performance and low cost gives it the potential to drive digital transformation in various industry sectors. This section will discuss the important use cases and applications of RedCap, which will be grouped according to their main domains: IIoT, wearables, video surveillance, and smart cities.

6.1. Industrial IoT (IIoT) and Factory Automation

The industrial market is the most valuable one for the RedCap technology as it will be able to facilitate many applications ranging from monitoring and control to automation in the factories, warehouses, and processing plants.

- **Industrial Wireless Sensors**: One of the main application areas in IIoT is the installation of large sensor networks for monitoring machines and the environment. The industrial sensors for pressure, temperature, humidity, vibration, and motion need connectivity that is more reliable and with lower latency (like <100ms) than NB-IoT, but not at the expense of multi-gigabit speeds. That is why RedCap is such a perfect match since it is granting the needed latency and reliability in a 5G SA private network, which keeps the data on-premise. Moreover, the technology's advanced power-saving options (eDRX, RRM relaxation) come in very handy when the sensors are battery-powered and need to last for years without receiving any maintenance.
- **Actuators and Low-End Robotics**: URLLC is a must for high-precision motion control, however, many industrial automation functions entail less critical control loops. The latency and reliability of RedCap are the main factors for controlling actuators, valves, and simpler robots (cobots) where instant reaction is not extremely important but steady performance is the main requirement.

 doi:10.20944/preprints202512.2156.v1

- **Asset Tracking and Logistics**: In the case of the large industrial facilities and yards, the tracking of the location and status of tools, equipment, and automated guided vehicles (AGVs) is a major prerequisite for operational efficiency. RedCap allows the required level of movement and even higher data rates than those of LTE-M for sending more detailed telemetry data. The advent of RedCap in Rel-18 and beyond to incorporate improved and sidelink-based positioning will make its application in these areas even more appropriate.
- **IoT Gateways**: In several deployments, traditional sensors and machines are linked through wired protocols (e.g., Modbus, PROFIBUS). An IoT gateway that is RedCap-enabled can collect data from these sensors in a cluster and send it wirelessly over the 5G network, representing a cost-efficient method for providing connectivity to the "brownfield" equipment that already exists.

6.2. Wearables and Healthcare

The consumer wearables market, which consists of smartwatches, fitness trackers, and new AR/VR glasses, is one of the main aims for RedCap. This kind of devices requires a small-size, a long-lasting battery, and a data transfer rate that is beyond LTE-M limit.

- **Smartwatches and Health Monitors**: The contemporary smartwatches persist in requiring non-stop connectivity for their features such as notifications, streaming audio, and health data (like heart rate, ECG, blood oxygen levels) transmitting. RedCap with data rates as high as 150 Mbps will easily handle these and moreover, its power efficiency will help in getting multi-day battery life. The 1T1R antenna setup, coupled with the HD-FDD mode, is what allows wearable devices to be so small. In addition, VoNR (Voice over NR) support provides the capability of making great quality voice calls straight from the gadget.
- **Low-End AR/VR Glasses**: On one hand, high-end and fully immersive AR/VR applications indeed need the huge capacity of eMBB, on the other hand, there are already new kinds of "assisted" or "lightweight" AR glasses that can be used for showing notifications and simple information overlays. Such devices can work on RedCap really well as it allows them to have low latency which results in smooth user experience without the accompanying cost and power consumption of eMBB. Sidelink RedCap, a future development, could possibly make it possible for these glasses to communicate directly with a smartphone or hub thus relieving the processing and network connectivity demands placed on them.
- **Remote Patient Monitoring**: The medical field will be one of the areas where RedCap will be used to the fullest as it will be able to connect wearable medical sensors for the remote monitoring of patients that suffer from chronic diseases. These gadgets are supposed to send vital signs and other physiological data in near real-time, which is exactly what RedCap's low latency and high reliability are good for.

6.3. Video Surveillance

Security and monitoring through real-time video feeds that have to be transmitted, are often application needs of smart cities, industrial sites, and retail environments.

- **Smart City and Public Safety**: Advanced surveillance cameras at public areas require strong wireless connections for the transmission of video streams to the central monitoring station. A regular HD video stream needs a continuous uplink throughput of 2-25 Mbps depending upon the resolution and compression [36]. This data rate is easily handled by RedCap but Zoom technologies sometimes can't cope with it. RedCap provides a cost-effective solution as compared to either wired connections or complete 5G eMBB modem setups for such applications.
- **Body Cameras**: Police and private security body cameras have the same advantages of RedCap as well. Its throughput efficiency, power consumption, and compactness make it perfect for these mobile, battery-operated devices.

 doi:10.20944/preprints202512.2156.v1

- **Industrial and Retail Monitoring**: The camera-related activities in factories and stores include process monitoring, quality control, security, etc. RedCap allows the required uplink bandwidth that can enable the use of multiple camera feeds in a single private 5G network, thus providing high-quality and real-time visibility of the operations.

6.4. Smart Grids and Smart Cities

Apart from monitoring, RedCap is a fundamental technology for all modern applications in smart cities and utilities that need performance and scalability to coexist.

- **Smart Grid Automation**: Contemporary electric networks demand instant supervision and management to handle loads, connect renewable energy sources, and eliminate faults. The combination of low latency and high dependability of RedCap makes it feasible to interconnect sensors, switches, and reclosers on the distribution grid, thus outperforming LPWA technologies and still being cheaper than URLLC.
- **Environmental Monitoring**: Sensor installations over a city to monitor air quality, water levels, and weather conditions will necessitate a connectivity solution that can scale and is very efficient in power consumption [37]. eRedCap, specifically, is the best choice for these applications, which usually carry non-moving, battery-operated devices sending data at intervals.
- **Fixed Wireless Access (FWA) CPE**: RedCap can be employed in lower-cost Customer Premises Equipment (CPE) for the purpose of delivering broadband to homes and businesses in developing markets or rural areas at a more affordable rate than previously. Though it does not reach the gigabit speeds of eMBB FWA, RedCap still performs fairly well in fulfilling the needs of basic internet access, video streaming, and online services at a far more affordable price point.

Table 3. Application Domains and Key RedCap Features.

Application Domain	Specific Use Case	Key Enabling RedCap Features and Rationale
Industrial IoT (IIoT)	Industrial Wireless Sensors	**eDRX & RRM Relaxation:** For multi-year battery life. **Low Latency (<100ms):** For process monitoring. **5G SA Support:** For secure private networks.
	Asset Tracking / AGVs	**Mobility Support:** Handover for moving assets. **Enhanced Positioning (Rel-18+):** For accurate location tracking.
Wearables & Healthcare	Smartwatches / Health Monitors	**1T1R/HD-FDD:** Enables compact, cost-effective form. **Power Efficiency:** For multi-day battery life. **Mid-Tier Data Rate (>5 Mbps):** Supports health data and audio.
	Low-End AR Glasses	**Low Latency:** Ensures smooth user experience. **Sidelink (Future):** For efficient connectivity.
Video Surveillance	Fixed Security Cameras	**High Uplink Throughput (2-25 Mbps):** Sufficient for HD video. **Lower Cost vs. eMBB:** More economical solution.
	Body Cameras	**Power Efficiency & Compact Size:** Essential for wearable devices. **Mobility Support:** Ensures continuous connectivity.
Smart Cities & Utilities	Smart Grid Monitors	**Low Latency & High Reliability:** For real-time grid control. **Scalability:** To support a large number of devices.
	FWA CPE	**Rel-17 Data Rate (≈150 Mbps):** "Good enough" broadband performance. **Lower Device Cost:** Makes FWA accessible to more users.

7. Performance Analysis and Evaluation

The theoretical specifications of 5G RedCap foresee a performance profile that is balanced among complexity and cost. Nevertheless, a quantitative analysis that is composed of simulations and

 doi:10.20944/preprints202512.2156.v1

empirical tests is required to get the real-world capabilities of 5G RedCap. This part combines performance statistics from sector white papers, academic work, and technical surveys in order to measure RedCap in terms of key performance indicators (KPI's) that are throughput, latency, power consumption, and coverage. We offer a comparative analysis in which we set RedCap against the baseline 5G NR and other cellular IoT technologies such as LTE-M and LTE Cat-4 to clearly indicate its performance under different scenarios.

7.1. Throughput Performance

The maximum theoretical data rate for Rel-17 RedCap is frequently mentioned, in terms of LTE Cat-4, as about 150 Mbps for the downlink (DL) and 50 Mbps for the uplink (UL), which is about the same figure for the case of Rel-18 eRedCap with a target of 10 Mbps. However, the actual throughput will depend on many factors such as the channel bandwidth, the number of MIMO layers, the modulation and coding scheme (MCS), and the signal-to-noise ratio (SNR). The empirical measurements have confirmed these performance projections. In a live commercial network, a study by Yang et al. tested Rel-17 RedCap devices with 2Rx antennas and 256QAM support.

- The measured peak downlink rate was 226 Mbps in a 20 MHz FDD band (2.1 GHz), which is a significant increase over the baseline target and even surpasses a 150 Mbps LTE Cat-4 device. The uplink peak rate was 90 Mbps, which is also above LTE Cat-4's 50 Mbps.
- In a 100 MHz TDD band (3.5 GHz), where the RedCap user equipment (UE) was restricted to a 20 MHz bandwidth part (BWP), the measured downlink peak rate was around 140 Mbps. This shows that RedCap can reach its target throughput even when it is functioning as a narrowband device within a wideband carrier.

SNR and throughput have a strong relationship, and it is an important factor to consider when judging the performance in non-ideal, cell-center conditions. This relationship is depicted in the empirical Hardware-in-the-Loop measurements reported by Jörke et al[12]. In the case of AWGN (Additive White Gaussian Noise) channel conditions, a 1-layer (1Rx) RedCap device can deliver more than 80 Mbps at a very high SNR (>25 dB). However, introducing realistic multipath fading (3GPP TDL-A model) results in the maximum achievable throughput being reduced to around 80 Mbps, plus a 4 dB increase in SNR to reach the same data rate is required, which stresses that real-world channel conditions can greatly influence the performance. The plot also indicates that a 2-layer (2Rx) RedCap device almost doubles the throughput for the entire SNR range and reaches more than 150 Mbps in very good conditions. This clearly emphasizes the great performance boost that comes with the additional 2Rx option.

7.2. Latency Performance

One of the major benefits of 5G NR technology is low latency, which is, in fact, passed on to RedCap as a quality. A theoretical analysis based on 3GPP slot structures and processing timeliness indicates that the air interface latency for NR (and consequently RedCap) is much less than for LTE. LTE had longer intervals for scheduling and HARQ feedback (K0, K1, K2) than NR has now. A study conducted by Yang et al [10] involved the measurement of the end-to-end user-plane latency (ping time) in circumstances of a commercial 5G SA network. Table 4 summarizes the findings that RedCap gets a latency almost the same as the baseline NR user equipment with an average of 13-15 ms for both small and large packet sizes, which is done really well. It is, in fact, a lot better compared to the latency measured for LTE Cat-4, which is estimated to be from 30 ms to 50 ms, in most cases and is a better performance. Thus, the RedCap technology becomes eligible for the use in the case of latency-sensitive applications, like industrial control and remote monitoring, which usually demand latencies below 100 ms.

 doi:10.20944/preprints202512.2156.v1

7.3. Power Consumption and Battery Life

Power efficiency is the main KPI that matters the most for RedCap's target scenarios. The reduction in power consumption is the result of a combination of simplification (narrow bandwidth, fewer RF chains) and improvement in software features (eDRX, RRM relaxation) which RedCap takes advantage of. Measurement of power in real-life gives clear proof of the reductions in power usage [38]. Jörke et al [12] performed in-depth power measurements for RedCap and baseline NR across various functional states:

- **Data Transfer (Uplink):** The power consumption of the RedCap module was 38–62% lower than that of the NR module, which is the main reason why it was operating at lower power levels (good coverage condition voltage levels). This is because of the RedCap's RF front-end efficiency and the baseband circuits that were optimized for 20 MHz operation.
- **Data Transfer (Downlink):** During the period of actively receiving data, the RedCap module's power consumption was calculated at 366.3 mW, while the NR module's was at 1104.0 mW—approximately 67% less.
- **Inactive/Sleep State (eDRX):** The longest state that one could consider battery-powered devices with long lives as a significant obstacle would be this one. The RedCap module's average power consumption in eDRX (RRC_INACTIVE state) was measured at 21.9 mW, compared to 34.8 mW for the NR module in its standard DRX mode, representing a 37% improvement. Although it is a significant improvement, this baseline sleep current is still much higher than that of NB-IoT devices (in the microwatt range), which is why RedCap is not expected to achieve a 10+ year battery life but is well-suited for applications requiring weeks, months, or a few years of continuous operation.

The power savings achieved are directly reflected in longer battery life. A smart signage application (5 MB data transfer every 15 minutes) case study computed that under good signal conditions, a RedCap device could achieve more than two months of battery life from a 10,000 mAh battery, which is a 57% improvement compared to a baseline NR device operating under the same conditions. In an uplink video surveillance application, the RedCap battery life was 1.5–2$\times$ that of the NR device.

7.4. Coverage Performance

A possible drawback to RedCap is that the limitations on its functionality are especially reflected by the fact that it works with only one or two receive antennas, unlike the four that are commonly used in most NR baseline devices; thus, it might not provide good coverage. The link budget is negatively impacted by the absence of receive diversity gain which is usually higher. The results of the field trials conducted in the "pull-far" test, where the UEs are moved from the cell center to the edge and the connection drops, show that the coverage area of RedCap is very much the same as that of a conventional NR UE. Practically, the coverage area for the 2.1 GHz (FDD) and 3.5 GHz (TDD) bands was identical for RedCap UEs as well as NR UEs. At the drop-out location, the signal strength measured (SS-RSRP) did show some difference, with the RedCap UE being 2-3 dBm lower (weaker) than the NR UE. The small difference in performance was explained by the smaller dimension of the RedCap test device, which probably led to a less efficient antenna design rather than a technological limitation. Moreover, 5G NR incorporates extensively powerful coverage enhancement features such as PUSCH repetitions that can be easily activated to offset any link budget drawbacks while still providing connectivity at the cell edge.

The performance statistics prove that 5G RedCap has successfully occupied the mid-tier segment that was reserved for it. It brings about a considerable increase in throughput as well as a decrease in latency when compared to LPWA technologies, while at the same time it offers significant and clear reductions in power consumption and complexity over baseline 5G NR.

 doi:10.20944/preprints202512.2156.v1

Table 4. Quantitative KPI Comparison(RedCap, NR, LTE).

	5G RedCap (Rel-17)	5G NR (Baseline)	LTE Cat-4 / LTE-M
Peak DL	150–226 Mbps	>1 Gbps	150 / 1 Mbps
Peak UL	90–121 Mbps	>285 Mbps	50 / 1 Mbps
Latency	13–15 ms	12–14 ms	30–100 ms
eDRX Power	≈22 mW	≈35 mW	<1 mW
Coverage	≈140 dB	Baseline	≈144/156 dB

8. Security Vulnerabilities and Attack Vectors in RedCap Networks

5G RedCap was introduced to not only allow the oxygenation of a gigantic new ecosystem of medium-tier Internet of things(IoT) devices but also to come up with comparatively new security aspects. There are several unique factors associated with RedCap that constitute its risk profile, which are its target applications, device limitations, and identification methods, though at a protocol level RedCap is not necessarily less secure in any way. Hereby, An analysis of security weaknesses and attack methods related to RedCap networks is made taking into account the existing 5G framework, application-specific vulnerabilities and the 3GPP standards governing the mitigation methods [39,40].

8.1. Foundational Protocol-Level Attack Vectors

The vulnerabilities that arise from RedCap's core technical design, as detailed in Section 3, independent of the final application. These vectors are a direct trade-off of the design choices made to reduce cost and complexity.

- **Identity Spoofing via Initial Access:** RedCap UEs are identified early, either via reserved PRACH preambles (Msg1) or specific MAC CE Logical Channel IDs (LCIDs) in Msg3 .This creates a vulnerability where a malicious (non-RedCap) device could spoof these identifiers. Such an attack could be used to gain unauthorized access to network slices or resources reserved for IoT traffic, or to launch a denial-of-service attack by flooding the RedCap-specific RACH resources .
- **Resource Exhaustion (Denial of Service):** The lower spectral efficiency of 1Rx RedCap devices (as noted in Section 5) is a protocol-level characteristic. An attacker could launch a large-scale attack using many compromised (or spoofed) 1Rx UEs to request data simultaneously. This would force the RAN to allocate a disproportionate amount of time-frequency resources to serve these inefficient devices, effectively "starving" legitimate eMBB users in the same cell and causing a degradation of service [41].
- **HD-FDD Timing and Conflict Attacks:** The HD-FDD feature (Section 3) mandates that a UE cannot transmit and receive simultaneously, and it defines deterministic rules for resolving collisions (e.g., "UE will skip RX" or "UE will skip TX"). A sophisticated attacker, such as a false base station, could exploit this. The attacker might force the UE to "skip RX," thereby missing crucial network commands or pages through a malice-causing DoS, by sending a fake uplink grant perfectly timed to coincide with a real downlink paging message.
- **Power-Saving (eDRX/RRM) Exploitation:** The power-saving features, though advantageous, are susceptible to abuse. An attacker who could provoke a device to go into its 2.9-hour eDRX cycle too soon would surreptitiously disconnect the device for a long time [42]. Furthermore, an attacker could spoof signals to trick a UE into believing it meets the "stationary" or "not-at-cell-edge" criteria for RRM relaxation. The UE would stop doing measurements of the adjacent cells, eventually experiencing a Radio Link Failure (RLF) due to the diminution of the signal from the serving cell.

8.2. Inherited 5G Security Framework

A foundational principle of RedCap is its integration into the 5G Standalone (SA) architecture. A key finding from industry analysis is that "RedCap UEs will still support the same high-level security procedures as other 5G UEs". Thus, RedCap devices are secure as they share the same

 doi:10.20944/preprints202512.2156.v1

security measures of the 5G System (5GS) with the 5G Core and RedCap devices, amongst others. **5G Core (5GC) Security:** RedCap devices which are connected to the 5GC obtain the benefits from its service-based architecture (SBA) which encompasses features for secure service authorization and communication between network functions.

- *User Plane Integrity Protection:* 3GPP Release 17, concurrent with RedCap, fortified 5G security with enhanced features. This includes User Plane Integrity Protection, which helps base stations and devices verify that received data has not been tampered with by malicious actors.
- *Unified Access Control (UAC):* The 5G system includes UAC mechanisms that can be used to manage network access and congestion. At the same time, this mechanism is intended to "make the distinction between RedCap and non-RedCap UEs" which means providing a tool to control the access and to avoid network congestion.
- From the standpoint of security, the legacy attacks may not affect the RedCap devices since they are protected by the native 5G security framework. Nonetheless, it is the use cases and constraints imposed on the devices that make RedCap less vulnerable than others with a strong protocol.

8.3. Application-Layer and Privacy Vulnerabilities

The most significant new security and privacy challenges arise from the specific applications RedCap is designed to enable, particularly wearables and human-machine interfaces (HMI).

- **Sensitive Data Collection:** Devices that are supported by RedCap such as smartwatches, health monitors, and AR/VR glasses are aimed at the collection of enormous amounts of personal and sensitive data. The data of such secretive nature consists of biometric data (voice, gestures, facial expressions), real-time location, and minute details of the human body's functions (heart rate, body temp).
- **Privacy Risks:** The process of collecting such personal data from various sources makes it a super attractive target for hackers. One of the big worries is that the privacy protecting techniques are up to the mark, especially when low-end devices are involved. Accidental or intentional access or leaking of such data will be an extensive violation of privacy.
- **Industrial Espionage:** In a factory environment where RedCap sensors detect "process automation" or "plant asset monitoring" the sensors can be wiretapped for corporate espionage. An attacker who has managed to reach the real-time production data, sensor readings, or video surveillance feeds could not only leak the trade secrets but also create disruptions in operations.

8.4. Mass-Scale and Data-Centric Attack Vectors

The Attack vectors are a consequence of RedCap's application and scale, rather than its protocol design.

- **Massive-Scale IoT Attacks:** RedCap is intended for mass adoption, enabling billions of new connections. This massive scale makes the RedCap device ecosystem an attractive target for botnets. A widespread vulnerability in a low-cost, mass-market RedCap module could allow attackers to compromise millions of devices (e.g., sensors, cameras) and use them to launch large-scale Distributed Denial of Service (DDoS) attacks.
- **Resource-Constrained Devices:** The goal of reducing device cost and complexity may lead to resource-constrained devices with limited processing power and memory. This can be a vulnerability if it "hinder[s] the implementation of robust, computationally intensive security algorithms". Attackers may target these devices with exploits that would be mitigated by more powerful hardware.
- **False Base Station Attacks:** Like all cellular devices, RedCap UEs are susceptible to false base stations (also known as "IMSI Catchers"). 3GPP recognized this, and the Release 17 work included a comprehensive study to "mitigate security and privacy issues arising from these fraudulent stations".

 doi:10.20944/preprints202512.2156.v1

8.5. 3GPP Mitigations for RedCap Use Cases

Critically, 3GPP developed RedCap in Release 17 concurrently with a suite of security enhancements designed to address the risks of an expanded 5G ecosystem. There are several protections, which are indirectly related to the use cases that RedCap devices are targeted for, that are inherited by RedCap devices:

- **Security for IIoT:** Release 17 of TSN (Time-Sensitive Networking), which is a core technology in the industrial automation sector, was given stronger support. Time-sensitive communication and "robust time synchronization" were part of the 5G system strengthening along with "secure interfaces, authentication and authorization" for TSC mechanisms.
- **Security for Proximity Services (Sidelink):** When RedCap grows to cater to sidelink for the likes of AR glasses and V2X, the Rel-17 security protocols that were to "protect mobile devices discovery and their communications" would be its main source of advantage.
- **Security for Non-Public Networks (NPN):** RedCap is among the top contenders for deployment in private 5G networks. Release 17 enhanced the security of Standalone Non-Public Networks (SNPNs), enabling "UE access using external credentials," which is vital for industrial and enterprise deployments.

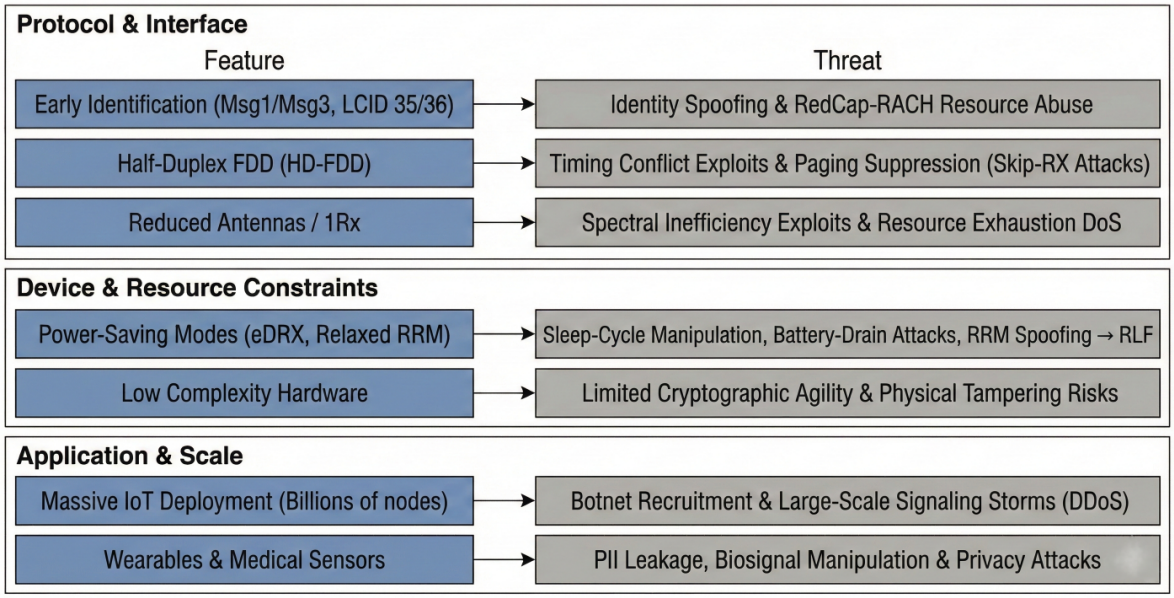

Figure 3. Taxonomy of Security Vulnerabilities in 5G RedCap.

9. Challenges and Future Research Directions

The widespread adoption, significant promise and rapid ecosystem development of 5G RedCap, is not totally without difficulties. The hurdles include the prerequisites for network deployment, the complex security considerations, and the management of resources. It is very important to deal with these difficulties if one wants to get the maximum benefit from RedCap and it also opens up a lot of opportunities for future research. This section gives a critical analysis of the main barriers to RedCap deployment and suggests specific and actionable research directions that the academic as well as industrial communities.

9.1. Real-World Implementation Challenges

- **Roaming and Network Fragmentation:** In contrast to LTE, which provides comprehensive international roaming, 5G Standalone (SA) roaming is not fully developed. Due to the fact that RedCap devices need 5G SA to operate, global logistics and asset management applications encounter major disconnections. The first implementations have to bear the cost of using LTE Cat-

 doi:10.20944/preprints202512.2156.v1

4 fallback to guarantee uninterrupted service, which somewhat diminishes the cost advantages of RedCap.

- **Module Cost vs. Legacy LTE:** The main obstacle to the implementation is the still unresolved issue of the paradox regarding cost and value. The RedCap modules are intended to have a lower price compared to eMBB, yet their present cost is nearly $50 which is still much higher than that of LTE Cat-4 which is around $20 for the matured modules. The device makers do not want to switch to RedCap until the costs are brought down to the same level as LTE through the larger scale of production which results in a "chicken-and-egg" delay for the adoption.
- **Spectral Efficiency Concerns:** Operators voiced worries that the presence of RedCap devices in large numbers (sp ecifically 1Rx types) might eventually lead to a reduction in cell capacity. The reason for this is that 1Rx devices cannot take advantage of receive diversity therefore they will need considerable amount of power from the base station in order to reach the same throughput and in such situations, the very expensive eMBB users might suffer from inadequate resources because of the congestion in the cell.
- **Managing New Security Attack Surfaces:** Comprehensively elaborated in Section 8, RedCap presents a distinctive security profile. The main difficulty is not a less secure protocol but rather a new variety of attack vectors coming from its particular design and use. The problems consist of:
  - **Protocol-level vulnerabilities**, among the possible cases were also the identity spoofing due to early RACH/LCID identifiers and DoS attacks that made use of HD-FDD timing conflicts or eDRX power-saving techniques.
  - **Mass-scale risks**, The situation is characterized by a vast, uniform population composed of cheap, resource-limited devices that together form an appealing target for both botnets and massive-scale DDoS attacks.
  - **Application-layer privacy risks**, particularly from wearable devices as well as health monitoring systems that capture highly confidential biometric and physiological information.

9.2. Future Evolution and Research Directions

The progress of RedCap in the direction of 3GPP Release 17 & 18 demands the resolution of these barriers to deployment and the improvement of security through accompanying research activities.

- **Lightweight and PHY-Layer Security:** There is a possibility that classical cryptographic protocols such as complex PKI might not be suitable for the lowest-tier eRedCap sensors or Ambient IoT devices due to their high computational requirements. Consequently, it is necessary to conduct research into:
  - **Lightweight Cryptography:** Development and standardization of encryption schemes specialized for the limited processing power and battery constraints of the eRedCap and Ambient IoT is essential.
  - **Physical Layer (PHY) Security:** Researching methods that use channel properties (e.g. channel state information fingerprints) for device authentication and detection of spoofing attacks in the initial access phase (Msg1/Msg3) thus reducing the possibility of identity spoofing before the security of higher layers is set up [43].
- **AI/ML-Driven Resource and Security Management:** The Massive scale of any RedCap implementation creates an administrative challenge that defies operational management.
  - **Intelligent Scheduling:** The creation of AI-based schedulers that can predict the traffic patterns of RedCap fleets, will result in switching BWP and scheduling of HD-FDD in a way that prevents the network from suffering the spectral efficiency penalty to the fullest extent.
  - **Anomaly Detection:** Development of scalable, network-based Machine Learning systems for the purpose of recognizing signaling anomalies that are characteristic of DDoS attacks or "signaling storms" caused by compromised RedCap botnets, in particular, focusing on RACH loads and control plane traffic [44,45].

 doi:10.20944/preprints202512.2156.v1

- **Advanced Power Saving for "Zero-Maintenance" IoT:** To compete with the 10-year battery life of NB-IoT, eRedCap requires going further with innovation beyond simple eDRX.
  - **Wake-Up Radios (WUR):** The work on the use of extremely low power-wake-up radios that will give the main RedCap modem the ability to be in deep sleep until a particular wake-up signal comes, and this would possibly bring down the idle power consumption to a few microwatt levels.
  - **Energy Harvesting Integration:** The research on cross-layer protocol modifications that enable RedCap devices to change their transmission cycles according to the real-time energy harvesting conditions (like solar, and vibration) for achieving energy-neutral operation.
- **Non-Terrestrial Network (NTN) Integration:** The expansion of RedCap support to the satellite networks (NTN-RedCap) is a necessary step for having a global coverage.Research will address the challenges of high Doppler shifts, long propagation delays, and link budget constraints inherent in satellite communication for devices with reduced antenna capabilities.
- **Validating Industrial Reliability at Scale:** Based on the industrial pilots of 5G-ACIA, future research should provide empirical evidence for RedCap's simplified redundancy techniques (e.g., no dual connectivity) to be able to bear the 99.99% reliability that is needed for industrial safety wearables and sensor clusters in various factory settings.

10. Bibliographic Analysis

A survey of this kind relies heavily on the collective of knowledge of both the industry leaders and the academic research community. In order to get a proper view of the research and development activities on 5G RedCap, this section goes ahead with bibliographic analysis of the source materials that were used in this paper. The analysis studies the types of publications and their distribution, the time trends in research output, and the main topics that have developed as technology has grown from standardization to deployment.

10.1. Publication Trends

- **Early Foundations (Pre-2021):** The publications of the years preceding 2021 is less on topics related to RedCap/5G-NR lite, and it mainly deals with topics of general 5G security, basic IoT concepts, and early LTE-M/NB-IoT technologies.
- **Standardization Phase (2021–2023):** During this time, there is an evident increase in the number of documents, mainly due to the 3GPP technical specifications and reports that characterize 3GPP Release 17 RedCap. Furthermore, the early industry white papers from significant contributors like Qualcomm and Ericsson emerge at this stage, and they are vital as they point to the future potential of the technology.
- **Explosion of Applied Research (2024–2025):** The data's shows an increase in the number of publications in 2024 and 2025. This time is marked by the performance evaluations that are empirical, security analyses, and industry-specific application studies. This trend shows that RedCap has moved from a perspective of theoretical standard to a deployable technology undergoing continuous real-world testing and optimization.

10.2. Source Distribution

- **Industry White Papers and Reports:** A significant amount of the fundamental technical understanding derives from white papers issued by the leading infrastructure suppliers (Ericsson, Nokia),chipmakers (Qualcomm),and the test & measurement industry (Rohde & Schwarz, Anritsu).These writings deliver the groundwork for understanding ways of implementation, device complexity reduction and market positioning.
- **Standardization Documents:** The assessment is predominantly based on the technical specifications (TS) and technical reports (TR) of the 3rd Generation Partnership Project (3GPP). The

 doi:10.20944/preprints202512.2156.v1

mentioned documents, indeed, create the trustworthy support of the study, setting the limits for the radio access potentials and the architecture necessities.

- **Academic Conferences and Journals:** The last few years have an increase in the number of peer-reviewed papers accepted at IEEE and ACM venues (IEEE Access, GLOBECOM, Sensors). The mentioned sources pinpoint particular problems like energy-saving approaches, security threats and their prevention, and throughput improvement on the uplink,RedCap.

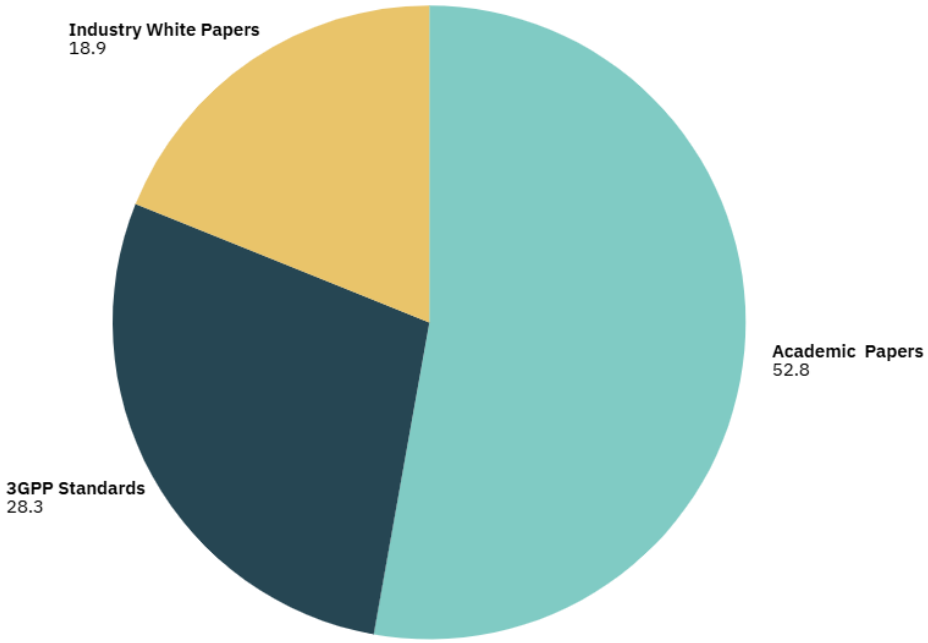

Figure 4. Distribution of Publication Sources.

10.3. Thematic Analysis

- **Performance Validation:** The terms "Performance Analysis," "Throughput," "Power Consumption," and "Energy Efficiency" are among the most common in the literature. This is an indication of the main concern in research nowadays which is to prove if RedCap devices really deliver the promised performance and battery life in real networks.
- **Security and Privacy:** A major cluster of research focuses on "Security," "Privacy," "Attack Vectors," and "Authentication". This highlights the industry's concern with securing billions of low-cost IoT devices against threats like Denial of Service and privacy leakage.
- **Industrial IoT (IIoT):** There is a strong thematic link between RedCap and industrial applications, evidenced by terms like "Industrial IoT," "Automation," "Smart Cities," and "Wearables".
- **Evolution of eRedCap:** The words "Release 18," "Evolution," and "eRedCap" signify a research agenda that looks ahead and prioritizes the reduction of costs and support for even lower-tier IoT use cases.

11. Conclusions

The evolution of the 5G New Radio (NR) standard has historically bifurcated into high-performance (eMBB/URLLC) and low-complexity (mMTC) domains. This survey has demonstrated that 5G Reduced Capability (RedCap), introduced in 3GPP Release 17 and refined in Release 18, serves as the critical architectural bridge between these extremes. By strictly defining a mid-tier device category, RedCap enables the migration of legacy LTE Industrial IoT (IIoT) and consumer wearable applications onto a unified 5G Standalone (SA) infrastructure.

Our technical analysis confirms that the reduction of device complexity—specifically through the limitation of bandwidth to 20 MHz (FR1), the optionality of Half-Duplex FDD (HD-FDD) operation, and the reduction of receive antennas (1Rx)—successfully lowers the barrier to entry for 5G-native IoT.

 doi:10.20944/preprints202512.2156.v1

Quantitative assessments support the assertion that various architectural trade-offs made in designing the RedCap system permit the system to operate at data rates similar to those of LTE Cat-4, while at the same time, through the use of Extended Discontinuous Reception (eDRX) and Radio Resource Management (RRM) relaxations, accomplish superior latency and power efficiency.

Meanwhile, one of the major contributions of this review is the recognition of the different security posture these limitations have resulted in. RedCap, although benefiting from the solid security structure of the 5G Core (5GC), is believed to open up new attack vectors by its implementation. Simplifications at the protocol level such as early indication during the Random Access Channel (RACH) procedure make devices vulnerable to impersonation and user counting before authentication is complete. Moreover, low-cost hardware constraints of sensors inbuilt limit the incorporation of cryptographic agility that is computationally intensive thus exposing them to physical tampering and side-channel attacks. The assessment reveals that the vast scale of RedCap rollouts results in an enlarged attack surface where hacked devices can be deployed for Distributed Denial of Service (DDoS) attacks without alerting the conventional network alarms. The deployment of challenges continues, especially in terms of reliance on 5G SA coverage everywhere and controlling the dropout of spectral efficiency owing to the use of single-antenna devices in crowded cells.

To deal with these problems, a collective research effort on light security methods is to be made. Moreover, the future research needs to develop unbreakable security methods, and AI-based malware detection systems that can recognize harmful traffic patterns at the access point of the network so the security of the 5G IoT ecosystem does not get weakened. Nonetheless, power and cost efficiencies that characterize RedCap should not be compromised. 5G RedCap is a revolutionary but complex technology. The success of this technology is going to be a mix of two factors: first, the development of the device ecosystem and, second, the hard application of security-by-design principles to protect the industrial and personal data transmitted through it, which are the most vulnerable ones.

Author Contributions: Conceptualization and problem formulation, P.K. and K.J.; methodology and system design, P.K., K.J. and S.S.N.; implementation and software development, P.R.I., S.S.N., and H.N.N.; experimentation and data analysis, P.R.I., S.S.N., and H.N.N.; validation and result interpretation, P.R.I., S.S.N., and H.N.N.; writing—original draft preparation, P.R.I. and K.J.; writing—review and editing, P.K, K.J., and S.S.N; visualization and figures, P.R.I; supervision and project guidance, P.K., H.N.N. and S.S.N.; funding acquisition and resource management, P.K. and K.J. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G NR	5th Generation New Radio
RedCap	Reduced Capability
eMBB	Enhanced Mobile Broadband
URLLC	Ultra-Reliable Low-Latency Communications
mMTC	Massive Machine-Type Communications
3GPP	3rd Generation Partnership Project
LPWA	Low-Power Wide-Area
IoT	Internet of Things

References

1. Gohil, A.; Modi, H.; Patel, S.K. 5G Technology of Mobile Communication: A Survey. In Proceedings of the 2013 International Conference on Intelligent Systems and Signal Processing (ISSP). IEEE, 2013, pp. 288–292.
2. Deepender.; Verma, J.K.; Manoj.; Shrivastava, U. A Study on 5G Technology and Its Applications in Telecommunications. In Proceedings of the 2021 International Conference on Computational Performance Evaluation (ComPE). IEEE, 2021, pp. 365–371. https://doi.org/10.1109/ComPE53109.2021.9752402.

 doi:10.20944/preprints202512.2156.v1

3. Parvez, I.; Rahmati, A.; Guvenc, I.; Sarwat, A.I.; Dai, H. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. *IEEE Communications Surveys & Tutorials* **2018**, *20*, 3098–3130. https://doi.org/10.1109/COMST.2018.2841349.
4. 3GPP. TS 22.104: Service requirements for cyber-physical control applications in vertical domains. Technical Specification 22.104, 3rd Generation Partnership Project, 2024. V19.2.0.
5. GSMA 5G IoT Community. RedCap/eRedCap for IoT. White paper, GSMA, 2025.
6. 3GPP. TR 22.832: Study on communication services for critical medical applications. Technical Report 22.832, 3rd Generation Partnership Project, 2019. V17.0.0.
7. Jamil, H.M.M.; Islam, M.; Das, R.K.; Pranto, S.A.; Amin, L.A. Enabling Human-Machine Interfaces with 5G RedCap: Architecture, Key Requirements, and Challenges. In Proceedings of the 2024 IEEE Conference on Engineering Informatics (ICEI). IEEE, 2024. https://doi.org/10.1109/ICE164305.2024.10912368.
8. 3GPP. RP-202933: Justification for NR-Light. RAN Plenary Document RP-202933, 3rd Generation Partnership Project, 2020.
9. FengQin.; WangHeChun.; Hao, C. 5G REDCAP DEVICE AND ITS LOW-COST HIGH EFFICIENCY ATE TEST SOLUTION. In Proceedings of the 2025 Conference of Science and Technology of Integrated Circuits (CSTIC). IEEE, 2025. https://doi.org/10.1109/CSTIC64481.2025.11017961.
10. Yang, M.; Zhang, N.; Li, X.; Chen, P. Research on RedCap UE's performance indicators in real network to support iot applications. In Proceedings of the 2024 the 9th International Conference on Cloud Computing and Internet of Things (CCIOT). ACM, 2024, pp. 1–10. https://doi.org/10.1145/3704304.3704305.
11. Song, P.; Xiong, S.; Wang, Q. RedCap Performance Analysis and Deployment Strategy Research. In Proceedings of the 2024 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). IEEE, 2024. https://doi.org/10.1109/BMSB62888.2024.10608332.
12. Jörke, P.; Schippers, H.; Wietfeld, C. Empirical Comparison of Power Consumption and Data Rates for 5G New Radio and RedCap Devices. In Proceedings of the 2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC). IEEE, 2025. https://doi.org/10.1109/CCNC54725.2025.10976177.
13. 3GPP. TR 38.848: Study on Ambient IoT (Internet of Things) in RAN. Technical Report 38.848, 3rd Generation Partnership Project, 2023. V18.0.0.
14. 3GPP. TS 36.300: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. Technical Specification 36.300, 3rd Generation Partnership Project, 2022. V17.2.0.
15. Anritsu. RedCap/eRedCap: The IoT Technology for 5G Networks. White Paper RedCap-E-R-1-(2.00), Anritsu, 2025.
16. Quectel. 5G RedCap white paper: Is 5G RedCap the right fit for your IoT connectivity needs? White paper, Quectel, 2024.
17. Hill, K. 5G-enabled IoT: Will RedCap help deliver on the promise of digital transformation? RCR Wireless News, 2023. Editorial Report.
18. 3GPP. TS 38.214: NR; Physical layer procedures for data (Release 17). Technical Specification 38.214, 3rd Generation Partnership Project, 2022. V17.3.0.
19. Li, X.; Xu, X.; Hu, C. Research on 5G RedCap Standard and Key Technologies. In Proceedings of the 2023 4th Information Communication Technologies Conference (ICTC), 2023, pp. 6–9. https://doi.org/10.1109/ICTC57116.2023.10154644.
20. Guo, J.; Li, N.; Zhu, J.; She, X.; Chen, P. Study on Key Characteristics and Standardization Evolution for NR RedCap UE. In Proceedings of the 2022 IEEE the 8th International Conference on Computer and Communications (ICCC), 2022, pp. 268–273. https://doi.org/10.1109/ICCC56324.2022.10065715.
21. Sudhamani, C.; Roslee, M.; Tiang, J.J.; Rehman, A.U. A Survey on 5G Coverage Improvement Techniques: Issues and Future Challenges. *Sensors* **2023**, *23*, 2356. https://doi.org/10.3390/s23042356.
22. Srivastava, M.; Ray, V.K. A Survey on User Equipment Power Saving for 5G Communication Systems. In Proceedings of the 2024 1st International Conference on Sustainability and Technological Advancements in Engineering Domain (SUSTAINED). IEEE, 2024, pp. 329–334. https://doi.org/10.1109/SUSTAINED63638.2024.11074181.
23. 3GPP. TS 38.331: NR; Radio Resource Control (RRC) protocol specification (Release 17). Technical Specification 38.331, 3rd Generation Partnership Project, 2022. V17.2.0.
24. Tayyab, M.; Kolehmainen, N.; Butt, M.M.; Khlass, A.; Ratasuk, R. Energy Efficient RRM Relaxation for Reduced Capability UEs in 5G Networks. In Proceedings of the 2022 IEEE Global Communications Conference (GLOBECOM), 2022, pp. 99–104. https://doi.org/10.1109/GLOBECOM48099.2022.10000873.

 doi:10.20944/preprints202512.2156.v1

25. Tayyab, M.; Sofonias, H.; Jarvela, R.; Kolehmanen, N.; Gursu, H.M. RRM Relaxation in Connected State for Reduced Capability (RedCap) NR UEs. In Proceedings of the 2021 17th International Symposium on Wireless Communication Systems (ISWCS), 2021, pp. 1–6. https://doi.org/10.1109/ISWCS49558.2021.9562143.
26. 3GPP. RP-213661: Study on further NR RedCap UE complexity reduction (Release 18). RAN Plenary Document RP-213661, 3rd Generation Partnership Project, 2021.
27. 3GPP. TR 22.837: Feasibility Study on Integrated Sensing and Communication (Release 19). Technical Report 22.837, 3rd Generation Partnership Project, 2023. V19.0.0.
28. 3GPP. TS 23.501: System architecture for the 5G System (5GS); Stage 2. Technical Specification 23.501, 3rd Generation Partnership Project, 2023. V17.8.0.
29. Oracle. Preparing your core network for 5G RedCap. White paper, Oracle, 2024.
30. 3GPP. TS 38.306: NR; User Equipment (UE) radio access capabilities (Release 17). Technical Specification 38.306, 3rd Generation Partnership Project, 2022. V17.5.0.
31. Saafi, S.; Vikhrova, O.; Andreev, S.; Hosek, J. Enhancing Uplink Performance of NR RedCap in Industrial 5G/B5G Systems. In Proceedings of the 2022 IEEE International Conference on Communications Workshops (ICC Workshops), 2022, pp. 520–525. https://doi.org/10.1109/ICCWORKSHOPS53468.2022.9814497.
32. Ferdous, N.S.; Hassan, M.Z.; Ahmed, I.; Akter, L. Resource Management for Reduced Capability New Radio Devices in Beyond 5G Networks: Opportunities and Research Road Map. In Proceedings of the 2024 7th Conference on Cloud and Internet of Things (CIoT), 2024. https://doi.org/10.1109/CIoT63799.2024.10757145.
33. Tikhvinskiy, V.; Pastukh, A.; Dymkova, S.; Varlamov, O. Compatibility Analysis Between RedCap Non-Public Networks and 5G NR in TDD FR1 and FR2 Bands. *Inventions* **2025**, *10*, 12. https://doi.org/10.3390/inventions10010012.
34. 3GPP. TR 37.817: Study on enhancements for RAN analytics. Technical Report 37.817, 3rd Generation Partnership Project, 2021. V17.0.0.
35. 3GPP. TR 38.843: Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR air interface. Technical Report 38.843, 3rd Generation Partnership Project, 2023. V18.0.0.
36. Zhang, R.; Zhang, Y.; Wang, N.; Zhao, Q.; Hu, W. Design and Application Exploration of Scenario Video Surveillance Based on RedCap Module. In Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR 2024), Chengdu, China, June 2024; pp. 539–545. https://doi.org/10.1145/3718751.3718837.
37. Aldehim, G.; khan, S.; Shahzad, T.; Khan, M.A.; Ghadi, Y.Y.; Jiang, W.; Mazhar, T.; Hamam, H. Balancing sustainability and security: a review of 5G and IoT in smart cities. *Digital Communications and Networks* **2025**. Journal Pre-proof, https://doi.org/10.1016/j.dean.2025.06.007.
38. Beschastnyi, V.; Ostrikova, D.; Moltchanov, D.; Gaidamaka, Y.; Koucheryavy, Y.; Samouylov, K. Comparison of energy conservation strategies for 5G NR RedCap service in industrial environment. *Computer Networks* **2024**, *254*, 110792. https://doi.org/10.1016/j.comnet.2024.110792.
39. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 170–195. https://doi.org/10.1109/COMST.2019.2951818.
40. Ahmed, S.F.; Alam, M.S.B.; Afrin, S.; Rafa, S.J.; Taher, S.B.; Kabir, M.; Muyeen, S.M.; Gandomi, A.H. Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities. *IEEE Access* **2024**, *12*, 13125–13145. https://doi.org/10.1109/ACCESS.2024.3352508.
41. Dias, J.; Pinto, P.; Santos, R.; Malta, S. 5G Network Slicing: Security Challenges, Attack Vectors, and Mitigation Approaches. *Sensors* **2025**, *25*, 3940. https://doi.org/10.3390/s25133940.
42. Dino, A.; Giuliano, F.; Mangione, S.; Garlisi, D.; Tinnirello, I. Silent Drain: From Energy Profiling to Practical Denial-of-Energy Attacks in 5G. In Proceedings of the ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WINTECH '25), Hong Kong, China, November 2025; pp. 113–120. https://doi.org/10.1145/3737895.3768308.
43. Sharma, H.; Kumar, N.; Tekchandani, R. Physical layer security using beamforming techniques for 5G and beyond networks: A systematic review. *Physical Communication* **2022**, *54*, 101791. https://doi.org/10.1016/j.phycom.2022.101791.

 doi:10.20944/preprints202512.2156.v1

44. Fakhouri, H.N.; Alawadi, S.; Awaysheh, F.M.; Hani, I.B.; Alkhalaileh, M.; Hamad, F. A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. *Electronics* **2023**, *12*, 4604. https://doi.org/10.3390/electronics12224604.
45. Antal, B.; Kail, E.; Orsós, M.; Bánáti, A. Simulation and detection methods of specific 5G attacks. In Proceedings of the 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), 2025, pp. 183–188. https://doi.org/10.1109/SAMI63904.2025.10883251.