Comeback Kid: Resilience for Mixed-Critical Wireless Network Resource Management

Robert-Jeron Reifert, *Graduate Student Member, IEEE*, Stefan Roth, *Graduate Student Member, IEEE*, Alaa Alameer Ahmad, and Aydin Sezgin, *Senior Member, IEEE*

***Abstract*—The future sixth generation (6G) of communication systems is envisioned to provide numerous applications in safety-critical contexts, e.g., driverless traffic, modular industry, and smart cities, which require outstanding performance, high reliability and fault tolerance, as well as autonomy. Ensuring criticality awareness for diverse functional safety applications and providing fault tolerance in an autonomous manner are essential for future 6G systems. Therefore, this paper proposes jointly employing the concepts of resilience and mixed criticality. In this work, we conduct physical layer resource management in cloud-based networks under the rate-splitting paradigm, which is a promising factor towards achieving high resilience. We recapitulate the concepts individually, outline a joint metric to measure the criticality-aware resilience, and verify its merits in a case study. We, thereby, formulate a non-convex optimization problem, derive an efficient iterative algorithm, propose four resilience mechanisms differing in quality and time of adaption, and conduct extensive numerical simulations. Towards this end, we propose a highly autonomous rate-splitting-enabled physical layer resource management algorithm for future 6G networks respecting mixed-critical quality of service (QoS) levels and providing high levels of resilience. Results emphasize the considerable improvements of incorporating a mixed criticality-aware resilience strategy under channel outages and strict QoS demands. The rate-splitting paradigm is particularly shown to overcome state-of-the-art interference management techniques, and the resilience and throughput adaption over consecutive outage events reveals the proposed schemes contribution towards enabling future 6G networks.**

***Index Terms*—Resilience, fault tolerance, mixed criticality, rate-splitting multiple access, resource management, quality of service.**

I. Introduction

A. Motivation

The road towards the sixth generation (6G) of wireless communication networks is already being pursued by researchers around the globe [3], [4]. Through a wide range of applications, the empowerment of anytime anywhere access, and an overwhelming amount of connected devices, 6G brings enormous challenges towards the development of future network technologies. Particularly, use cases such as wireless-based cloud office for small and home office, smart cities, and smart factory, depend on high-performance and reliable networks [5].

It is forecasted that the number of internet of things (IoT) connections increases from 14.6 billion in 2021 to 30.2 billion in 2027 [5]. Hence, there is a huge number of devices with different levels of criticality, such as safety-critcal, mission-critical, and low-critical IoT devices, which also coexist within one system [6]. In industrial context, mixed criticality corresponds to different priorities of applications, e.g., a security monitoring system is more critical than a maintenance scheduler. To ensure fulfilling the quality of service (QoS) demands, we investigate QoS target capabilities of the considered network. On the physical layer, QoS is often translated to the allocated rates of network participants [7], [8]. Thereby, the QoS assigned to the nodes is designed to match the desired data rates (target rates), which depend on the subscribed contract (service provider networks) or criticality level (industrial context). In terms of resource management, criticality allows prioritizing different (more critical) network participants or applications. That is, critical devices might be assigned greater portions of the overall available resources, up to a point, where low-critical communication links may be halted completely to assure service for the critical ones.

The continuously increasing IoT connectivity brings along another hurdle in the design of future 6G networks, namely resilience. Resilience is the capacity of a system to absorb a disturbance and reorganize while undergoing change so as to still retain its essential function. In other words, resilience captures a system's ability to maintain functionality facing errors, adapt to erroneous influences, and recover the functionality in a timely manner. As this should be achieved in an automated fashion without the need for human interaction [9, Principle P16], autonomy is a central principle at the design stage. Resilience is a topic of interest throughout various areas of industry and academia (psychology [10], industrial-ecological systems [11], communications [12], security [13]). Generally, the overall concept of resilience includes different system characteristics, i.e., *detection*, *remediation*, and *recovery* [9]. By that, resilience as a concept allows for detecting errors in malfunctioning communication systems, remediating the effects on the network functionality, e.g., data rate or delay

Part of this paper was presented at the IEEE International Conference on Communications Workshops, May 2022 [1]. An extended version of this paper is available on arxiv [2].

This work was supported in part by the German Federal Ministry of Education and Research (BMBF) in the course of the 6GEM Research Hub under grant 16KISK037, in part by the BMBF (Förderkennzeichen ReMiX) under Grant 01IS18063A, and in part by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

Robert-Jeron Reifert, Stefan Roth, and Aydin Sezgin are with Digital Communication Systems, Ruhr University Bochum, Bochum, Germany. (Email: {robert-.reifert,stefan.roth-k21,aydin.sezgin}@rub.de).

Alaa Alameer Ahmad was with Digital Communication Systems, Ruhr University Bochum, Bochum, Germany during the work on this paper, and is now with Cariad SE, Wolfsburg, Germany. (Email: alaa.alameer85@gmail.com).

performance, and recovering to a normal functioning state. Thereby, resilience clearly broadens the applicability of wireless communication towards many use cases, and enhances performance metrics in the face of unforseeable influences.

Especially in the context of high critical IoT nodes, the concept of resilience is of significant importance. Providing a robust communication system is equally vital that timely recovery from failures to an acceptable service level, in order to deploy such systems for real-time safety-critical applications. In this context, *rate-splitting* comes into play as an efficient and robust communication scheme [14], [15]. Originating in the early 80's [16], and shown to achieve within one-bit of the interference channel capacity [17], rate-splitting mutliple access (RSMA) achieved significant attention in research, e.g., [18]–[24]. Conventionally, each user is assigned to a single message stream (*private message*), however, under RSMA, an additional *common message* is utilized for two reasons: (1) Taking over parts of the data transmission from the private message, and (2) interference mitigation by common message decoding at other users to reduce the interference level when decoding their own private messages. Especially due to the enhanced opportunities for communication (multiple message streams, *redundancy*) and different purposes of streams (private and common, *diversity*), we identify RSMA as a promising resilience enhancing paradigm.

In this work, we aim at tackling the fundamental challenge of integrating mixed criticality levels in the physical layer of a wireless communication system. Thereby designing a resilient RSMA-enabled network architecture ensuring high robustness, automated adaption, and fast recovery, especially when the network resources are constrained. An example of such architecture can be seen in Fig. 1, where we distinguish between mixed criticality information, the ISO/OSI lower layers, and a resilience controller at the cloud connected to the RSMA-enabled radio access network. Mixed criticality information serves as input to the ISO/OSI model, while the resilience controller manages the network's operation via control signals. A resilient resource management promises to enhance future networks' performance in an automated manner without inducing major losses in terms of service quality. To the best of the authors knowledge, this is the first work which considers resilience and mixed criticality for the physical layer of wireless communication systems under the RSMA paradigm. We aim to provide the general concepts, design recommendations, and a case study to evaluate the proposed methodology.

B. Related Literature

The considered methodology of combining resilience and mixed criticality for physical layer resource management in this paper is related to works residing in the domains of resilience (especially network resilience), robustness, reliability, and mixed criticality of communication systems. Additionally, there are recent related works considering the RSMA paradigm.

[1]The criticality index may for instance refer to safety integrity levels (SILs) as a real-world mixed criticality application (IEC 61508) [25], see section II-B.

The term resilience has its roots in the Latin verb *resiliere*, meaning to rebound or recoil [26]. Nowadays, resilience relates to many engineering fields [11], [27], environmental and regional studies [28], psychology [10], as well as economics [29]. While definitions and methodologies may differ among the research directions, a common overlap is that resilience refers to some kind of disruption and the return to the normal situation [30]. A great amount of work towards (network) resilience in communication systems was done by the ResiliNets initiative [31]. Especially, the seminal paper [9] point out axioms, strategies, and principles of resilience in communication networks, with a focus on the internet. The recent book [32] describes techniques for disaster-resilient communication networks and includes many works of international researchers. Work [33] elaborates on communications in industrial IoT describing potential network architectures, with a focus on security. In [34], the authors investigate the reliability of the IP multimedia subsystem and define the interplay between *availability* and *reliability* and their relation to resilience. Work [35] describes a framework to evaluate network dependability and performability in the face of challenges such as attacks and disasters. The authors point out that redundancy and diversity increase the reliability but also increase the costs. Since many related works on resilience in the communication domain regard networking problems, the work [9] notes a major challenge as *failures at a lower layer*, e.g., a fibre cut causes a link-layer failure, which has to be remediated by re-routing at a higher layer. However, with the utilization of wireless communications under cloud-based architectures, it is necessary to include resilience at the lower layers to assist the overall network resilience capabilities.

In this work, we adapt the concept of resilience for the physical layer of wireless communication systems, a field in which only limited considerations of resilience exist. 6G communication is the enabling infrastructure for many critical applications and therefore resilience becomes a very important topic in these scenarios. Some related chapters in [32] reside in this domain: (a) In [36], QoS in modular positioning systems, wireless sensor networks, and free-space optical (FSO) communication systems is reviewed under weather disruptions. (b) In [37], the availability of FSO systems under atmospheric impacts is studied. (c) In [38], resilience enhancing techniques for 5G systems are studied, namely frequency fallback, segment interleaving, and multi-operator protection. Further works on resilience for wireless communications include [39], with radio and FSO backhauling for network resilience, [40], emphasizing the need for intelligent fault management and mitigation strategies at design and run-time, and [41], where an experimental PC-USRP hardware platform evaluates the performance in the face of pulse interference for in industrial environments. Most of these works consider resilient systems, but do not consider holistic metrics for resilience.

The concepts of robustness and reliability, being one aspect of resilience, correspond, in part, to the concept of ultra-reliable low-latency communication [42], [43].

The concept of mixed criticality has been introduced in 2007 for task scheduling in real-time systems [44]. Since then, mixed criticality has been adapted for a wider range

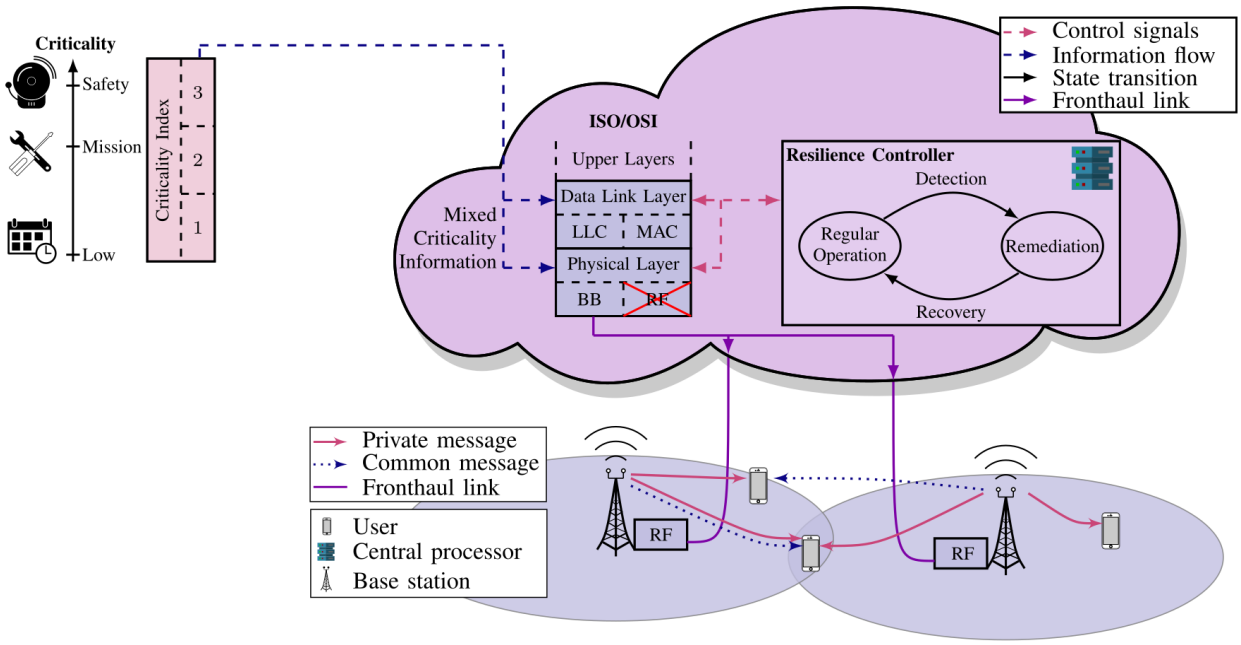


Figure 1: The considered cloud-based network architecture including mixed criticality, resilience, and RSMA elements.[1]

of applications in the field of communications [6], [45]–[48]. In general, mixed criticality refers to communication links having different priority levels, typically because failures have different consequences. Usually, the links are categorized as safety-, mission-, and low-critical links. AirTight, a protocol for time-critical cyber physical systems (CPS) including real-time and mixed criticality requirements, has been proposed in [45] and [46]. Thereby, a criticality-aware fault model is utilized to capture external interference, in which mixed criticality is implemented as different amounts of maximum deadline misses of traffic links. The goal of reliable real-time performance for data delivery in industrial wireless sensor networks was approached in [6]. Thereby, a criticality-aware wireless fieldbus protocol was proposed for different data flows with different importance levels, i.e., delay and reliability constraints. In the same context, work [47] states that high critical real-time flows must be guaranteed reliability in the face of errors. Further, [48] aims at providing response time guarantees within wireless communication networks, which consist of mixed-critical services, by using network slicing and priority-aware resource block allocation. However, most related works lack considerations of the lower layers on the protocol stack, especially the physical layer of wireless communication networks.

Smart interference management schemes, such as RSMA, inherently posses some resilience characteristics, i.e., robustness, as they cope well with high interference scenarios, and can guarantee a certain connectivity. We give a brief overview of related works on robustness of RSMA and QoS-aware RSMA schemes. A general overview of RSMA is provided in [20], revisiting fundamental concepts and future trends, see also references therein. Scalability and robustness, especially robustness against channel state information (CSI) imperfections, of an RSMA-enabled network is analyzed in [14]. Work [15] considers the robust design problem for achieving max-min fairness among all users and shows the superior performance of the proposed RSMA scheme under CSI uncertainty. Mixed criticality and RSMA are combined in [49] with the aim of identifying queue stability regions. QoS constrainted power minimization is conducted in [7], [15]. Therein, the authors investigate the minimization of a weighted-sum of transmit powers subject to per-user QoS constraints. Hence, such scheme is only feasible in networks, where the QoS is achievable. However, this assumption is rather optimistic and we herein propose a more generalized scheme, which provides feasible solutions for networks with insufficient resources.

While the related literature includes several general research directions, to fill some of the gaps, we build up onto these ideas and extend the contribution towards considering mixed criticality on the physical layer and the combination of resilience and mixed criticality for wireless communication resource management, especially using RSMA.

C. Contributions

In this paper, we design a general framework for wireless communication systems that accounts for the merits of mixed criticality in the physical layer, and also provides aspects of resilience, i.e., high reliability, automated adaption to failures, and rapid recovery. As such, we recap the individual concepts of resilience and mixed criticality and define their manifestations for the physical layer resource management. Thereby, we strike a connection of QoS and criticality level, and define mathematical formulations of resilience metrics for wireless communications. Combining those two concepts, we employ the unified framework in a case study, involving RSMA-enabled cloud-radio access networks (C-RAN). Thus, this work is one step forward to design criticality-aware, highly-automated 6G communication systems for various industrial and service applications. The contributions of the work are summarized as

- Establishing the concepts of resilience and mixed criticality for cloud-assisted wireless networks to enable the vision of 6G
- Designing a unified framework to consider resilience and mixed criticality jointly in the physical layer communication resource management
- Presenting a case study on RSMA-enabled cloud networks, in which the following resilience mechanisms are employed: (1) A *rate adaption* mechanism adjusts the QoS to a value feasible with the selected parameters, (2) a *beamformer adaption* mechanism is optimizing the beamformers according to the new situation, (3) a *BS-user-allocation adaption* mechanism optimizes the allocation of BSs to users and (4) a *comprehensive adaption* mechanism re-visits the original formulations and adjusts all parameters jointly.

D. Notation and Organization

The paper notation is as follows: Vectors $\boldsymbol{a}$ (matrices $\boldsymbol{A}$) are denoted as bold lower-case (upper-case) letters, respectively. Sets $\mathcal{A}$ are denoted in calligraphic and have cardinality $|\mathcal{A}|$. $\mathbb{C}$ denotes the complex field, $\mathbf{0}_N$ an all-zero vector of dimension $N \times 1$, $|\cdot|$ the absolute value, $\|\cdot\|_p$ the L_p-norm, and $(\cdot)^H$ the Hermitian transpose operator. At last, $\mathrm{Re}\{\cdot\}$ is the real part of a complex number.

The rest of this paper is organized as follows: Section II introduces resilience, mixed criticality, and a joint metric combining those concepts. Then, in section III we conduct a case study on RSMA-enabled C-RAN as follows: III-A system model introduction; III-B problem formulation and solution; III-C resilient and criticality-aware resource allocation algorithm. Corresponding numerical simulations are provided in section IV. At last, section V concludes this paper.

II. Resilience and Mixed Criticality Concept

In this section, we introduce the concepts of resilience and mixed criticality and consequently combine these considerations into a joint metric based on the allocated and desired data rate.

A. Resilience

Resilience describes the ability of a network or system to provide and maintain an acceptable service level while facing errors or unexpected events that impact the workflow of the service [9]. Hence, resilience is the ability to recover from erroneous conditions or faulty situations [30]. In this context, we clearly differentiate between resilience and robustness, whereas resilience is the more general concept which includes robustness along with other aspects, e.g., survivability, dependability, and many more [9]. Therefore, a fault, error, and failure chain is established by the authors of [9] in the network resilience context. Thereby, a fault is a system flaw that can be present on purpose (constraints) or accidentally (software bug, hardware flaw) and cause an observable error. An error is defined as a deviation between the observed and the desired state. A failure is the deviation of service functionality from a desired/required functionality, resulting from an error. In this work, a wireless communication resource management system is considered, which is faulty by nature due to the unreliability of wireless channels and strict constraints, e.g., transmit power. Hence, errors may manifest as channels outages or hardware failures at the transmitter and/or receiver, which then correspond to service failures, such as outages or deviations of the provided and requested QoS, e.g., data rate drops.

In general, redundancy and diversity are typical enablers of fault tolerance and survivability, respectively. Herein, we aim to design a resource management mechanism that is resilient such that major service failures do not occur. Additionally, we consider the performance in terms of QoS fulfillment (QoS metrics are delay, throughput, etc. [9]). As faults are inevitable, the herein developed resource management should also be able to mitigate the effects of service failures.

The work [9] proposes four vital strategies for the design and assessment of resilient systems: $1)$ *Defending* against threads to normal operation, which can be done actively and passively, e.g., via redundancy and diversity; $2)$ *detection* of erroneous conditions, e.g., via cyclic redundancy checks; $3)$ *remediation* of the erroneous effects, e.g., via automatic adaption of resource allocation; $4)$ *recovery* to normal operations. Especially, strategies $2) - 4)$ are shown in Fig. 1 in the resilience controller, which detects errors and performs resource allocation on the lower layers. Strategy $1)$ *defending*, is implicitly considered to be part of the initial resource management solution, i.e., we propose passive defense against errors (redundancy and diversity).

Further, to measure the resilience of a system, the work [30] proposes general resilience metrics. In this work, such metrics are tailored to the physical layer of wireless communication systems to make them applicable in this context. Especially, the considerations capture the resilience aspects of *anticipation*, *absorption*, *adaption*, and *recovery*. Here, *anticipation* is happening before an adverse event (prefailure), which corresponds to $1)$ *defending*. Note that *anticipation* is also not covered in the considered postfailure-related resilience metric. It is assumed to be done a priori by the network operator using established techniques, i.e., we assume the system to be in an optimized state initially until a failure occurs. For more details to prefailure aspects, we refer to works on reliability, e.g., [43] and references therein. Next, we characterize the remaining resilience aspects:

- *Absorption*: Measure of the ability to maintain functionality facing errors, i.e., how well a system absorbs a hazard's impact and restrains the severity, corresponding to $1)$ *defending*.
- *Adaption*: Measure of the loss of functionality after performance degradation until recovery, i.e., how well the system utilizes existing resources to mitigate the failure consequences, corresponding to $3)$ *remediation*.
- *Recovery*: Measure of the ability to recover to a stable state after experiencing degraded functionality, i.e., how fast the system can return to normal (or stable) operation, corresponding to $4)$ *recovery*.

Note that this work assumes ideal $2)$ detection, i.e., perfect and immediate knowledge of failure conditions.

A major complication of physical layer communication resource management comes from wireless channels, which are unreliable due to fading, blockage, the nature of electromagnetic radiation, etc. Such behavior can be tackled by introducing diversity techniques, i.e., time/frequency/spatial-diversity, sub-carrier coding, and multiple antennas, respectively [42]. While such techniques generally aim at providing reliability/robustness of the wireless communication, we note that resilience includes more aspects which need to be considered from an overall network perspective. Mostly, resilience is implemented as a redundancy mechanism by retransmitting the data. While retransmission is the only feasible solution to recover from an outage, i.e., packet loss, resilience mechanisms based solely on retransmission are not able to account for long-term outages due to blockage, hardware impairments, or transmitter outages. Transmit devices could face an infinite loop of retransmission on such link failures which deteriorates any spectral and energy efficiency. To recover from such outages, resilience is a key technique preventing long-term link losses, outage situations, and increasing the overall error/failure tolerance of the communication system. Many network-layer works consider the resilience by rerouting traffic, thereby avoiding the failed links. To depart from these works, we consider the resilience capabilities of lower layers for the resource management in wireless communication systems.

B. Mixed Criticality

The integration and coexistence of data links/flows, which generally have different criticality (importance) levels, into a common communication system is the major challenge of the mixed criticality concept tailored to the communications domain.[2] Generally, there is not only a huge number of safety-critical, mission-critical, and low-critical IoT devices, moreover, these criticality levels coexist within one system [6]. The concept is demonstrated in Fig. 1. A corresponding example are the safety integrity levels (SILs), which specify the target level of function safety, for more details see [25]. Conceptually, within the mixed critical network, critical links/devices are prioritized, i.e., they are assigned greater portions of the available resources. Low-critical links could be temporarily halted or be served with decreased QoS to ensure service of critical links.

Common principles for mixed criticality in terms of different tasks are given in [50]. Each data flow is defined by its period, deadline, computation time, and criticality level. In [47], this concept is extended to data flows, which are periodic end-to-end communications between source and destination. In this case, each flow is defined by its period, deadline, criticality level, number of hops, and routing path. These considerations are high-level characteristics, i.e., while the physical layer is utilized solely for data transmission, it does not account for mixed criticality. While such mixed criticality characteristics for higher layers provide a certain degree of resilience, a cross layer resilience strategy design is needed. It is essential for the performance to implement criticality levels also in the physical layer. Hence, departing from the conventional definition of mixed criticality for higher layers, in this work, we propose and design common definitions and concepts for mixed criticality in the physical layer. To provide methods for supporting such criticality considerations, the work [48] proposes assigning resource blocks to services, whereas critical services are scheduled with higher bandwidth than lower-critical services. In contrast, herein we define QoS requirements of data links to represent the criticality level. We herein assume that the criticality levels are provided by higher layer algorithms, thereby the QoS demands are given to the underlying layers, which need to account for them, e.g., see Fig. 1. Such criticality levels can be obtained by lookup tables by the service provider, within the frame structure of a data flow, referring to the type of service, or by the transmitting device itself.

Mixed criticality is usually implemented via weighting the utilities under optimization, e.g., weighted sum rate maximization. However, this does not necessarily satisfy the requirements and demands of mixed criticality, the weights need to be carefully chosen to incorporate a mixed criticality factor and be updated in an adaptive fashion. Other approaches present in literature are the considerations of specific constraints capturing such system demands, e.g., QoS constraints. Such constraints might render a lot of networks infeasible, especially in case the QoS demands are overall hardly achievable. In general, such weight-based or constraint-based approaches are not well suited to provide mixed criticality from a network perspective. In this work, utilizing the novel approach proposed in [1], we consider the mean squared error (MSE) of QoS deviation, i.e., the gap of allocated and desired rate (rate matching). Thereby, we are able to achieve a good-effort QoS fulfillment and avoid the infeasibility problems of QoS constraints. Hence, we optimize the resource allocation under a mixed critical network in order to fulfill QoS demands subject to various network constraints. This approach captures the possibility of having different criticality levels on the physical communication layer.

In the next subsection, we address the performance metric capturing the essentials of mixed criticality and resilience. Especially, we propose a time-dependent criticality-aware resilience metric including absorption, adaption, and recovery.

C. Joint Metric

As per [9], the considered QoS metrics can be delay, throughput, packet delivery ratio, etc. A common translation of QoS on the physical layer are the data rates of different network participants (throughput, parts of the delay), e.g., [7]. Thereby, the QoS assigned to a network participant is designed to match the desired data rates of the participant (target rates). The considered resilience metrics are postfailure-related formulations, we consider the system's *absorption*, *adaption*, and *recovery* in analogy to [30]. However, as opposed to [30], a failure in our work is assumed to occur instantly, which allows us to forgo integrals in the metric. As potential failures of the communication system are manyfold, in this work, we

[2]Mixed criticality research originates from a focus on real-time embedded systems with the aim of integrating components of different criticalities into a common hardware platform [50].

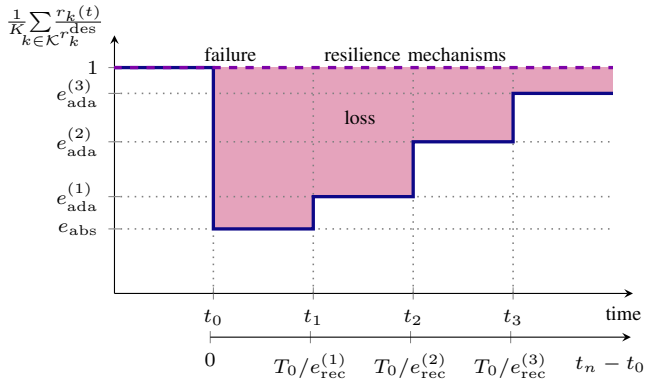


Figure 2: Fraction of the allocated and desired sum rate as a function of discrete time points showing the resilience metrics for $n = 3$ mechanisms.

quantify a failure to influence the achievable rates of the users. For instance, this could be the loss of connection between user and BSs, i.e., BS breakdowns, blockages, as well as hard- and software failures. Other failure models might include higher layer features, such as delay, or interference related failures, e.g., due to adversarial jamming. In the following, let $\mathcal{K} = \{1, \cdots, K\}$ be the set of K network participants, whereas the index k refers to the k-th network participant.

a) Absorption: For the *absorption*, we consider the time t_0 at which a service failure occurs. Given the time-dependent achievable allocated rate $r_k(t)$ and the constant desired rate r_k^{des}, the absorption is then defined as the sum of ratios of $r_k(t)$ and r_k^{des}:

$$e_{\text{abs}} = \frac{1}{K} \sum_{k \in \mathcal{K}} \frac{r_k(t_0)}{r_k^{\text{des}}}, \tag{1}$$

evaluated at the time of failure t_0. As illustrated in Fig. 2, *absorption* can already be observed as performance drop at the time of failure t_0. A normalization is calculated in equation (1), that is, assuming a system does not enhance its functionality ($r_k(t_0)$) above the demand level (r_k^{des}), the optimal value of e_{abs} is 1, while the lowest value tends to zero. Conceptually, the *absorption* can be considered as the performance drop at the time of failure t_0. A value of $e_{\text{abs}} = 1$ would mean the system's performance is unaffected by the failure. However, at t_0, a failure, e.g., a blockage, may render some (or all) participants' allocated rates $r_k(t_0)$ unachievable. Physically, for these rates we have $r_k(t) = 0$, as long as there is no remediation or adaption. The system functionality is now in a degraded steady state. As soon as at least one network participant experiences a lower-than-desired QoS, e_{abs} would drop below 1, resulting in a deviation from the optimum. In the worst case, the whole network is in outage and $e_{\text{abs}} = 0$.

b) Adaption: For the *adaption*, a resilience controller triggers mechanisms utilizing the existing resources to remediate the failure effects. This metric is then defined as ratio of the actual system functionality and the desired functionality at the time t_n, where the recovered state is reached, i.e., the time in which an automated remediation mechanism n has finished operating. For an adaption mechanism n, this can be formulated as

$$e_{\text{ada}}^{(n)} = \frac{1}{K} \sum_{k \in \mathcal{K}} \frac{r_k(t_n)}{r_k^{\text{des}}}. \tag{2}$$

Physically, $e_{\text{ada}}^{(n)}$ measures the participants' fraction of allocated data rates and desired rates at t_n. That is, how well the adaption mechanism provides the desired data rate. In other words, the *adaption* describes the improvement of functionality from the degraded steady state in relation to the desired functionality. If multiple remediation mechanisms are in place, we obtain different values for the adaption which represent the different remediation steps (see Fig. 2). Similar to the absorption, the optimal value of $e_{\text{ada}}^{(n)}$ is 1.

c) Recovery: At last, we consider the time-to-recovery, which is measured between the failure time t_0 and the time of recovery t_n and compared to a desired time-to-recovery T_0 as

$$e_{\text{rec}}^{(n)} = \begin{cases} 1 & t_n - t_0 \leq T_0 \\ \frac{T_0}{t_n - t_0} & \text{otherwise} \end{cases}, \tag{3}$$

where the optimal $e_{\text{rec}}^{(n)}$ is 1. This means that $e_{\text{rec}}^{(n)}$ measures the elapsed time between failure time and the application of the adaption mechanism, and relates it to a desired time. The operational meaning is that if the time between failure and remediation becomes larger, $e_{\text{rec}}^{(n)}$ decreases. For the time-to-recovery, Fig. 2 includes a second horizontal axis.

With these considerations at hand, we propose a criticality-aware resilience metric considering the aspects of absorption, adaption, and recovery. The utilized resilience metric is a linear combination of all components defined as

$$e^{(n)} = \lambda_1 e_{\text{abs}} + \lambda_2 e_{\text{ada}}^{(n)} + \lambda_3 e_{\text{rec}}^{(n)}, \tag{4}$$

where λ_a are non-negative weights that satisfy $\sum_{a=1}^{3} \lambda_a = 1$. The vector $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \lambda_3]$ contains the individual weights. Both the *absorption* (1) and the *adaption* (2) include the term $\frac{r_k(\cdot)}{r_k^{\text{des}}}$, which describes the gap of allocated and desired rate. In this context, the criticality-awareness of metric (4) originates from the consideration of r_k^{des}, which may take different values for different criticality levels. Note that the considered metric originates from use cases with single criticality levels and was developed for resilience scenarios [30]. The differentiation of target performance levels, which correspond to the criticality, is a novel aspect considered in our work. Thus, the proposed metric captures the possibility of measuring resilience for network participants with different QoS requirements. To summarize, the metric $e^{(n)}$ includes the resilience aspects *absorption*, *adaption*, and *recovery*, and the mixed criticality aspect r_k^{des}. Here, the desired rates may differ for different participants, which corresponds to mixed criticality, as critical participants have stricter QoS requirements.

With the above considerations at hand, a metric for measuring and quantifying the resilience of wireless communications networks is proposed. The challenge remains to, on the one hand, include robust mixed-critical resource management and, on the other hand, provide mechanisms for an autonomous controller. Such controller needs to enable smart adaption of resources in the face of system errors, e.g., outages, in order to recover the data rates. In other words, initially, the resources

should be allocated to fulfill the mixed-critical QoS demands whilst providing robustness, e.g., by overprovisioning certain resources, or multi-connectivity. In case of system errors, e.g., outage events, resources need to be adapted in order to best restore the performance, e.g., re-allocating some or all resources from the initial solution. The decision on the resource allocation mechanism depends on the desired trade-off between quality and complexity of the adaption.

In what follows, a verification and demonstration of the proposed resilience and mixed criticality framework is provided in terms of a case study. Especially, the case study is related to cloud-based wireless networks, with a focus on RSMA-enabled C-RANs.

III. Case Study: RSMA-enabled C-RAN

In this section, we investigate the proposed resilience and mixed criticality framework within a network, where various users are connected to multiple base stations (BSs), which are jointly controlled by a central processor (CP) at the cloud, as drawn in Figure 1. Such C-RAN is a promising network architecture, which enables centralization and virtualization providing high elasticity, high QoS, and good energy efficiency [51]. Therefore, it is a suitable candidate to demonstrate the usage of the proposed framework. To ensure fulfilling the QoS demands, we investigate QoS target capabilities. Thereby, the QoS assigned to a user is designed to match the desired data rate of the user (target rates). Hence, we aim at designing the C-RAN to enable mixed criticality regarding different communication links. For the communication between the the BSs and the users, we are employing the RSMA as a promising resilience-enhancing paradigm.

In this case study, we consider minimizing the MSE of QoS deviation, i.e., the gap of allocated and desired rate. Thereby, we utilize a mixed-critical C-RAN under the RSMA paradigm in order to fulfill all QoS demands. As such, we jointly optimize the beamforming vectors and allocated rates subject to per-BS fronthaul capacity, maximum transmit power, and per-user achievable rate constraints as an initial solution. While such optimization determines the optimal allocation of network resources under regular operation, this paper focuses on the behavior after failures in the network, e.g., outages. That is, firstly, resources are allocated using this optimization, then different outage scenarios are considered. Building upon such system, there are multiple recovery mechanisms, which possibly can be applied and distinguish in the quality of recovery and execution times. In this case study, we apply

- a *rate adaption* mechanism to allocate feasible QoS parameters within the failure condition,
- a *beamformer adaption* mechanism that updates the beamformers according to the new situation,
- a *BS-user-allocation adaption* mechanism which optimizes the allocation of BSs to users and
- a *comprehensive adaption* mechanism to optimize the QoS to a value feasible with the selected parameters.

Upon proposing resilience mechanisms for resource management, we present a resilient RSMA rate management algorithm jointly managing allocated rates, beamforming vectors, and BS-user clustering.

A. System Model

The network considered is a downlink C-RAN utilizing *data-sharing* transmission strategy. Under such architecture, a cloud coordinates B BSs via fronthaul links in order to serve K users, where the CP at the cloud performs most baseband processing tasks. More specifically, the CP encodes messages into signals and designs the joint beamforming vectors. These signals and coefficients are then forwarded to the BSs to perform modulation, precoding, and radio transmission. We denote $\mathcal{B}$ and $\mathcal{K}$ as the set of BSs and single-antenna users, respectively, where the number of BS antennas is L. Further network parameters are the fronthaul capacity $C_b^{\max}$, the maximum transmit power $P_b^{\max}$, and the transmission bandwidth τ. We assume the cloud to have access to the full CSI, which is reasoned in the assumption of a *block-based transmission model*. A transmission block is made of a couple of time slots in which the channel state remains constant, thus the CSI needs to be acquired at the beginning of each block. Without the loss of generality, the proposed algorithm optimizes the resource allocation and provides resilience within one such block.

Under the RSMA paradigm, messages requested by users are split into a private and common part. These messages are independently encoded into s_k^p and s_k^c, the private and common signal to be transmitted to user k. We assume the signals to be zero mean, unit variance complex Gaussian variables with the property of being independent identically distributed and circularly symmetric. Note that under RSMA s_k^p is intended to be decoded by user k only, while s_k^c may be decoded at multiple users, which necessitates a successive decoding strategy.

The channel vector linking user k and BS b is denoted by $\boldsymbol{h}_{b,k} \in \mathbb{C}^{L\times 1}$, and we define $\boldsymbol{h}_k = [(\boldsymbol{h}_{1,k})^T, \dots, (\boldsymbol{h}_{B,k})^T]^T \in \mathbb{C}^{LB\times 1}$ as the aggregate channel vector of user k. Similar to these definitions, we denote the beamforming vectors as $\boldsymbol{w}_{b,k}^o \in \mathbb{C}^{L\times 1}$ and the aggregate beamforming vectors as $\boldsymbol{w}_k^o = [(\boldsymbol{w}_{1,k}^o)^T, \dots, (\boldsymbol{w}_{B,k}^o)^T]^T \in \mathbb{C}^{LB\times 1}$, where $o \in \{p, c\}$ denotes private and common vectors, respectively. Throughout this work, the index o denotes the differentiation of private and common signal related variables.

Due to limited radio resources, BSs naturally have limited capabilities regarding the number of served users. Hence, we introduce the sets $\mathcal{K}_b^p$ and $\mathcal{K}_b^c$, which include only the users whose private or common signal is served by BS b. These clusters can be formulated as

$$\mathcal{K}_b^p = \{k \in \mathcal{K} | \text{BS } b \text{ serves } s_k^p\}, \tag{5a}$$

$$\mathcal{K}_b^c = \{k \in \mathcal{K} | \text{BS } b \text{ serves } s_k^c\}. \tag{5b}$$

Note that the design of these sets has crucial impact on the system performance. We provide more details in Appendix B. Thereby, the previously defined beamforming vectors often contain zeros, i.e., $\boldsymbol{w}_{b,k}^o = \boldsymbol{0}_L$ when $k \notin \mathcal{K}_b^o$. Each message stream transmits the data via a specific rate r_k^o, while the total rate assigned to user k is $r_k = r_k^p + r_k^c$. To ensure operation of the considered network, the CP has to respect the finite fronthaul capacity of the CP-BS links with

$$\sum\nolimits_{k\in\mathcal{K}_b^p} r_k^p + \sum\nolimits_{k\in\mathcal{K}_b^c} r_k^c \leq C_b^{\max}. \tag{6}$$

In what follows, we explain the construction of the transmit signal and the successive decoding scheme for the common streams.

1) Transmit Signal and Successive Decoding: Upon receiving the transmit signals and beamforming coefficients, the BSs construct the transmit signal $\boldsymbol{x}_b$ by

$$\boldsymbol{x}_b = \sum\nolimits_{k\in\mathcal{K}} \boldsymbol{w}_{b,k}^{p} s_k^{p} + \sum\nolimits_{k\in\mathcal{K}} \boldsymbol{w}_{b,k}^{c} s_k^{c}. \tag{7}$$

Thereby, the signal transmitted by each BS is subject to the maximum transmit power constraint denoted by

$$\mathbb{E}\{\boldsymbol{x}_b^H \boldsymbol{x}_b\} = \sum_{k\in\mathcal{K}} \left(\left\| \boldsymbol{w}_{b,k}^{p} \right\|_2^2 + \left\| \boldsymbol{w}_{b,k}^{c} \right\|_2^2 \right) \leq P_b^{\max}. \tag{8}$$

Note that (8) can be derived using the defined signal traits and assuming Gaussian codebooks, i.e., $\mathbb{E}\{|s_k^p|^2\} = \mathbb{E}\{|s_k^c|^2\} = 1$.

In the RSMA framework, multiple users may decode each common message to reduce the interference for messages decoded afterwards. It is thus relevant to consider additional definitions of the network, which are provided as follows:

- The set of users, which decode user k's common message, is defined by $\mathcal{M}_k = \{j \in \mathcal{K} | \text{user } j \text{ decodes } s_k^c\}$. Within this expression j is a set-internal auxiliary index.
- The users, whose common messages are decoded by user k, are denoted in the set $\mathcal{I}_k = \{i \in \mathcal{K} | k \in \mathcal{M}_i\}$, where i is a set-internal auxiliary index.
- The decoding order at user k is written as π_k, where $\pi_k(m) > \pi_k(i)$ means that user k decodes common message i before message m.
- The set of users, whose common messages are decoded after decoding user i's message at user k, become $\mathcal{I}'_{i,k} = \{m \in \mathcal{I}_k | \pi_k(m) > \pi_k(i)\}$.

A suitable method of calculating $\mathcal{M}_k$, $\mathcal{I}_k$, $\mathcal{I}'_{i,k}$, and π_k is provided by [14]. To better illustrate the impact of the above parameters, consider the following example: Let user 1's common message be decoded by user 1 and 2 and user 2's common message be decoded only by user 2, i.e., we obtain $\mathcal{M}_1 = \{1, 2\}$ and $\mathcal{M}_2 = \{2\}$. Consequently, we have $\mathcal{I}_1 = \{1\}$ and $\mathcal{I}_2 = \{1, 2\}$, meaning that user 1 decodes its own, and user 2 decodes both its own and user 1's common message. The decoding orders could be $\pi_1 = \{1\}$ and $\pi_2 = \{2 > 1\}$, where the latter describes user 2 decoding common message 1 before its own message. Hence, $\mathcal{I}'_{1,1} = \varnothing$, $\mathcal{I}'_{2,2} = \varnothing$, and $\mathcal{I}'_{1,2} = \{2\}$, since each user decodes its own common message last, and upon decoding user 1's common message, user 2 needs to decode its own message afterwards.

Upon reception, a user receives a superposition of all possible private and common messages sent by all network BSs. Based on the previous definitions, we obtain the received signal at user k as

$$\begin{aligned} y_k = \boldsymbol{h}_k^H \boldsymbol{w}_k^{p} s_k^{p} + \sum_{j\in\mathcal{I}_k} \boldsymbol{h}_k^H \boldsymbol{w}_j^{c} s_j^{c} + \sum_{m\in\mathcal{K}\setminus\{k\}} \boldsymbol{h}_k^H \boldsymbol{w}_m^{p} s_m^{p} \\ + \sum_{l\in\mathcal{K}\setminus\mathcal{I}_k} \boldsymbol{h}_k^H \boldsymbol{w}_l^{c} s_l^{c} + n_k. \end{aligned} \tag{9}$$

Here, $n_k \sim \mathcal{CN}(0, \sigma^2)$ represents additive white Gaussian noise, assumed to have the same power at all users. Equation (9) includes all users' private and common signals transmitted by all BSs in a superposition manner. In more details, in (9), the first two terms consist of private and common signals, which are decoded during the successive decoding. In contrast, the last three terms in (9) denote interference from private signals, common signals, and noise, respectively. Using this definition, the signal to interference plus noise ratio (SINR) of user k decoding its private message, i.e., Γ_k^p, and the common message of user i, i.e., $\Gamma_{i,k}^c$, are formulated respectively as

$$\Gamma_k^{p} = \frac{\left| \boldsymbol{h}_k^H \boldsymbol{w}_k^{p} \right|^2}{\sum\limits_{j\in\mathcal{K}\setminus\{k\}} \left| \boldsymbol{h}_k^H \boldsymbol{w}_j^{p} \right|^2 + \sum\limits_{l\in\mathcal{K}\setminus\mathcal{I}_k} \left| \boldsymbol{h}_k^H \boldsymbol{w}_l^{c} \right|^2 + \sigma^2}, \tag{10a}$$

$$\Gamma_{i,k}^{c} = \frac{\left| \boldsymbol{h}_k^H \boldsymbol{w}_i^{c} \right|^2}{\sum\limits_{j\in\mathcal{K}} \left| \boldsymbol{h}_k^H \boldsymbol{w}_j^{p} \right|^2 + \sum\limits_{l\in\{\{\mathcal{K}\setminus\mathcal{I}_k\}\cup\mathcal{I}'_{i,k}\}} \left| \boldsymbol{h}_k^H \boldsymbol{w}_l^{c} \right|^2 + \sigma^2}. \tag{10b}$$

2) Mixed Criticality-aware MSE Metric: To analyze the MSE of QoS deviation, i.e., the gap of desired and allocated rate, we define the metric Ψ as this paper's objective function:

$$\Psi = \frac{1}{|\mathcal{K}|} \sum_{k\in\mathcal{K}} \left| (r_k^{p} + r_k^{c}) - r_k^{\mathrm{des}} \right|^2, \tag{11}$$

where r_k^{des} is the desired rate of user k. Note that, due to different failure states (and consequences on network parameters, e.g., the wireless channel), the resource allocation based on (11) results in different solutions at different times, e.g. initial state, post-failure states. That is, the resource allocation is updated in a resilient manner, e.g., see Fig. 2. In (11), the mixed criticality of links is represented in r_k^{des}, where critical applications have greater QoS requirements than others.

Remark 1. *Minimizing a function based on the MSE such as* (11) *(alternatively based on the mean absolute error) contributes to finding a good trade-off between minimizing the resource usage and providing QoS. On the one hand, systems which can hardly fulfill the desired QoS will fall into a mode of maximizing each user's rate upon meeting those demands. On the other hand, as rate targets are met, no further enhancement of the rates is conducted, so as to avoid wasting resources which provides a form of energy efficiency.*

Note that an MSE-based metric as (11) does not guarantee QoS fulfillment, especially in networks with insufficient resources. However, such objective results in a solution, which best approaches the (unreachable) target rates, all while prioritizing critical users. To explain the effects of criticality on the resource management, we note that a optimal value of $\Psi = 0$ is only reachable, if all QoS requirements can be fulfilled, i.e., sufficient resources are available. Otherwise, when the network resources are insufficient, we have $\Psi > 0$. Now, assuming equal resource allocation, e.g., transmit power allocation, to both a high-critical and low-critical user with similar channel quality, the QoS deviation of the high-critical user would result in higher values of Ψ due to the *absolute value squared*-operator. Upon minimizing Ψ, the higher-critical users are assigned greater portions of the resources.

Such effect is best illustrated using the following example: Consider low-critical user 1 with $r_1^{\mathrm{des}} = 1$ and high-critical

user 2 with $r_2^{\mathrm{des}} = 4$. Further, consider that simplified the algorithm can only assign a total rate of 2. Under equal resource allocation, we obtain $\Psi = \frac{1}{2}\left((1-1)^2 + (1-4)^2\right) = 4.5$. Whereas the optimal allocation is $r_1 = 0$ and $r_2 = 2$, i.e., $\Psi = 2.5$. Under such strictly limited resources, the low-critical user is not served upon trying to fulfill the high-critical user QoS. Contrary, let the same system be capable of assigning a total rate of 3.5. With optimal allocation $r_1 = 0.25$ and $r_2 = 3.25$ we have $\Psi = 0.5625$. Thus, in this work, higher-critical users will be assigned a greater portion of the resources; however, they may not be strictly prioritized over the low-critical users in terms of halting the service. This is backed up by [52], which notes that for example based on the SILs it is not possible to completely sacrifice a lesser-critical for a higher-critical function.

B. Problem Formulation and Convexification

This paper considers the problem of minimizing the constrained network-wide rate gap (QoS deviation) as initial problem, which can be formulated mathematically as follows:

$$\begin{aligned} \min_{\boldsymbol{w},\boldsymbol{r},\boldsymbol{\mathcal{K}}} \quad & \Psi && (12)\\ \text{s.t.} \quad & (6), (8), \\ & r_k^p \le \tau \log_2(1+\Gamma_k^p), && \forall k \in \mathcal{K}, \quad (12a)\\ & r_i^c \le \tau \log_2(1+\Gamma_{i,k}^c), && \forall i \in \mathcal{I}_k, \forall k \in \mathcal{K}. \quad (12b) \end{aligned}$$

The above problem minimizes the gap of assigned (private and common) rate to the desired rate by jointly managing the allocated rates, beamforming vectors, and BS-user clustering. Hereby, the beamforming and rate vector

$$\begin{aligned} \boldsymbol{w} &= \left[\left(\boldsymbol{w}_1^p\right)^T, \ldots, \left(\boldsymbol{w}_K^p\right)^T, \left(\boldsymbol{w}_1^c\right)^T, \ldots, \left(\boldsymbol{w}_K^c\right)^T\right]^T, \\ \boldsymbol{r} &= \left[r_1^p, \ldots, r_K^p, r_1^c, \ldots, r_K^c\right]^T, \end{aligned}$$

and the clustering set $\boldsymbol{\mathcal{K}} = \{\mathcal{K}_b^o | \forall b \in \mathcal{B}, \forall o \in \{p, c\}\}$ denote the optimization variables. The feasible set of problem (12) is defined by the fronthaul capacity constraints per BS (6), the maximum transmit power constraint per BS (8), the achievable rates per user (12a) and (12b). The latter constraints, namely (12a) and (12b), depend on the SINR defined in (10a) and (10b), which is non-convex. In contrast, the objective function (12) is already in convex form, since the squared absolute value is convex. However, as the constraints (12a) and (12b) are non-convex, problem (12) is in general non-convex and difficult to solve directly. Therefore, this paper proposes various reformulation techniques to devise the optimization problem in a more tractable form.

A few notes on problem (12)'s constraints. Constraint (10b) takes the form of a multiple access constraint. Specifically, r_i^c is the rate of user i's common stream and the subset of users $\mathcal{M}_i$ are going to decode that specific signal. Therefore, r_i^c is bounded by the lowest $\Gamma_{i,k}^c$, i.e., the lowest SINR of all decoding users. Also, the constraints (6) and (8) are highly dependent on the clustering sets $\mathcal{K}_b^p$ and $\mathcal{K}_b^c$, which are also subject to optimization. Hence, problem (12) has non-convex constraints and is thus non-convex. Therefore, we propose a convex reformulation of problem (12) in Theorem 1 based on fractional programming, inner-convex approximation, and an l_0-norm approximation clustering approach. Before stating Theorem 1, consider the following definitions: Let $\boldsymbol{u}$ be an auxiliary variables vector defined as $\boldsymbol{u} = [(\boldsymbol{u}_1^p)^T, \ldots, (\boldsymbol{u}_K^p)^T, (\boldsymbol{u}_1^c)^T, \ldots, (\boldsymbol{u}_K^c)^T]^T$, consisting of $\boldsymbol{u}_k^o = [u_{1,k}^o, \ldots, u_{B,k}^o]^T$. Similarly, the auxiliary variable $\boldsymbol{\gamma}$ covers all possible non-zero elements of $\boldsymbol{\gamma}' = [\gamma_1^p, \ldots, \gamma_K^p, \gamma_{1,1}^c, \gamma_{1,2}^c, \ldots, \gamma_{K,K}^c]^T$, as each common message is only decoded by a part of all users. Let $\beta_{b,k}^o$ denote weights of the l_0-norm approximation. The functions $g^p(\boldsymbol{w}, \boldsymbol{\gamma})$ and $g^c(\boldsymbol{w}, \boldsymbol{\gamma})$ are defined as

$$\begin{aligned} g^p(\boldsymbol{w}, \boldsymbol{\gamma}) &= \gamma_k^p - 2\,\mathrm{Re}\Big\{(\chi_k^p)^* \left|\boldsymbol{h}_k^H \boldsymbol{w}_k^p\right|^2\Big\} + |\chi_k^p|^2 \\ &\quad \cdot \left[\sigma^2 + \sum_{j \in \mathcal{K}\setminus\{k\}} \left|\boldsymbol{h}_k^H \boldsymbol{w}_j^p\right|^2 + \sum_{l \in \mathcal{K}\setminus\mathcal{I}_k} \left|\boldsymbol{h}_k^H \boldsymbol{w}_l^c\right|^2\right], \quad (13) \\ g^c(\boldsymbol{w}, \boldsymbol{\gamma}) &= \gamma_{i,k}^c - 2\,\mathrm{Re}\Big\{(\chi_{i,k}^c)^* \left|\boldsymbol{h}_k^H \boldsymbol{w}_i^c\right|^2\Big\} + |\chi_{i,k}^c|^2 \\ &\quad \cdot \left[\sigma^2 + \sum_{j \in \mathcal{K}} \left|\boldsymbol{h}_k^H \boldsymbol{w}_j^p\right|^2 + \sum_{l \in \{\{\mathcal{K}\setminus\mathcal{I}_k\} \cup \mathcal{I}'_{i,k}\}} \left|\boldsymbol{h}_k^H \boldsymbol{w}_l^c\right|^2\right], \quad (14) \end{aligned}$$

where χ_k^o denote auxiliary variables of the quadratic transform. At last, the reformulated fronthaul constraint (6) is given as

$$\begin{aligned} \sum_{k \in \mathcal{K}} \Big(& \left(u_{b,k}^p + r_k^p\right)^2 - 2\left(\tilde{u}_{b,k}^p - \tilde{r}_k^p\right)\left(u_{b,k}^p - r_k^p\right) + \left(\tilde{u}_{b,k}^p - \tilde{r}_k^p\right)^2 \\ & + \left(u_{b,k}^c + r_k^c\right)^2 - 2\left(\tilde{u}_{b,k}^c - \tilde{r}_k^c\right)\left(u_{b,k}^c - r_k^c\right) + \\ & + \left(\tilde{u}_{b,k}^c - \tilde{r}_k^c\right)^2\Big) \le 4C_b^{\max}, \qquad \forall b \in \mathcal{B}, \quad (15) \end{aligned}$$

where $\tilde{\boldsymbol{u}}$ and $\tilde{\boldsymbol{r}}$ are feasible fixed values, which originate from the inner-convex approximation.

Theorem 1. *Problem* (12) *can be transformed into the following convex reformulation based on fractional programming, inner-convex approximation, and l_0-norm approximation:*

$$\begin{aligned} \min_{\boldsymbol{w},\boldsymbol{r},\boldsymbol{u},\boldsymbol{\gamma}} \quad & \Psi && (16)\\ \text{s.t.} \quad & (8), (15), \\ & r_k^p \le \tau \log_2(1+\gamma_k^p), && \forall k \in \mathcal{K}, \quad (16a)\\ & r_i^c \le \tau \log_2(1+\gamma_{i,k}^c), && \forall i \in \mathcal{I}_k, \forall k \in \mathcal{K}, \quad (16b)\\ & g^p(\boldsymbol{w}, \boldsymbol{\gamma}) \le 0, && \forall k \in \mathcal{K}, \quad (16c)\\ & g^c(\boldsymbol{w}, \boldsymbol{\gamma}) \le 0, && \forall i \in \mathcal{I}_k, \forall k \in \mathcal{K}, \quad (16d)\\ & \beta_{b,k}^p \left\|\boldsymbol{w}_{b,k}^p\right\|_2^2 \le u_{b,k}^p, \ \beta_{b,k}^c \left\|\boldsymbol{w}_{b,k}^c\right\|_2^2 \le u_{b,k}^c, && \\ & && \forall b \in \mathcal{B}, \forall k \in \mathcal{K}. \quad (16e) \end{aligned}$$

Proof. For a detailed derivation, we refer to Appendix A. □

An efficient procedure to solve the resource allocation problem of the considered network, i.e., problem (16), can be found in Appendix B of the extended version of the paper available on arxiv [2]. With the above considerations at hand, problem (16) is solved as an initial resource management step. The objective function defined in (11) provides the necessary means for mixed criticality-awareness of the resource allocation. Additionally, in networks with sufficient resources, e.g., fronthaul capacity, problem (16) yields a robust solution, providing high levels of *absorption*. This is due to the fact that the rates are allocated to meet the QoS, while the actual achievable rates might be much higher, i.e., so called SINR margins. Also,

network participants are multi-connected to multiple BSs. In resource limited networks, however, i.e., fronthaul capacity limited regimes, a solution based on problem (16) yields worse robustness, e.g., due to single-link connections, but achieves a best-effort QoS fulfillment solution. In other words, QoS targets might not be fully satisfied, whereas, due to the nature of Ψ (11), the priority lays in meeting high critical targets.

Remark 2. *Note that the resilience aspect* time-to-recovery *is not considered in the optimization problem itself, as closed-form expressions on the amount of time a remediation mechanism takes for resource allocation after an unexpected and unforseeable failure are hardly obtainable. The timing aspect, however, is respected by introducing multiple resilience mechanisms, whereas each proposed mechanism differs in approximated computation time.*

C. Resilient and Criticality-aware Resource Allocation

In this work, we utilize four different resilience mechanisms, which differ in calculation time and quality of recovery. Hence, the four algorithms can run in parallel to sequentially recover from the outage.

a) Resilience Mechanism 1 (M1): As first mechanism in line, *rate adaption* is used. Hereby, the algorithm calculates the achievable rates of all users, based on the new SINR measured after occurrence of the failure, while the beamformers are kept fixed. Thereby, from comparing allocated and achievable rate, the algorithm determines which users experience outage. The rate of these users is then set to the new achievable rate, which will be lower than the previously allocated rate and, in fact, might be zero. By doing so, M1 recovers the communication links to users, which otherwise could not decode their messages after outage due to unadjusted rates. *Rate adaption* is the resilience mechanism of the lowest complexity ($\mathcal{O}(1)$) and thus, also the fastest. However, it is also the weakest recovery mechanism, i.e., most recovered rates will only be a fraction of the users desired rate. We associate $e_{\text{ada}}^{(1)}$ and $e_{\text{rec}}^{(1)}$, i.e., the adaption and recovery metrics, with this mechanism.

b) Resilience Mechanism 2 (M2): As second resilience mechanism in line, *beamformer adaption* is employed. This scheme solves a reduced-complexity version of problem (16) and thereby calculates new beamforming coefficients while keeping the clustering fixed. The utilization of a previous feasible solution to initialize the procedure reduces the time to convergence. This mechanism has an intermediate complexity ($d_2 = K(2BL+K+3)$) but, compared to M1, leads to a higher recovered QoS. In comparison, this mechanism manages the interference more efficiently utilizing spatial dimensions. We associate $e_{\text{ada}}^{(2)}$ and $e_{\text{rec}}^{(2)}$.

c) Resilience Mechanism 3 (M3): This mechanism is referred to as *BS-user-allocation adaption* and repeats the network's clustering using the updated CSI by solving a generalized assignment problem (GAP). For more details on solving the GAP, we refer to Appendix B. Afterwards, the remaining mechanism operates analog to M2. This mechanism has a high complexity ($d_{3,1} = KB$ and $d_{3,2} = K(2BL + K + 3)$) but offers good-quality recovered QoS, we associate $e_{\text{ada}}^{(3)}$ and $e_{\text{rec}}^{(3)}$.

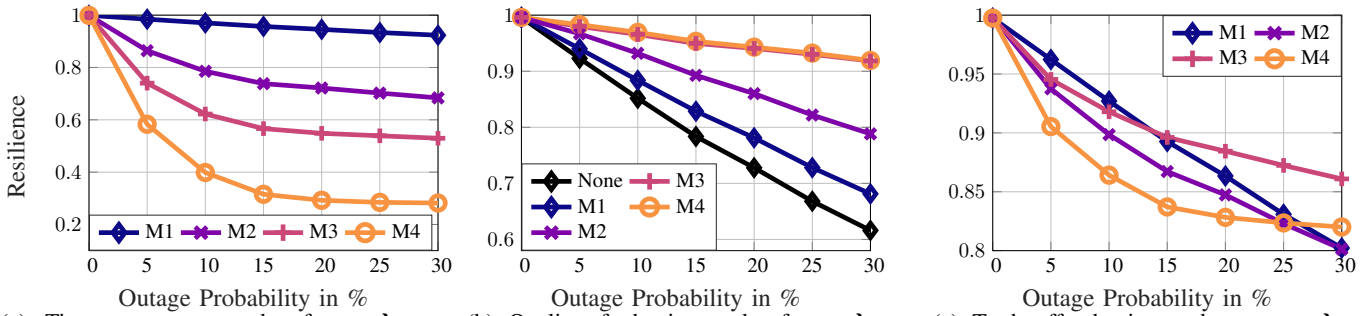
d) Resilience Mechanism 4 (M4): At last, we employ *comprehensive adaption*, which repeats the solution to problem (16), solving the network's clustering, beamforming, power control, and rate allocation jointly using the updated CSI. This mechanism has a very high complexity ($d_4 = K(2B(L+1)+K+3)$) and thus it is rather optimistic to use this technique in practice. However, this adaption can either be seen as an mechanism for networks with slowly changing channels or as bound and approximate for other resilience strategies. This yields $e_{\text{ada}}^{(4)}$ and $e_{\text{rec}}^{(4)}$.

The full mechanism, which detects outages and then applies the resilience mechanisms is referred to as *Resilient and Criticality-aware RSMA Resource Management* algorithm and can be found in Algorithm 1. The algorithm gets as input the desired rates of all user, as these rates are typically specified by the users. First, the initial solution resource allocation strategy is computed by solving problem (16). For each transmission, the algorithm checks if an outage occurs by checking if the new achievable rate of any user is smaller than the allocated rate. Note that ε refers to a small tolerance threshold value to increase robustness. If an outage or failure happens, the algorithm sequentially executes all four resilience mechanism, namely *rate adaption*, *beamformer adaption*, *BS-user-allocation adaption*, and *comprehensive adaption*, as described previously. Note that the algorithm stops as soon as any mechanism achieves the desired functionality, otherwise it finishes after *comprehensive adaption* ends. Thereby, we assume that no second failure occurs while executing the recovery mechanisms. Afterwards, the algorithm continues checking each transmission for outages.

Algorithm 1 Resilient and Criticality-aware RSMA Resource Management

Input: desired rate r_k^{des} $\forall k \in \mathcal{K}$
1: $\boldsymbol{r}$, $\boldsymbol{w}$, $\boldsymbol{u}$, $\boldsymbol{\gamma} \leftarrow$ solution from (16)
2: **while** true **do**
3: t_0, $\boldsymbol{r}(t_0) \leftarrow$ latest transmission time and achievable rate
4: ▷ *Obtain channel outage information*
5: **if** $\exists k : r_k(t_0) < r_k + \varepsilon$ **then**
6: ▷ *Resilience Mechanism 1 (rate adaption)*
7: $\boldsymbol{r} \leftarrow$ new achievable rates of (12a) and (12b)
8: ▷ *Resilience Mechanism 2 (beamformer adaption)*
9: $\boldsymbol{r}$, $\boldsymbol{w}$ $\leftarrow$ new solution to (12), starting from the previously feasible solution
10: ▷ *Resilience Mechanism 3 (BS-user-allocation adaption)*
11: $\mathcal{K}_b^p$, $\mathcal{K}_b^c$ $\forall b \in \mathcal{B} \leftarrow$ new clustering, see Appendix B
12: $\boldsymbol{r}$, $\boldsymbol{w}$ $\leftarrow$ new solution to (12)
13: ▷ *Resilience Mechanism 4 (comprehensive adaption)*
14: $\boldsymbol{r}$, $\boldsymbol{w}$, $\boldsymbol{u}$, $\boldsymbol{\gamma} \leftarrow$ new solution to (16)
15: **end if**
16: **end while**

Remark 3. *When having the choice between multiple resilience mechanism, the resilience mechanisms with the fastest computation time should be scheduled first, while the ones leading to the highest recovery quality should be scheduled last. Thereby, it depends on the different computation times*



(a) Time-to-recovery under focus, $\boldsymbol{\lambda} = [0.2,\ 0.0,\ 0.8]$.
(b) Quality-of-adaption under focus, $\boldsymbol{\lambda} = [0.2,\ 0.8,\ 0.0]$.
(c) Trade-off adaption and recovery, $\boldsymbol{\lambda} = [0.2,\ 0.4,\ 0.4]$.

Figure 3: Resilience over outage probability comparing the mechanisms.

and recovery qualities, if it is optimal to use all mechanisms, or just a few of them.

IV. Numerical Simulations

To evaluate the performance of the proposed methods, we conduct numerical simulations in this section. Please note that in this paper, we conduct numerical simulations to demonstrate and validate the inherent advantages of applying criticality-aware resilience in the considered system model. The Monte-Carlo simulations are done via MATLAB. Future works may include a formal proof to back up the theoretical aspects of the proposed scheme, and practical demonstration setups to show the applicability to real-world communication system use cases. We consider a network over a square area of $800\,\mathrm{m}$ by $800\,\mathrm{m}$, in which BSs and users are placed randomly. Each BS is equipped with $L = 2$ antennas and has a maximum transmit power of $P_b^{\max} = 28\,\mathrm{dBm}$. Unless mentioned otherwise, we fix $C_b^{\max} = 50\,\mathrm{Mbps}$, the number of BS $B = 6$, and the number of users $K = 14$. Regarding M3, the assignment problem related parameters are set as $B_k^{\max} = 2$ and $K_n^{\max} = 2 \cdot K$. We consider a channel bandwidth of $\tau = 10\,\mathrm{MHz}$, and a path-loss model given by $\mathrm{PL}_{b,k} = 128.1 + 37.6 \cdot \log_{10}(d_{b,k})$, where the distance of user k and BS b is denoted as $d_{b,k}$. Additionally, we consider log-normal shadowing with 8 dB standard deviation and Rayleigh fading with zero mean and unit variance. The noise power spectral density is $-168\,\mathrm{dBm/Hz}$. Unless mentioned otherwise, we set the mixed-critical QoS demands r_k^{des} to $12\,\mathrm{Mbps}$, $8\,\mathrm{Mbps}$, and $4\,\mathrm{Mbps}$. Users are randomly assigned to criticality levels, whereas each criticality level consists of 4 users. This corresponds to three criticality levels, namely high (HI), medium (ME), and low (LO).

In the simulations, a failure is modeled as the loss of connection between a user and a BS. We construct a uniformly distributed random matrix (distributed between 0 and 1) representing the links of BSs and users. The severity of system failures is determined by the amount of links, which are blocked, i.e., the outage probability. For example, 50% outage probability refers to all links with values ≥ 0.5 in the random matrix being blocked. While this failure model is a first step, the considered link-level binary failure model is sufficient to show the effectiveness and importance of resilience and criticality-awareness for potential 6G communication networks. More sophisticated failure models need, however, to be considered in future works.

A. Resilience Components

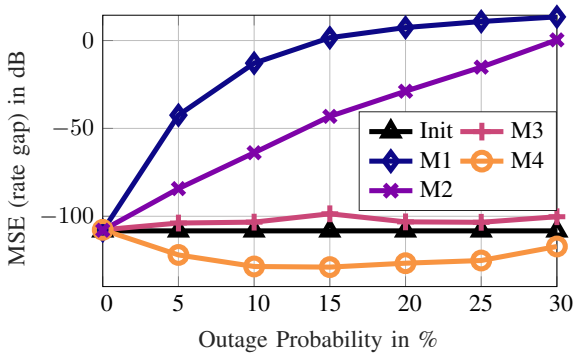
At first, we aim at comparing the proposed mechanisms in terms of resilience and analyzing the individual components of resilience, i.e., absorption, adaption, recovery, and how they combine.

In the first set of simulations, we compare the performance of the four considered schemes in terms of resilience, i.e., $e^{(n)}$ as per (11), where $n \in \{1, \cdots, 4\}$. Fig. 3 shows three plots from the same data set, differing in the exact weightings $\boldsymbol{\lambda}$ in (11). That is, Fig. 3a shows the resilience when the *recovery* (time-to-recovery) is weighted most, i.e., systems where timely recovery is valued over all other aspects, over the channel outage probability. As expected, M1 and M2 provide the fastest recovery due to inhabiting the lowest complexity, however, this result does not capture the quality-of-adaption. The resilience of M3 and M4 decreases with increasing outage probability. Interestingly, we observe a stabilization at approximately 15%, implying that this parameter has only slight impact on the calculation time of M3 and M4. In contrast, M2 and especially M1 are steadily decreasing with rising outage probability. This behavior comes due to the fact that M1's computation time is strongly coupled to the amount of users experiencing outages. M2 is in part dependent on the quality of the previously feasible solution, and with increasing outages, the previous solution looses its value as an initial point.

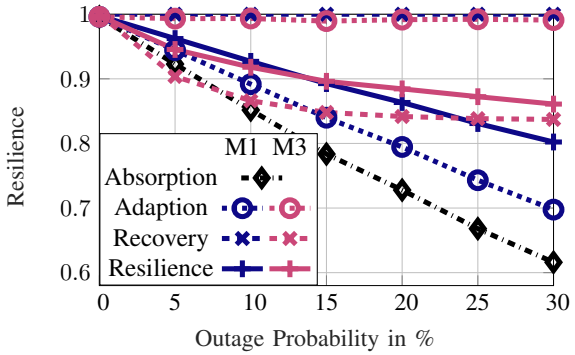
In Fig. 3b, the resilience for setups, which value *adaption* most, is plotted over outage probability. Results emphasize the quality-of-adaption difference of the mechanisms, as M1 performs worst, M2 medium, and M3 as well as M4 best. Interestingly, we observe M3 closely approaching M4, which, for this network setup, highlights M3's superiority, as it is less complex than M4 providing almost the same *adaption*. Overall, Fig. 3b underlines the need for resilience, especially in networks where channel outages occur, i.e., all realistic setups, as all mechanisms outperform the *no-reaction* baseline (None), where no resilience action is taken.

A combination of both results is shown in Fig. 3c. We show the resilience versus the outage probability for a reasonable trade-off weight vector. It comes clear that a dynamic switching between M1 and M3 provides the best resilience over the considered outage probabilities. While at the lower probabilities, such scheme mostly benefits from M1's quick recovery, at higher values, M3's quality-of-adaption are most beneficial.

From Fig. 4a, we get a different point of view, as the figure

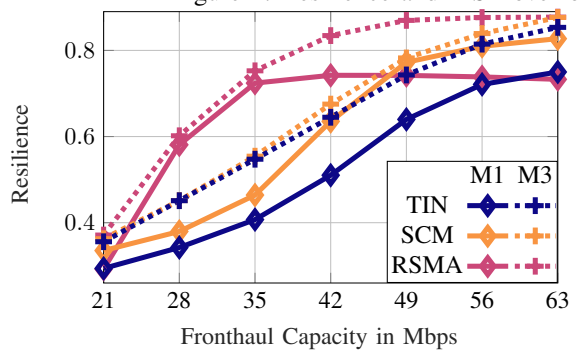


(a) MSE in dB comparing initial solution and all mechanisms.

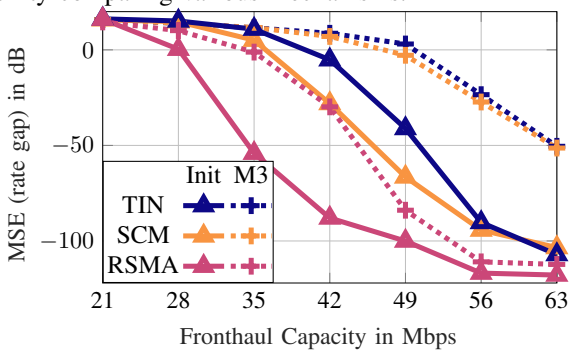


(b) Resilience components of M1 and M2, with $\boldsymbol{\lambda} = [0.2,\ 0.4,\ 0.4]$.

Figure 4: Resilience and MSE over outage probability comparing various mechanisms.



(a) Resilience of TIN, SCM, and RSMA for M1 and M3.



(b) MSE in dB comparing initial solution and M3.

Figure 5: Resilience and MSE over fronthaul capacity comparing interference management schemes.

shows the objective function (12), i.e., the MSE in dB as a function of outage probability. The initial performance (Init) depicts the performance baseline of the algorithm for 0% outage probability. While M1 and M2 are significantly affected by the rising outages, M3 performs close to and M4 even outperforms Init. This emphasizes the fact that a re-clustering approach as M3 can almost keep the initial performance level facing outages. The performance gap between M3 and M4 can be seen as a dynamic clustering benefit, as such approach can lower the MSE even further. Note that outages do not solely impact active channels, channels that cause interference (e.g., unassociated BS and user) are also subject to outage. Thus, M4 can beat the initial performance facing outages.

The individual aspects of the proposed resilience metric are shown in Fig. 4b for M1 and M3. Here, absorption, adaption, recovery, and the resulting total resilience are plotted. Consistent with previous observations, M1 has a better time-to-recovery, yet worse adaption and thus worse total resilience, than M3. Note that the herein considered results are highly dependent on the weight vector $\boldsymbol{\lambda}$, which has to be tailored to the needs of different services, networks, and providers.

B. Impact of Interference Management Techniques

In addition to the herein proposed scheme, referred to as RSMA, we consider 2 different reference schemes for interference management, namely treating interference as noise (TIN) and a single common message (SCM)-based RSMA scheme. TIN does not consider any rate-splitting capabilities, i.e., TIN is less complex than RSMA, yet offers less opportunities for resilience, e.g., redundant and diverse message streams. Contrary to that, the SCM scheme employs one-layer rate-splitting, where one *super common* stream (additional message stream) is decoded by all users in addition to private messages, e.g., used in [15], [19]. SCM requires each user to decode two messages, therefore, has higher complexity than TIN, but lower complexity than RSMA. Hence, such complexity differences have impact on the time-to-recovery $e_{\text{rec}}^{(n)}$, as computing times differ. As a highlight of the proposed resilience metric, it captures these computation time differences numerically within the overall resilience metric (11). Thereby, the comparison of RSMA, SCM, and TIN in terms of resilience is fair by nature, as it includes complexity differences.

Fig. 5a shows the resilience of M1 and M3 using TIN, SCM, and RSMA as a function of the fronthaul capacity for an outage probability of 25%, with $\boldsymbol{\lambda} = [0.3,\ 0.65,\ 0.05]$. Observing M1, all three plots have a similar starting point at $C_b^{\max} = 21\,\text{Mbps}$ and saturate at higher capacities. Especially in the medium fronthaul regime, i.e., mostly relevant in practice, (here, $28 - 49$ Mbps), RSMA provides significant resilience enhancements compared to TIN and SCM. Similarly, SCM is able to outperform TIN in every point of the x-axis. This result highlights the potential gain from using rate-splitting-based schemes for ensuring resilience of communication networks. In the higher fronhaul regime, where QoS targets are easily achievable, RSMA is outperformed by SCM (and TIN), as time-to-recovery gains importance over quality-of-adaption, especially for M1, which is the fastest mechanism. Considering M3, we observe that RSMA outperforms SCM and TIN for all fronthaul capacities, emphasizing the gain of the proposed scheme in terms of resilience.

To gain insights into the algorithm's behavior in terms of rate gap, i.e., MSE objective (11), Fig. 5b plots Ψ in dB as a

function of $C_b^{\max}$ for the initial solution (Init), i.e., performance before outage, and M3. RSMA's initial performance is able to provide the lowest MSE among all interference management schemes, saturating at high fronthaul capacity, as QoS targets are already met up to a minimal error, which explains the reduced gap towards TIN and SCM. Interestingly, observing M3's MSE performance, it is noteable that RSMA enables the mechanisms to closely approach the MSE performance before outage. In contrast, TIN and SCM experience a large gap between Init and M3, highlighting RSMA's resilience enhancing capabilities.

C. Longer Scale Resilience

In these set of simulations, we consider only the proposed scheme and investigate its performance as a function of time facing subsequent outage events, which increase in their severity over time. In more details, the first event denotes channel outages with 10% probability, and all following events have additional 10% probability each. The times of these outage events (upper plot), the throughput, which is defined as the sum of allocated rates that are achievable, the sum QoS target, and the adaption events (middle plot), as well as the momentarily resilience (lower plot) are shown in Fig. 6. Plenty of observations can be made: Algorithm 1 is able to recover the throughput completely (after some time) for events up to 70% channel outage probabilities. While the throughput is able to be restored (for events 1-6), the resilience does never return to 1, which comes from the time-to-recovery component. Regardless of the severity of outages, M1 offers outstanding time-to-recovery while also providing good adaption. Especially at the earlier events, consider the gap of resilience at the time of outage and at the time of M1's adaption: This gap is larger than at other mechanisms. While for lower outage probabilities, the first two mechanisms provide the best throughput adaption, and thus resilience, in high outage regime, M3 and M4 dominate the achievable adaption and the resilience quality. This results captures once again the trade-off between quality and time of adaption, which the proposed resilience metric includes. Interestingly, even in the face of 90% outages, especially the *BS-user-allocation adaption* is able to recover the throughput up to around $70\,\mathrm{Mbps}$, which is more than 50% of the QoS target. In comparison to the proposed resource management scheme, Fig. 6 shows the throughput of a non-resilient system. With no mitigation techniques employed, the non-resilient system can not restore the throughput and features major loss. On the final outage event, the non-resilient system even completely looses the connection. These results further emphasize the suitability of C-RAN, especially due to the great amount of links between BSs and users, for resilient networks, as C-RAN provides great absorption and adaption potential. Further, the advantages of applying resilience in terms of throughput and, consequently, transmission delay are validated.

D. Data Rate Performance

In the last set of simulations, for the ease of presentation, we consider a small network with $B = 2$ BSs, $K = 3$ users, and

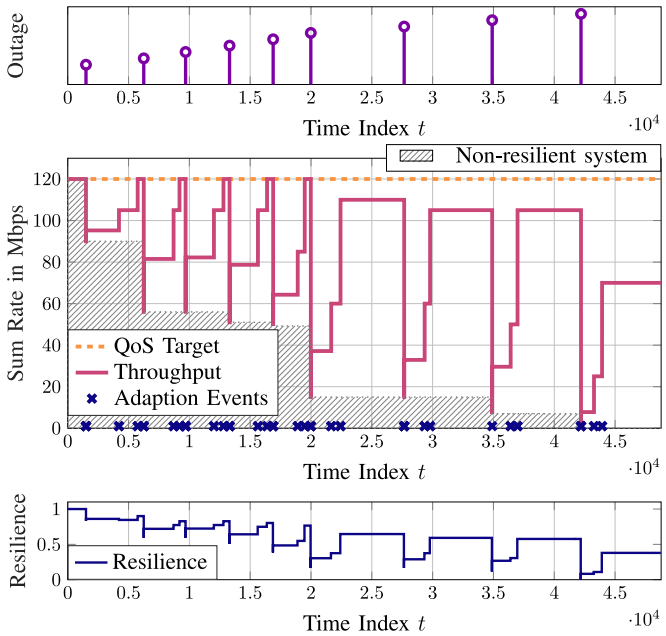


Figure 6: Throughput, adaption events, and resilience over the time index t facing subsequent outage events.

an outage probability of 60%, whereas users $1, 2, 3$ represent HI, ME, and LO critical levels, with $r_k^{\mathrm{des}} \in \{15, 10, 5\}\mathrm{Mbps}$. Fig. 7 depicts each users private and common data rate in Mbps for each discrete time point of the resilience procedure. In other words, Fig. 7 shows an example recovery process, similar to Fig. 6 for a single outage event, but with more details in terms of user rates and RSMA message split. From the initial solution, which shows a balanced allocation of private and common rate for each user, the network experiences severe performance degradation after the outage. Users 1 and 2 degrade to zero-rate and user 3 remains connected only by the common message. The fast M1 is able to recover parts of the rates, significantly boosting the performance back up, whereas mostly common rates can be restored. Consequently, M2 is able to restore the rate to a level similar to before the outage. At this point, Algorithm 1 may choose to abort the adaption process, dependent on the computational resources. However, by re-clustering, M3 changes the rate allocation towards enabling only private messages. This interesting behavior can be explained by the loss of about 60% of links, including interference links. In the new situation, common message decoding, as per the proposed RSMA scheme, is not needed due to the decreased interference. At last, M4 does not influence the resource allocation in this case. These results, albeit missing the timing (time-to-recovery) information, show the high dynamics of private and common rate during the adaption process, which emphasize the promising factor that RSMA provides for high levels of resilience within a mixed-critical network.

V. Conclusion

Serving the needs of mixed-critical functional safety in future 6G networks is reliant on modern resource management techniques not only respecting the mixed criticality aspect

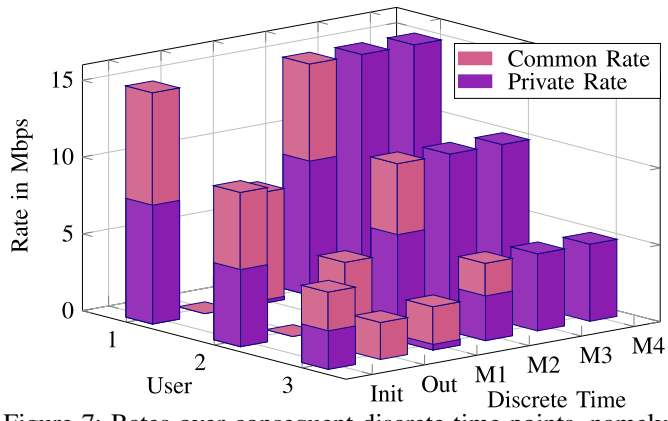


Figure 7: Rates over consequent discrete time points, namely, initial allocation, outage rate, recovered rates from M1-M4.

but also providing high levels of resilience, to enable fault tolerance and ensuring safety for operating personnel, environment, and machinery. This contribution proposes a metric for jointly incorporating mixed criticality and resilience for the physical layer resource management respecting diverse QoS targets. This paradigm is investigated in an RSMA-enabled C-RAN subject to maximum transmit power, fronthaul capacity, and achievable private and common message rate constraints. An efficient resource management algorithm was derived using fractional programming, inner-convex approximation, and l_0-norm approximation. Building upon these considerations, four resilience mechanisms differing in complexity and expected quality-of-adaption are proposed and combined into a resilience and criticality-aware RSMA-enabled resource management algorithm. Various numerical results show the dynamics of the proposed metric, the resilience and MSE behavior, the resilience over consecutive outage events, and an explicit recovery procedure. Results show that there is a trade-off between the optimal resilience mechanism and the outage probability, RSMA outperforms reference interference management schemes, and the consideration of mixed criticality is a crucial factor in the considered system model. A simulation of the algorithm's behavior over time verifies the practical and numerical merits of the proposed scheme, and emphasizes its importance for future 6G wireless communication networks.

Unifying the frameworks mixed criticality and resilience becomes a major enabler for 6G as a means to enable critical use cases and many extended applications. Future challenges include finding trade-offs between robustness and post-failure resilience, i.e., how to balance resources which are reserved for expected fluctuations and for unexpected events. Further, fast detection becomes vital in time-critical contexts, where the time-to-recovery is of special interest. In future works, the failure model for the wireless communication systems can potentially be extended to include more sophisticated influences, e.g., unforseeable processing latencies, link congestion, etc. This also relates to considering different system stability aspects, different types of failures, and the consideration of Lyapunov optimization techniques. Lastly, the prospects of different remediation mechanisms and the idea of learning to be resilient from unexpected failures of the past need to be considered. Resilience and mixed criticality in modern communication systems provide thus a huge research area with many open directions and prospects.

Appendix A
Proof of Theorem 1

1) Inner-convex and l_0-norm approximation: Problem (12) is a mixed-integer non-convex optimization problem due to the variables $\boldsymbol{\mathcal{K}}$ and fronthaul constraint (6), reformulated as

$$\sum_{k\in\mathcal{K}} \left(\left\| \left\| \boldsymbol{w}_{b,k}^{p} \right\|_2^2 \right\|_0 r_k^p + \left\| \left\| \boldsymbol{w}_{b,k}^{c} \right\|_2^2 \right\|_0 r_k^c \right) \leq C_b^{\max}, \quad \forall b \in \mathcal{B}. \tag{17}$$

The discrete l_0-norm in (17) helps formulating the constraint in such a way, that a possible transmission of user k's signal over the fronthaul link of BS b is indicated by the entries of the beamforming vector of k's signal at b. In more details, $\left\| \left\| \boldsymbol{w}_{b,k}^{p} \right\|_2^2 \right\|_0 = 1$, if and only if b allocates some power towards k's private message (similar for the common message), otherwise it is zero. Following [53], we approximate the l_0-norm with a weighted l_1-norm as $\left\| \left\| \boldsymbol{w}_{b,k}^{o} \right\|_2^2 \right\|_0 \approx \beta_{b,k}^{o} \left\| \left\| \boldsymbol{w}_{b,k}^{p} \right\|_2^2 \right\|_1$, where $\beta_{b,k}^{o}$ are the weights calculated by $\beta_{b,k}^{o} = \left(\delta + \left\| \boldsymbol{w}_{b,k}^{o} \right\|_2^2 \right)^{-1}$, with $\delta > 0$ being a regularization constant. Note that this formulation is an application of l_1-norm to a quadratic function of the beamformers, which yields a smooth, convex, and continuous function. A few notes on the weights: In case BS b assigns low transmit powers to user k's private or common signal, $\beta_{b,k}^{o}$ increases. Having the choice to serve only few selected users with reasonable transmit power allocation, the algorithm would eventually exclude messages with high weights in order to achieve higher rates, since the fronthaul link is a bottleneck in C-RAN. This interplay naturally balances the load between the BSs and leaves users being served only by BSs with reasonable transmit power. The fronthaul constraint becomes thereby

$$\sum_{k\in\mathcal{K}} \left(\beta_{b,k}^{p} \left\| \boldsymbol{w}_{b,k}^{p} \right\|_2^2 r_k^p + \beta_{b,k}^{c} \left\| \boldsymbol{w}_{b,k}^{c} \right\|_2^2 r_k^c \right) \leq C_b^{\max}, \quad \forall b \in \mathcal{B}. \tag{18}$$

Note that the l_1-norm is omitted here as the argument is scalar. By introducing the slack variable $\boldsymbol{u}$, we transform (18) into the constraints (16e) and

$$\sum_{k\in\mathcal{K}} \left(u_{b,k}^{p} r_k^p + u_{b,k}^{c} r_k^c \right) \leq C_b^{\max}, \quad \forall b \in \mathcal{B}, \tag{19}$$

which is bilinear in the optimization variables and thereby amenable for applying ICA. In this context, we first provide an equivalent difference of convex formulation of (19) and subsequently create a first-order Taylor series expansion of the non-convex terms around operating points:

$$\sum_{k\in\mathcal{K}} \frac{1}{4} \Big(\big((u_{b,k}^{p} + r_k^p)^2 - (u_{b,k}^{p} - r_k^p)^2 \big) + \big((u_{b,k}^{c} + r_k^c)^2 - (u_{b,k}^{c} - r_k^c)^2 \big) \Big) \leq C_b^{\max}, \tag{20}$$

and the first-order Taylor series expansion around $\tilde{\boldsymbol{u}}$ and $\tilde{\boldsymbol{r}}$, being feasible fixed values from the previous iteration's solution, is then formulated into (15). Note that $\tilde{\boldsymbol{u}}$ and $\tilde{\boldsymbol{r}}$ are vectors of similar dimension as $\boldsymbol{u}$ and $\boldsymbol{r}$, respectively.

2) Quadratic transform: Due to the complex fractional form of constraints (12a) and (12b), the problem (12) is of non-convex nature. We consider the following Lemma 1, to introduce γ_k^p and $\gamma_{i,k}^c$ for the SINR terms, and transform the original non-convex problem.

Lemma 1. *A rewritten formulation of the optimization problem* (12)*, including ICA and l_0-norm relaxation, is given by*

$$\begin{aligned}
\min_{\boldsymbol{w},\boldsymbol{r},\boldsymbol{u},\boldsymbol{\gamma}} \quad & \Psi && (21)\\
\text{s.t.} \quad & (8),(15),(16e),\\
& r_k^p \le \tau \log_2(1+\gamma_k^p), && \forall k \in \mathcal{K}, \quad (21a)\\
& r_i^c \le \tau \log_2(1+\gamma_{i,k}^c), && \forall i \in \mathcal{I}_k, \forall k \in \mathcal{K}, \quad (21b)\\
& \gamma_k^p \le \Gamma_k^p, && \forall k \in \mathcal{K}, \quad (21c)\\
& \gamma_{i,k}^c \le \Gamma_{i,k}^c, && \forall i \in \mathcal{I}_k, \forall k \in \mathcal{K}. \quad (21d)
\end{aligned}$$

Given the stationary solution $(\boldsymbol{w}^\star, \boldsymbol{r}^\star, \boldsymbol{u}^\star, \boldsymbol{\gamma}^\star)$ to problem (21)*, we note that $(\boldsymbol{w}^\star, \boldsymbol{r}^\star, \boldsymbol{u}^\star)$ is a stationary solution of the l_1-norm approximation of problem* (12)*.*

Problem (21) is still non-convex due to the constraints (21c) and (21d). However, such formulations are amenable for applying fractional programming techniques. Especially, we utilize the quadratic transform (QT) in multidimensional and complex case proposed by [54, Theorem 2], tailored to the constraints (21c) and (21d) in this work. In more details, after subtracting the right term from both sides and applying QT, the functions can be formulated as given in (13) and (14), respectively. In this context, (13) and (14) are the QT formulations of (21c) and (21d), respectively, where χ_k^p and $\chi_{i,k}^c$ are auxiliary variables. Consider following remark on the convexity of (13) and (14), and Lemma 2 for obtaining the optimal auxiliary variables, when $\boldsymbol{w}$ and $\boldsymbol{\gamma}$ are fixed.

Remark 4. *For fixed χ_k^p and $\chi_{i,k}^c$, the second terms in* (13) *and* (14) *become linear functions of the beamformers, also the latter terms become convex. Thus,* (13) *and* (14) *denote convex functions of the beamforming vectors and the SINR variables, in case the auxiliary variables are fixed.*

Lemma 2. *The optimal auxiliary variable results are*

$$\chi_k^p = \frac{\left(\boldsymbol{w}_k^p\right)^H \boldsymbol{h}_k}{\sigma^2 + \sum\limits_{j \in \mathcal{K}\setminus\{k\}} \left|\boldsymbol{h}_k^H \boldsymbol{w}_j^p\right|^2 + \sum\limits_{l \in \mathcal{K}\setminus\mathcal{I}_k} \left|\boldsymbol{h}_k^H \boldsymbol{w}_l^c\right|^2}, \tag{22}$$

$$\chi_{i,k}^c = \frac{\left(\boldsymbol{w}_i^c\right)^H \boldsymbol{h}_k}{\sigma^2 + \sum\limits_{j \in \mathcal{K}} \left|\boldsymbol{h}_k^H \boldsymbol{w}_j^p\right|^2 + \sum\limits_{l \in \{\{\mathcal{K}\setminus\mathcal{I}_k\}\cup\mathcal{I}'_{i,k}\}} \left|\boldsymbol{h}_k^H \boldsymbol{w}_l^c\right|^2}. \tag{23}$$

Due to the nature of the QT, which requires the update of auxiliary variables in an iterative fashion, the overall solution results an iterative procedure. Thereby, the algorithm computes the auxiliary variables following Lemma 2, for given beamforming vectors, and consequently solves a convex problem resulting optimal resource allocation variables. At each iteration, the optimization problem is given in (16) (as defined above). Hereby, the objective function (16) and the feasible set defined by all constraints are convex. Therefore, problem (16) is a convex optimization problem that can efficiently solved using established solvers, such as CVX [55]. Proofs of the Lemmas can be found in the extended paper version [2].

APPENDIX B
GAP-BASED CLUSTERING

The clustering sets are computed by a generalized assignment problem formulation. To obtain $\mathcal{K}_b^p$ and $\mathcal{K}_b^c$, we define the binary variable $\nu_{b,k}^o \in \{0,1\}$, $o \in \{p,c\}$, referring to BS b serving the private (or common) message of user k. Next, we give a GAP-based formulation which captures the benefit of assigning BS b to serve a message intended for user k. Such benefit is defined in terms of the channel norm, so as to preferably utilize strong links. This can be mathematically formulated as

$$\begin{aligned}
\max_{\boldsymbol{\nu}} \quad & \sum_{(k,b)\in(\mathcal{K},\mathcal{B})} \left(\nu_{b,k}^p \left\|\boldsymbol{h}_{b,k}\right\|_2^2 + \nu_{b,k}^c \sum_{i \in \mathcal{M}_k} \left\|\boldsymbol{h}_{b,i}\right\|_2^2 \right) && (24)\\
\text{s.t.} \quad & \sum_{b \in \mathcal{B}} \nu_{b,k}^o \le B_k^{\max}, && \forall k \in \mathcal{K}, \forall o \in \{p,c\}, \quad (24a)\\
& \sum_{k \in \mathcal{K}} \nu_{b,k}^p + \nu_{b,k}^c \le I_b^{\max}, && \forall b \in \mathcal{B}, \quad (24b)\\
& \nu_{b,k}^p + \nu_{b,k}^c \le 1, && \forall k \in \mathcal{K}, \forall b \in \mathcal{B}. \quad (24c)
\end{aligned}$$

Problem (24) maximizes a channel quality utility by jointly optimizing the binary clustering variables $\boldsymbol{\nu} = \left[\nu_{1,1}^p, \nu_{1,2}^p, \ldots, \nu_{B,K}^p, \nu_{1,1}^c, \ldots, \nu_{B,K}^c\right]^T$ and is in the form of a integer linear program (ILP). Constraint (24a) restricts the maximum number of BSs that serve the private (common) message of each user, where $B_k^{\max}$ are the maximum number of BSs per message. Each BS can only serve a fixed number of messages, which is denoted by (24b), where $I_b^{\max}$ describes the maximal amount of supported messages. Both of the previously mentioned constraints help balancing the load. Constraint (24c) is especially chosen to enhance the resilience behavior of the proposed RSMA scheme. The idea behind (24c) is to split the serving BSs of both private and common message of user k. Thereby, the scheme becomes more resilient when outages occur.

Problem (24) follows a GAP structure [56] and can be solved using well studied methods, e.g., branch and cut algorithm [57]. This allows us to fix the clustering sets $\mathcal{K}_b^p$ and $\mathcal{K}_b^c$, by setting $\mathcal{K}_b^o = \{k \in \mathcal{K} | \nu_{b,k}^o = 1\}$.

REFERENCES

[1] R.-J. Reifert, S. Roth, A. A. Ahmad, and A. Sezgin, "Energy efficiency in rate-splitting multiple access with mixed criticality," in *Proc. IEEE ICC Workshops*, 2022, pp. 681–686.

[2] ——, "Comeback kid: Resilience for mixed-critical wireless network resource management," 2022. [Online]. Available: https://arxiv.org/abs/2204.11878

[3] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies," *IEEE Access*, vol. 7, pp. 175 758–175 768, 2019.

[4] L. Zhang, Y.-C. Liang, and D. Niyato, "6G visions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence," *China Communications*, vol. 16, no. 8, pp. 1–14, 2019.

[5] "Ericsson mobility report november 2021," Ericson, Tech. Rep., Nov. 2021. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2021

[6] H. Farag, E. Sisinni, M. Gidlund, and P. Österberg, "Priority-aware wireless fieldbus protocol for mixed-criticality industrial wireless sensor networks," *IEEE Sens. J.*, vol. 19, no. 7, pp. 2767–2780, 2019.

[7] A. A. Ahmad, H. Dahrouj, A. Chaaban, A. Sezgin, T. Y. Al-Naffouri, and M.-S. Alouini, "Power minimization via rate splitting in downlink cloud-radio access networks," in *IEEE ICC Workshops*, 2020, pp. 1–6.

[8] C. Pan, H. Zhu, N. J. Gomes, and J. Wang, "Joint user selection and energy minimization for ultra-dense multi-channel C-RAN with incomplete CSI," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 8, pp. 1809–1824, 2017.

[9] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[10] S. Schwarz, "Resilience in psychology: A critical analysis of the concept," *Theory & Psychology*, vol. 28, no. 4, pp. 528–541, 2018.

[11] J. Park, S. E. Thompson, T. P. Seager, F. Zhao, S. Beigzadeh-Milani, R. Wu, and P. S. C. Rao, "Design for resilience in coupled industrial-ecological systems: Biofuels industry as a case study," in *IEEE ISSST*, 2011, pp. 1–1.

[12] J. P. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, and J. P. Rohrer, "Modelling and analysis of network resilience," in *3rd COMSNETS*, 2011, pp. 1–10.

[13] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, 2013.

[14] A. A. Ahmad, Y. Mao, A. Sezgin, and B. Clerckx, "Rate splitting multiple access in c-ran: A scalable and robust design," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 5727–5743, 2021.

[15] H. Joudeh and B. Clerckx, "Robust transmission in downlink multiuser MISO systems: A rate-splitting approach," *IEEE Trans. Signal Process*, vol. 64, no. 23, pp. 6227–6242, 2016.

[16] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, 1981.

[17] R. H. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5534–5562, 2008.

[18] H. Dahrouj and W. Yu, "Multicell interference mitigation with joint beamforming and common message decoding," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2264–2273, 2011.

[19] Y. Mao, B. Clerckx, and V. O. K. Li, "Rate-splitting for multi-antenna non-orthogonal unicast and multicast transmission: Spectral and energy efficiency analysis," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8754–8770, 2019.

[20] Y. Mao, O. Dizdar, B. Clerckx, R. Schober, P. Popovski, and H. V. Poor, "Rate-splitting multiple access: Fundamentals, survey, and future research trends," 2022. [Online]. Available: https://arxiv.org/abs/2201.03192

[21] A. Sezgin, "The diversity multiplexing tradeoff for interference networks," in *22nd WSA*, 2018, pp. 1–7.

[22] A. Chaaban and A. Sezgin, "The capacity region of the linear shift deterministic y-channel," in *IEEE Int. Symp. Inf. Theory*, 2011, pp. 2457–2461.

[23] J. Kakar, S. Gherekhloo, Z. H. Awan, and A. Sezgin, "Fundamental limits on latency in cloud- and cache-aided hetnets," in *IEEE ICC*, 2017, pp. 1–6.

[24] A. Sezgin, A. S. Avestimehr, M. A. Khajehnejad, and B. Hassibi, "Divide-and-conquer: Approaching the capacity of the two-pair bidirectional gaussian relay network," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2434–2454, 2012.

[25] "IEC 61508 (all parts), Functional Safety of Electrical /Electronic/Programmable Electronic Safety-related Systems," International Electrotechnical Commission, Geneva, CH, Standard, Apr. 2010.

[26] A. McAslan, "The concept of resilience: Understanding its origins, meaning and utility," *Adelaide: Torrens Resilience Institute*, vol. 1, 2010.

[27] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016.

[28] J. Holm and C. Østergaard, "Regional employment growth, shocks and regional industrial resilience: A quantitative analysis of the danish ICT sector," *Reg. Stud.*, vol. 49, 01 2013.

[29] A. Madariaga, "Mechanisms of neoliberal resilience: comparing exchange rates and industrial policy in Chile and Estonia," *Socio-Economic Review*, vol. 15, no. 3, pp. 637–660, 07 2016.

[30] M. Najarian and G. J. Lim, "Design and assessment methodology for system resilience metrics," *Risk Anal.*, vol. 39, no. 9, pp. 1885–1898, Sep. 2019.

[31] J. Rohrer, J. Sterbenz, D. Hutchison, and with significant input from the ResiliNets group., "Resilinets: Resilient and survivable networks," https://resilinets.org/, accessed: 2022-02-08.

[32] J. Rak and D. Hutchison, *Guide to Disaster-Resilient Communication Networks*. Springer, Cham, 2020.

[33] M. Borhani, M. Liyanage, A. H. Sodhro, P. Kumar, A. D. Jurcut, and A. Gurtov, "Secure and resilient communications in the industrial internet," in *Guide to Disaster-Resilient Communication Networks*. Springer, 2020, pp. 219–242.

[34] C. Kamyod, R. H. Nielsen, N. R. Prasad, and R. Prasad, "Resilience of the IMS system: The resilience effect of inter-domain communications," in *4th VITAE*, 2014, pp. 1–4.

[35] E. Cetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. Sterbenz, "Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach," *Telecommunication Systems*, pp. 1–16, 02 2013.

[36] R. Bruzgiene, L. Narbutaite, T. Adomkus, P. Pocta, P. Brida, J. Machaj, E. Leitgeb, P. Pezzei, H. Ivanov, N. Kunicina, A. Zabasta, J. Caiko, and A. Patlins, *Quality-Driven Schemes Enhancing Resilience of Wireless Networks under Weather Disruptions*. Cham: Springer International Publishing, 2020, pp. 299–326.

[37] H. Ivanov, E. Leitgeb, D. Kraus, F. Marzano, A. Jurado-Navas, S. Dorenbos, R. Perez-Jimenez, and G. Freiberger, *Free Space Optics System Reliability in the Presence of Weather-Induced Disruptions*. Cham: Springer International Publishing, 2020, pp. 327–351.

[38] T. Cinkler, A. Ladanyi, J. Rak, C. Esposito, and G. Rizzo, *Resilience of 5G Mobile Communication Systems to Massive Disruptions*. Cham: Springer International Publishing, 2020, pp. 699–719.

[39] H. Dahrouj, A. Douik, F. Rayal, T. Y. Al-Naffouri, and M.-S. Alouini, "Cost-effective hybrid RF/FSO backhaul solution for next generation wireless systems," *IEEE Wirel. Commun.*, vol. 22, no. 5, pp. 98–104, 2015.

[40] G. Arfaoui, J. M. Sanchez Vilchez, and J.-P. Wary, "Security and resilience in 5G: Current challenges and future directions," in *IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 1010–1015.

[41] M. Zhan, K. Yu, and Z. Pang, "Pulse interference resilience of convolutional codes in WirelessHP physical layer protocols: Experiment in real factory environments," in *1st IAI*, 2019, pp. 1–6.

[42] V. N. Swamy, P. Rigge, G. Ranade, B. Nikolić, and A. Sahai, "Wireless channel dynamics and robustness for ultra-reliable low-latency communications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 705–720, 2019.

[43] M. Bennis, M. Debbah, and H. V. Poor, "Ultrareliable and low-latency wireless communication: Tail, risk, and scale," *Proc. IEEE*, vol. 106, no. 10, pp. 1834–1853, 2018.

[44] S. Vestal, "Preemptive scheduling of multi-criticality systems with varying degrees of execution time assurance," in *28th IEEE RTSS*, 2007, pp. 239–243.

[45] A. Burns, J. Harbin, L. Indrusiak, I. Bate, R. Davis, and D. Griffin, "AirTight: A resilient wireless communication protocol for mixed-criticality systems," in *24th IEEE RTCSA*, 2018, pp. 65–75.

[46] J. Harbin, A. Burns, R. I. Davis, L. S. Indrusiak, I. Bate, and D. Griffin, "The AirTight protocol for mixed criticality wireless CPS," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 2, dec 2019.

[47] C. Xia, X. Jin, L. Kong, and P. Zeng, "Bounding the demand of mixed-criticality industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 7505–7516, 2017.

[48] A. Nota, S. Saidi, D. Overbeck, F. Kurtz, and C. Wietfeld, "Providing response times guarantees for mixed-criticality network slicing in 5G," in *in. Proc. DATE*, 2022, pp. 552–555.

[49] Y. Karacora and A. Sezgin, "Rate-splitting enabled multi-connectivity in mixed-criticality systems," in *IEEE ICC*, 2023, pp. 1–6.

[50] A. Burns and R. Davis, "Mixed criticality systems-a review," *Department of Computer Science, University of York, Tech. Rep*, pp. 1–69, 2013.

[51] D. Pompili, A. Hajisami, and T. X. Tran, "Elastic resource utilization framework for high capacity and energy efficiency in cloud RAN," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 26–32, 2016.

[52] R. Ernst and M. Di Natale, "Mixed criticality systems—a history of misconceptions?" *IEEE Design & Test*, vol. 33, no. 5, pp. 65–74, 2016.

[53] B. Dai and W. Yu, "Sparse beamforming and user-centric clustering for downlink cloud radio access network," *IEEE Access*, vol. 2, pp. 1326–1339, 2014.

[54] K. Shen and W. Yu, "Fractional programming for communication systems—part I: Power control and beamforming," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2616–2630, 2018.

[55] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," 2014. [Online]. Available: http://cvxr.com/cvx

[56] L. Luo, N. Chakraborty, and K. Sycara, "Distributed algorithm design for multi-robot generalized task assignment problem," in *2013 IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2013, pp. 4765–4771.

[57] P. Avella, M. Boccia, and I. Vasilyev, "A branch-and-cut algorithm for the multilevel generalized assignment problem," *IEEE Access*, vol. 1, pp. 475–479, 2013.

Robert-Jeron Reifert (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degree in Electrical Engineering and Information Technology from Ruhr University Bochum, Germany, in 2019 and 2021, respectively. He is one of the recipients of the Association for Electrical, Electronic and Information Technologies (VDE) Rhein-Ruhr graduate student award 2021. He is currently pursuing the Ph.D. degree with the Institute of Digital Communication Systems, Ruhr University Bochum, Germany. His research interests include wireless communication systems, mixed criticality, and resilience in 6G communication networks and beyond.

Stefan Roth (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degree in Electrical Engineering and Information Technology from Ruhr University Bochum, Germany, in 2016 and 2019, respectively.

Currently, he is pursuing his Ph.D. degree at the institute of digital communication systems at Ruhr University Bochum. From September 2016 to September 2017, he studied at the University of Birmingham, UK. From June to August 2019, he was a visiting student at Princeton University, NJ. His research focus includes physical layer security and communication in the internet of things (IoT).

Alaa Alameer Ahmad received his B.Sc. degree in electrical engineering from the Higher Institute of Applied Sciences and Technology (Hiast), Damascus, Syria in 2008, his M.Sc. degree in information and communication technology from TU-Darmstadt, Darmstadt, Germany, in 2015, and his Ph.D. in wireless communication from Ruhr University Bochum. He received the AKDN scholarship for the year 2011-2012. He is currently working in Cariad SE in Berlin, Germany. His research interests include optimization of wireless communication systems, signal processing in communication, and large language models applications in automotive.

Aydin Sezgin (Senior Member, IEEE) received the Dipl.Ing. (M.S.) degree in communications engineering from Technische Fachhochschule Berlin (TFH), Berlin, in 2000, and the Dr. Ing. (Ph.D.) degree in electrical engineering from TU Berlin, in 2005.

From 2001 to 2006, he was with the Heinrich-Hertz-Institut, Berlin. From 2006 to 2008, he held a postdoctoral position, and was also a lecturer with the Information Systems Laboratory, Department of Electrical Engineering, Stanford University, Stanford, CA, USA. From 2008 to 2009, he held a postdoctoral position with the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA. From 2009 to 2011, he was the Head of the Emmy-Noether- Research Group on Wireless Networks, Ulm University. In 2011, he joined TU Darmstadt, Germany, as a professor. He is currently a professor of information systems and sciences with the Department of Electrical Engineering and Information Technology, Ruhr University Bochum, Germany.

He is interested in signal processing, communication, and information theory, with a focus on wireless networks. He has published several book chapters more than 65 journals and 200 conference papers in these topics. He has coauthored a book on multi-way communications. Aydin is a winner of the ITG-Sponsorship Award, in 2006. He was the first recipient of the prestigious Emmy-Noether Grant by the German Research Foundation in communication engineering, in 2009. He has coauthored papers that received the Best Poster Award at the IEEE Communication Theory Workshop, in 2011, the Best Paper Award at ICCSPA, in 2015, and the Best Paper Award at ICC, in 2019. He has served as an Associate Editor for the IEEE Transactions on Wireless Communications (2009-2014), and as an area editor for the Elsevier Journal of Electronics and Communications (2010-2011). He was also the General Co-chair of the 2018 International ITG Workshop on Smart Antennas, the program co-chair of the 2019 Crowncom Conference, and the workshop co-chair of the 2022 WCNC workshop on rate-splitting and next generation multiple access.