Packet Level Resilience for the User Plane in 5G Networks

Fabian Ihle*, Tobias Meuser†, Michael Menth*, Björn Scheuermann†
*University of Tübingen, Chair of Communication Networks
†Communication Networks Lab, Technical University of Darmstadt, Germany
Email: {*fabian.ihle, menth*}@uni-tuebingen.de, {*tobias.meuser, bjoern.scheuermann*}@kom.tu-darmstadt.de

***Abstract*—The growing demands of ultra-reliable and low-latency communication (URLLC) in 5G networks necessitate enhanced resilience mechanisms to address user plane failures caused by outages, hardware defects, or software bugs. An important aspect for achieving ultra-reliable communication is the redundant transmission of packets, as also highlighted in 3GPP Release 18. This paper explores leveraging the Packet Replication, Elimination, and Ordering Function (PREOF) to achieve 1+1 path protection within private 5G environments. By extending existing 5G components with mechanisms for packet level redundancy and offloading the reordering mechanism to external servers, the proposed approach ensures minimal packet loss in case of a failure. A conceptual integration of redundant paths and programmable elements is presented, with considerations for deployment in existing 5G infrastructures and the trade-offs of latency versus enhanced traffic engineering. Future work aims to evaluate practical implementations using an open source 5G core, P4-based hardware and offloading technologies like DPDK and eBPF.**

***Index Terms*—5G, 6G, Data Plane Programming, Resilience, PREOF**

I. Introduction

In the past years, new applications emerged such as smart factories with industrial machine-to-machine communication, and 5G network slicing with Ultra-Reliable and Low Latency Communication (URLLC) for self-driving vehicles, remote surgery, or drone control. Those applications require extremely low packet loss and bounded latency [1]. One possible technology to provide connectivity to such applications in a private environment are 5G and beyond networks. In this paper, we focus on the reliability aspect of URLLC in private networks, i.e., reducing packet loss in 5G and beyond communication.

In a 5G network, traffic is forwarded from the User Equipment (UE), through the user plane in the Radio Access Network (RAN) to the data network. However, a failure in the user plane is detrimental to connectivity. Connectivity in the user plane may fail due to power outages, fiber cuts, hardware defects, or software bugs. Redundant links are therefore a common approach to ensure the connectivity even during failures. Mechanisms such as Fast ReRoute (FRR) provide a failover mechanism reacting on a sub-millisecond scale [2]. However, for mission-critical applications, an even smaller restoration time is required. In 3GPP release 18 [3], packet duplication and elimination has been described as possible approach to achieve ultra-high reliability. Therefore, this work suggests a design for packet duplication and elimination in the context of 5G and beyond that leverages the Packet Replication, Elimination, and Ordering Function (PREOF) mechanism introduced in the IETF DetNet working group to protect the user plane of 5G networks with a 1+1 protection scheme. PREOF provides redundant data paths by replicating traffic, sending it over multiple disjoint paths, and eliminating duplicates at the tail end [4], [5].

The authors acknowledge the funding by the Deutsche Forschungsgemeinschaft (DFG) under grant ME2727/3-1, by the Federal Ministry of Education and Research of Germany in the project Open6GHub (grant number: 16KISK014), and the LOEWE initiative (Hessen, Germany) within the emergenCITY center. The authors alone are responsible for the content of the paper.

II. Background

In this section, we provide technical background on components in the 5G architecture and the Packet Replication, Elimination, and Ordering Function (PREOF).

A. Components in the 5G Architecture

Similar to previous generations of cellular networks, 5G-based networks consist of a UE, the gNodeB (gNB) inside the RAN, and the core network. The core network is subdivided into two parts: the control plane and the user plane. While the control plane is responsible for functions related to network access and management, the user plane forwards packets from authenticated UEs to the data network, commonly the Internet. Once a packet from the UE is received by the gNB, it encapsulates it in a GPRS Tunneling Protocol – User (GTP-U) tunnel and forwards it via a fiber connection to the user plane function (UPF). The UPF is the network function responsible for forwarding user packets to the data network and can be implemented both in hardware and in software [6].

The UE is anchored to a specific UPF, leading to a disconnection if the UPF fails, even if the gNB remains functional. Only after the connection is reset, the UE can reconnect to a new UPF and continue communication. While UPFs may be redundant, the UE must explicitly trigger the reconnection to a different UPF on a failure. Furthermore, the reconnection process to a different UPF with an active failover mechanism causes a short disruption in communication leading to a small packet loss [7].

B. The Packet Replication, Elimination, and Ordering Function (PREOF)

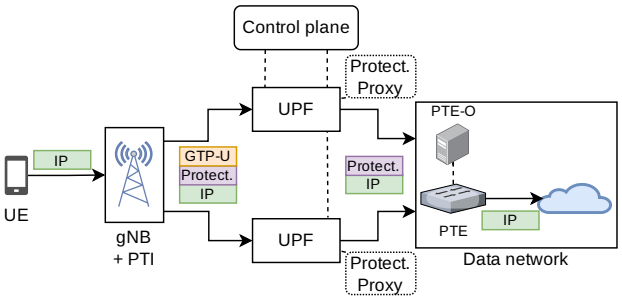
The DetNet working group aims to provide mechanisms that enable real-time applications with extremely low data loss, e.g., in IP/UDP networks [4]. For that purpose, the DetNet working group defined a resilience mechanism called Packet Replication, Elimination, and Ordering Function (PREOF) which features a 1+1 protection scheme. The replication function of PREOF replicates packets and tunnels them over disjoint links towards the elimination function. To that end, the replication function encapsulates packets with sequence numbers and tunnel destination information. The elimination function eliminates duplicate packets based on the sequence number and forwards them to their destinations. Furthermore, the ordering function located at the elimination endpoint ensures that forwarded packets are delivered in-order, which requires a packet buffer and adds significant complexity.

A P4-based implementation of the packet replication and elimination functionalities is provided in [8] on an Intel Tofino™ with a forwarding speed of 100 Gb/s. However, the authors emphasize that the objective of their protection mechanism is to protect quickly against path failures and does not compensate for individual packet loss. Further, the implementation does not provide the ordering function because of limited arithmetic operations and storage access on their hardware target. To include the compensation for individual packet loss and the ordering function into their approach, a packet buffer is required which is typically not available in P4 switches. Traffic can be offloaded to an external server that buffers packets and performs the mechanisms. For offloading, techniques such as eBPF [9] or the kernel-bypass Snabb [10] can be used.

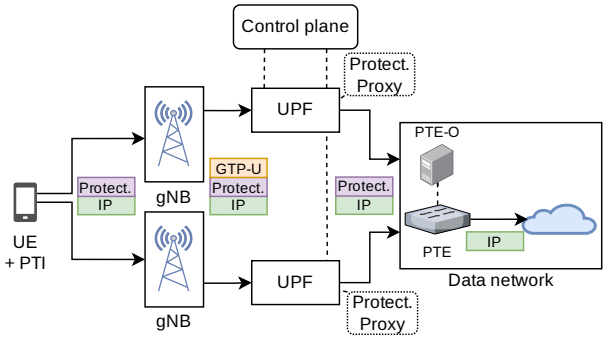
III. Concept

In this section, we propose a concept of the proposed resilience mechanism leveraging the PREOF mechanism in a 5G networking environment. In Figure 1, we describe two approaches: providing packet level redundancy for the UE with redundant UPFs, and with redundant UPFs and gNBs.

In both approaches in Figure 1, UEs, i.e., mobile phones, send their traffic via a wireless link to a gNB station in the RAN. A Protection Tunnel Ingress (PTI) node performs the replication and encapsulation mechanism of PREOF. To that end, the PTI node adds a protection header to the packet that contains sequence number information and addresses the Protection Tunnel Egress (PTE) node. The packets are then replicated by the PTI and are sent over multiple disjoint paths towards the PTE node. The gNB station encapsulates traffic with a GTP-U header that addresses the corresponding UPF according to the 5G standard. On all disjoint paths, redundant UPFs with synchronized session states are deployed. The UPF removes the GTP-U header and forwards the packets towards the PTE node based on the address information in the protection header. At the PTE node, duplicate packets are eliminated and traffic is forwarded into the data network.



(a) PTI included in gNB.



(b) PTI included in UE.

Fig. 1. Overview of a 5G core network incorporating redundant data paths and UPFs using the PREOF mechanism.

Further, the PTE node performs offloading for the ordering function of PREOF to an external server, the PTE-O.

The first approach in Figure 1(a) incorporates a PTI node in the gNB station, which performs the replication and encapsulation mechanism of PREOF. Packets are replicated at a single gNB station and are sent over multiple disjoint paths and UPFs.

The second approach in Figure 1(b) includes the PTI in the UE. Here, the UE performs the protection header encapsulation. Further, the UE sends the encapsulated traffic to multiple gNB via multiple wireless links.

For simplicity, only the uplink direction is shown in Figure 1. The PREOF mechanism is applied in both directions, i.e., from the gNB station / the UE to the data network and from the data network to the gNB station / the UE. In the downlink direction, an edge node of the data network encapsulates packets with the protection header and addresses the PTE, i.e., the gNB in Figure 1(a), or the UE in Figure 1(b). Further, the UPF adds the GTP-U header which addresses the gNB station.

Typically, the UPF terminates the GTP-U tunnel and forwards packets based on the underlying Layer 3 information. However, in large 5G domains, the UPF may apply additional traffic engineering mechanisms, such as prioritization with QoS. This traffic engineering is applied based on the IP header received from the UE. With the proposed protection mechanism, this poses a challenge as the UE IP header is not

directly accessible by the UPF because it is encapsulated by the protection header. To allow this packet inspection of the UPF with PREOF, we propose to employ a protection proxy in this case, e.g., using eBPF. A similar approach using eBPF for an SFC proxy is described in [11].

IV. Discussion

In this section, we discuss the tradeoffs between the two proposed approaches for path redundancy in Section III. Further, we discuss the implications of employing a proxy for traffic engineering in the UPF, and offloading the ordering function to an external server at the PTE node.

In the first approach, including the PTI node in the gNB protects the communication in case of a UPF failure while being transparent to the UE. For this purpose, the gNB can either be modified to include the packet replication functionality, or the PTI can be a co-located node. In this case, the replication is applied after the gNB has encapsulated the packet with the GTP-U header. The former may require changes in the standardization of 5G while the latter does not. However, including the PTI node in the gNB does not protect in case of a gNB station failure. Therefore, in the second approach, the PTI is included in the UE. Including the PTI in the UE does not require changes to the 5G standards as the packet replication can be handled at the UE operating system level. While the second approach protects more points of failure in the 5G network, it also puts more load on the UE compared to the first approach. The gNB station typically contains more powerful network components compared to the UE for which a packet replication and encapsulation function is more feasible. Performing such an operation in the UE is energy-intensive. Further, it multiplies the traffic on the wireless link which is not cost-efficient. Therefore, the second approach, while being more resilient, is more expensive and should only be used for selected applications where URLLC is the highest priority. For both approaches, the PTE, i.e., the elimination functionality, is standardized in RFC 9566 [4]. The UPF does not require any modifications and forwards traffic based on the IP header.

The proposed protection proxy enables traffic engineering mechanisms in the UPF. While the UPF could also be modified to ignore PREOF headers, thereby eliminating the proxy, such a modification would complicate the deployment of PREOF in existing 5G networks. In contrast, using a proxy increases the latency on the path and adds another point of failure that should be well considered in a URLLC environment. Therefore, the proxy is considered optional in the proposed mechanism.

In addition, we have proposed to offload the ordering function to an external server, as the reordering mechanism is beyond the capabilities of programmable switches such as the Intel Tofino™. However, this also increases the latency and possibly limits the available bandwidth while not being required by every application. Hence, this mechanism is also considered optional.

V. Conclusion

In this work, we proposed to leverage the PREOF mechanism introduced in the IETF DetNet working group to achieve packet level redundancy for components in a 5G environment. For that purpose, existing 5G networking equipment is extended with a packet replication and elimination function. Further, a packet ordering function is offloaded to an entity in the network to achieve in-order delivery of recombinated packets. We proposed two approaches: one that includes the packet replication function in the gNB station and one that includes it in the UE. To enable traffic engineering capabilities in the user plane, we propose to employ an optional proxy in the UPF. We discussed the tradeoffs of the two proposed approaches, and the implications of the optional proxy and the offloaded ordering function. In the future, we want to provide an implementation leveraging P4-based hardware switches and offloading technologies such as DPDK and eBPF to further evaluate the implications of the proposed concept. For the implementation, we consider an open-source 5G core network, e.g., free5GC, coupled with a RAN emulator such as UERANSIM or a physical RAN.

References

[1] E. Grossman, "Deterministic Networking Use Cases." RFC 8578, May 2019.

[2] D. Merling, S. Lindner, and M. Menth, "Robust LFA Protection for Software-Defined Networks (RoLPS)," *IEEE Transactions on Network and Service Management*, vol. 18, pp. 2570–2586, Sept. 2021.

[3] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 18 Description; Summary of Rel-18 Work Items (Release 18)," Tech. Rep. TR 21.918 V2.0.0 (2025-01), 3GPP, 2025.

[4] B. Varga, J. Farkas, and A. G. Malis, "Deterministic Networking (DetNet) Packet Replication, Elimination, and Ordering Functions (PREOF) via MPLS over UDP/IP." RFC 9566, Apr. 2024.

[5] N. Finn, P. Thubert, B. Varga, and J. Farkas, "Deterministic Networking Architecture." RFC 8655, Oct. 2019.

[6] R. Kundel, T. Meuser, T. Koppe, R. Hark, and R. Steinmetz, "User Plane Hardware Acceleration in Access Networks: Experiences in Offloading Network Functions in Real 5G Deployments," in *Hawaii International Conference on System Sciences. Computer Society Press*, pp. 1–10, 2022.

[7] L. Wernet, L.-M. Spang, F. Siegmund, and T. Meuser, "Resilient User Plane Traffic Redirection in Cellular Networks," in *IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 1–6, 2024.

[8] S. Lindner, D. Merling, M. Häberle, and M. Menth, "P4-Protect: 1+1 Path Protection for P4," in *P4 Workshop*, pp. 21–27, 2020.

[9] T. Høiland-Jørgensen, J. D. Brouer, D. Borkmann, J. Fastabend, T. Herbert, D. Ahern, and D. Miller, "The eXpress data path: fast programmable packet processing in the operating system kernel," in *ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, pp. 54–66, Dec. 2018.

[10] M. Paolino, N. Nikolaev, J. Fanguede, and D. Raho, "SnabbSwitch User Space Virtual Switch Benchmark and Performance Optimization for NFV," in *Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, pp. 86–92, 11 2015.

[11] M. Haeberle, B. Steinert, M. Weiss, and M. Menth, "A Caching SFC Proxy Based on eBPF," in *International Conference on Network Softwarization (NetSoft)*, pp. 171–179, 2022.