FRANCO-GERMAN ECOSYSTEM
FOR PRIVATE 5G NETWORKS

5G-RACOM

Franco-German Innovation Project on 5G for Resilient and Green Rail Communications

Work Package 3: Hybrid FRMCS Networks

D3.1 Report on Assessment and Implementation of Multipath Technologies for Hybrid FRMCS Networks

Final Report *(public)*

June 2025

Version History

Version	Date	Description	Reviewers/Contributors
V1.0.0	2025-06-11	Released document	DB InfraGO, Funkwerk, Kontron DE, TU Chemnitz, TU Ilmenau

Authors

Name	Affiliation	Role
Richard Fritzsche	DB InfraGO	Contributor
Bernd Holfeld	DB InfraGO	Reviewer
Shirish Kendre	DB InfraGO	Reviewer
Tomas Karabinos	DB InfraGO	Project Manager WP3
Arne Weber	DB InfraGO	Reviewer
Zubair Shaik	TU Ilmenau	Contributor
Daniil Chirkov	TU Ilmenau	Contributor
Ricardo Quiceno	TU Ilmenau	Contributor
Manfred Taferner	Kontron DE	Contributor
Peter Beicht	Kontron DE	Contributor
Jens Koecher	Funkwerk	Contributor
Bastian Reukauf	Funkwerk	Contributor
Alexander Ende	Funkwerk	Reviewer
Niclas Schreiber	Funkwerk	Reviewer
Klaus Moessner	TU Chemnitz	Reviewer
Pedram Delavari	TU Chemnitz	Reviewer

Contents

Executive Summary

The 5G-RACOM project is a Franco-German initiative focused on deploying resilient and sustainable rail communications using 5G technologies, specifically for hybrid Future Railway Mobile Communication System (FRMCS) environments. Within Work Package 3 (WP3), this report describes the process applied to identify, assess and evaluate candidate multipath technologies to improve reliability, performance, and continuity in critical rail applications.

The project defines a set of use cases that are relevant for the operational needs of the rail applications:

1. Application-specific data path selection
2. Resilience via fallback
3. Resilience via best data path selection
4. Resilience via packets replication
5. Coverage complement
6. Capacity complement

Based on these use cases, a comprehensive set of functional requirements was derived, covering aspects such as general requirements, data flow specific path management, path management capabilities and architectural requirements.

A two-phase assessment framework was established:

- Phase 1 included theoretical and comparative evaluation of multipath technologies against standardized and practical criteria. Mostly pen & paper studies accompanied work with basic lab activities in later stages of the phase.
- Phase 2 involves implementation and field testing to observe fulfilling functional requirements and to measure performance and resilience under realistic operating conditions.

From a broad pool of assessed candidate multipath technologies, including MP-TCP, MP-QUIC, MAMS, ATSSS, SCTP, SD-WAN, and others, the project has selected two primary multipath transport protocols for implementation, validation and demonstration:

1. Multipath TCP (MP-TCP) – a reliable extension of TCP, suited for connection-oriented, reliable applications (file transfers, streaming over TCP, transactional apps)
2. Multipath QUIC (MP-QUIC) – a more flexible, UDP-based solution designed for low-latency and encrypted communication scenarios, supporting both reliable and unreliable applications

These selections align with project goals to verify envisioned benefits of hybrid FRMCS networks with multipath technologies for rail applications.

1 Introduction

This document presents the D3.1 report produced under WP3 of the 5G-RACOM project, which addresses the assessment, selection, and implementation of multipath technologies for hybrid FRMCS networks with multipath technology.

The purpose of the document is to:

- Analyse architectural options and traffic characteristics for rail-specific data flows
- Define relevant multipath use cases and derive associated technical requirements
- Establish an evaluation framework to benchmark candidate technologies
- Guide the selection and deployment of suitable multipath solutions within FRMCS

The report integrates input from prior work packages, notably WP1 (use case analysis), and extends it with technical evaluations, structured requirement modelling, and field-test planning.

Key components of the document include:

- A review of multipath use cases reflecting operational and technical needs
- A classification of functional, architectural, and performance requirements
- A comparative assessment of candidate multipath technologies
- Selection of the most suitable multipath technology for implementation

This report will serve as a foundation for the demonstration, integration, and further development of multipath communications within FRMCS networks and contributes to shaping future standards.

2 Architecture and Traffic Characteristics

The 5G-RACOM WP1 report on use cases, requirements and assumptions [1] has listed and described relevant use cases for multipath in hybrid FRMCS networks. This chapter briefly elaborates on the established high-level architecture and on traffic characteristics with its basic QoS requirements [1]. The network of the Mobile Network Operator (MNO) may support 4G, 5G and in the future potentially 6G, hence it is denoted as xG.

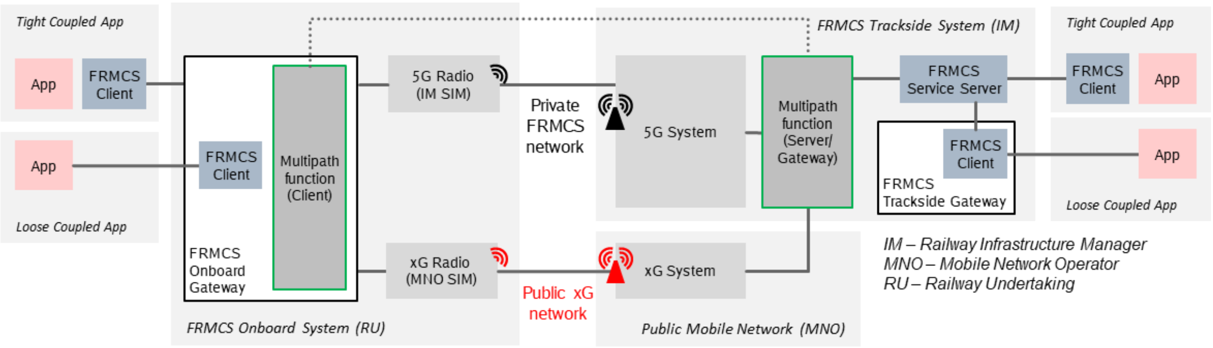

Figure 1: High-level FRMCS architecture including the multipath function

The figure above shows the high-level hybrid FRMCS architecture including the multipath function (MPF) with a client/server architecture. The architecture includes the MPF server in the FRMCS trackside system residing between transport and service stratum [1] and the MPF client as part of the FRMCS onboard gateway enabling the use of multiple wireless transmission Data Paths between train and network infrastructure. The MPF client can be also used at the FRMCS trackside gateway to enable redundant connection (e.g. wireless connection in addition to wired connection) of trackside applications (e.g. a dispatcher terminal, an RBC in ETCS or ATO-TS). Note that for transferring information related to negotiation and management of the use of multiple Data Paths between the MPF client and the MPF server the FS_MPM interface has been defined in [2], however detailed specification is so far not available. Any number of UEs (i.e. 5G/xG Radio) may be used in principle, depending on FRMCS onboard gateway implementation.

Note that for simplicity, the following chapters are describing the use cases primarily from the perspective of the MPF client at the onboard gateway as it is considered that the FRMCS architecture inherently supports MPF clients independent of the location (onboard or trackside).

Within the WP1 report [1], Quality of Service (QoS) requirements per application are listed and Table 1 below further elaborates them. In order to capture all traffic characteristics that need to be identified by the MPF, Table 1 lists the relevant Data Flows referring to dedicated application exchange or FRMCS service stratum signalling. The Data Flow is assumed to refer to IP packets carrying a Layer 4 (L4) session (i.e. TCP/UDP). The Table 1 is listing the expected Layer 4 protocol(s) as well as indications on the retransmission timeout (RTO) for TCP (in case TCP is used). In this project the considered Data Flows cover TCP/UDP traffic, while the MPF aims towards a solution agnostic of the L4 protocol i.e. other L4 protocols should be possible as well.

A routing decision in the MPF is assumed to take place for each Data Flow, identified, e.g. via 5-tuple (source IP, destination IP, source port, destination port, L4 protocol).

Data Flow	Transmission Type	Direction	E2E Packet Latency	E2E Packet Reliability	L4 Protocol	TCP Retransmission Timeout (RTO)
FRMCS Service Stratum Signalling	MCX over HTTP/SIP Messages	UL+DL	100 – 500 ms	99.9 %	TCP assumed	1 s

Voice	Audio Stream/RTP	UL+DL	100 – 500 ms	99 %	UDP	n/a
ETCS	Messages (Position Report)	UL	100 – 500 ms	99.9 %	TCP	1 – 5 s
	Messages (Movement Authority)	DL	100 – 500 ms	99.9 %	TCP	1 – 5 s
ATO	Messages (Journey Profile)	DL	100 – 500 ms	99.9 %	TCP	1 – 5 s
	Messages (Segment Profile)	DL	100 – 500 ms	99.9 %	TCP	1 – 5 s
	Messages (Status Report)	UL	100 – 500 ms	99.9 %	TCP	1 – 5 s
TCMS	Messages	UL+DL	500 ms	best effort	TCP	1 – 5 s
Video Based Remote Operation	Video/Audio Stream for Remote Driving	UL	100 – 200 ms	99 %	UDP	n/a
	Control Data for Remote Driving	DL	50 – 100 ms	99 %	TCP assumed	n/a
	Video/Audio Stream for Remote Supervision	UL	100 – 200 ms	99 %	UDP	n/a
	Control Data for Remote Supervision	DL	100 – 200 ms	99 %	TCP assumed	n/a

Table 1: Traffic categories and their characteristics to be considered for multipath

3 Use Cases and Policies

The following descriptions of the use cases include the general behaviour w.r.t. Data Flow routing, key associated requirements and example of Multipath Policies.

Triggers, thresholds and criteria for indicating availability and quality of the Data Paths and Data Flows are implementation specific are not part of this document.

Note: Information provided in this chapter shall be taken into account in conjunction with UIC's document "FRMCS Multipath use cases" [3].

3.1 UC01: Application-Specific Data Path Selection (Prio 1)

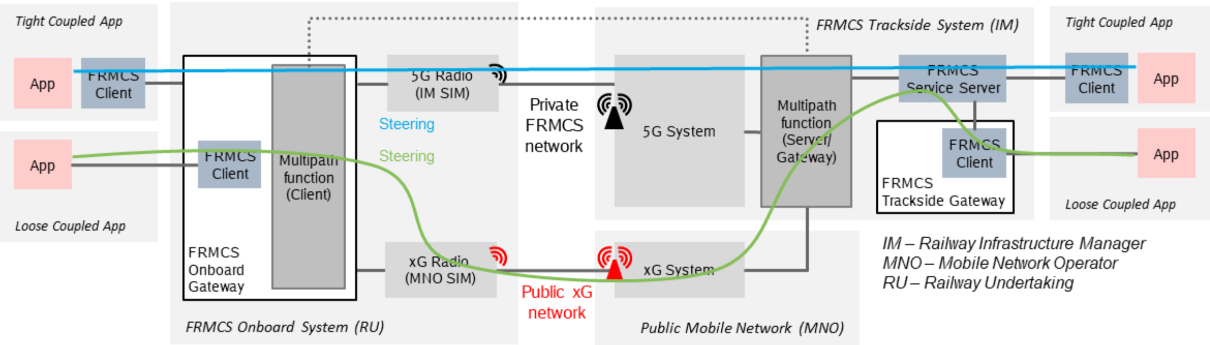

Figure 2: Traffic flow for application-specific Data Path selection

3.1.1 Description

In this use case, each Data Flow is assigned by the Multipath Policy to a Data Path for routing the corresponding traffic. The Data Flow will use this default Data Path for the lifetime of communication as long as it is available and meets criteria defined by the Multipath Policy. Routing decision shall be taken in the MPF client based on the Multipath Policy provided by the infrastructure manager (IM) to the MPF server which in turn provides it via designated interface (e.g. FSmpm) to the MPF client. Both client and server MPFs need to be able to identify the Data Flow (e.g. a voice stream), e.g. via 5-tuple and the Data Path to select i.e. to route the traffic.

3.1.2 Requirement Indications

- Possibility to identify the Type of Data Flow (e.g. voice stream, ETCS data traffic, FRMCS signalling) via 5-tuple or its part
- Knowledge of Data Paths availability
- Availability of Multipath Policy that maps the Type of Data Flow to a Data Path
- Capabilities for routing the Data Flow via the Data Path defined in the Multipath Policy
- Abilities to pre-empt lower priority Data Flow in favour of higher priority Data Flow and to drop/halt the Data Flow in case of insufficient resources, note that higher protocol layers shall be informed accordingly to take appropriate action

3.1.3 Example Multipath Policy

If **data flow type** == "Voice" (same for "FRMCS signalling", "ETCS", "ATO" or "Remote Driving"):

Then **selected path** (data flow type) = private FRMCS network;

Else if **data flow type** == "TCMS" (same for "Remote Supervision"):

Then **selected path** (data flow type) = public xG network;

3.2 UC02: Resilience via Fallback (Prio 1)

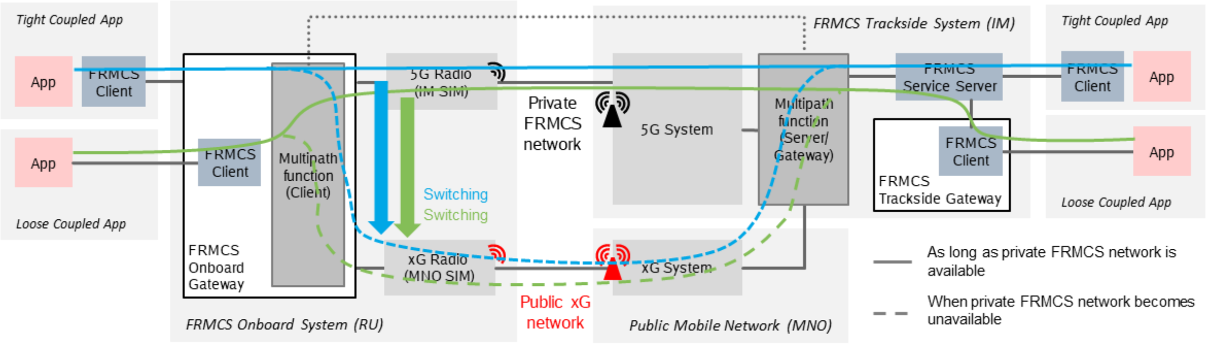

Figure 3: Traffic flow for resilience via fallback

3.2.1 Description

In this use case, the currently used default Data Path through which the Data Flow is routed becomes unavailable and therefore the Data Flow is switched (fallback) to an alternative Data Path. The switching shall only happen if the alternative Data Path is available. During the switching, the L4 session of the Data Flow should be kept established, while temporary performance degradations due to the switching might be acceptable (the QoS requirements defined in chapter 2 should be fulfilled). The Multipath Policy, which is provided by the IM to the MPF server, should define the alternative Data Paths that the Data Flow can be switched to. This policy should be then propagated to the MPF client. As soon as the default Data Path becomes available (i.e. meets the availability criteria) again, the Data Flow should be switched back employing “make-before-break” principle.

3.2.2 Resulting Requirements

- Requirements of UC01
- Periodic/aperiodic (event-based) measurements and indication of instantaneous Data Path availability and its quality (incl. hysteresis/threshold to prevent ping-pong)
- Multipath Policy that indicate the default and alternative Data Path for each Type of Data Flow incl. definitions which applications are subject to fallback and related switching criteria
- Capability of re-routing (switching) Data Flows based on instantaneous Data Path availability and quality employing “make-before-break” principle

3.2.3 Example Multipath Policy

```
If data flow type == “Voice”” (same for “ETCS”, “ATO” or “Remote Driving”):
    If availability (private FRMCS network) == true:
            Then selected path (data flow type) = private FRMCS network;
    Else if availability (public xG network) == true
            Then selected path (data flow type) = public xG network;
    Else error (“Voice”, “noNetworkAvailable”)
Else if data flow type == “TCMS” (same for “Remote Supervision”):
    If availability (public xG network) == true
            Then selected path (data flow type) = public xG network;
    Else error (“TCMS”, “noNetworkAvailable”)
```

3.3 UC03: Resilience via Best Data Path Selection (Prio 2)

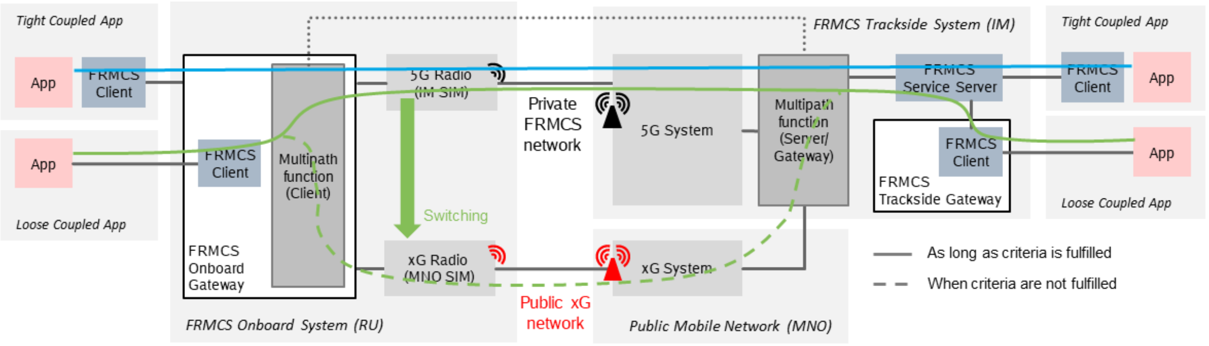

Figure 4: Traffic flow for resilience via best Data Path selection

3.3.1 Description

In this use case, the currently used default Data Path through which the Data Flow is routed is switched to an alternative Data Path with better measured quality. The switching shall only happen if the alternative Data Path meets the criteria defined in the Multipath Policy. Those criteria can be defined per Data Flow and focuses primarily on the fulfilment of QoS requirements, i.e. the Data Flow is switched from the default Data Path to an alternative Data Path as soon as the measured quality (e.g. latency, data rate) of the former one is not fulfilling the QoS requirements of the Data Flow. It shall be possible to indicate a priority (in terms of an order) of Data Flows that shall be switched to the alternative Data Path (switching by priority). It shall further be possible to decide that a Data Flow is not switched to an alternative Data Path, e.g. due to the occupation/load of the alternative Data Path. This should ensure successful transmission of other critical data via an alternative Data Path, which itself may not be Multipath Policy controlled or configurable w.r.t. priority and QoS by the FRMCS trackside system of the IM (e.g. if the FRMCS has no N33/N5/Rx interface to the public network).

3.3.2 Resulting Requirements

- Requirements of UC02
- Measurements of the instantaneous Data Path and Data Flow quality (e.g. latency, data rate, reliability) available at the MPF
- Information on QoS requirements (e.g. latency, data rate, reliability) for each Type of Data Flow available at the MPF
- Multipath Policy that indicate switching criteria, e.g. QoS requirements, measured quality
- Multipath Policy that define switching priorities for Data Flows
- Capability of re-routing (switching) Data Flows based on instantaneous Data Path or Data Flow quality measurements employing “make-before-break” principle

3.3.3 Example Multipath Policy

The example Multipath Policy is assuming a defined parameter for “QoS_threshold” for each application. This parameter is based on the QoS requirement per Type of Data Flow as indicated in Table 1. For simplicity, multiple QoS parameters (latency, reliability, data rate) are summarized here. Note that QoS_threshold does not need to be equivalent with the QoS requirement but could also include, e.g. buffers to smoothen policies enforced by the MPF.

```
If data flow type == “Voice” (same for “ETCS”, “ATO” or “Remote Driving”):”):
    If availability (private FRMCS network) == true:
        If QoS (privateFRMCS_radio1) >= QoS_threshold (“Voice”)
```

```
                Then selected path (data flow type) = privateFRMCS_radio1;
        Else if QoS (privateFRMCS_radio2) >= QoS_threshold (“Voice”)
                Then selected path (data flow type) = privateFRMCS_radio2;
        Else if availability (public xG network) == true
                If QoS (public xG network) >= QoS_threshold (“Voice”)
                        selected path == public xG network;
```

3.4 UC04: Resilience via Packets Replication (Prio 3)

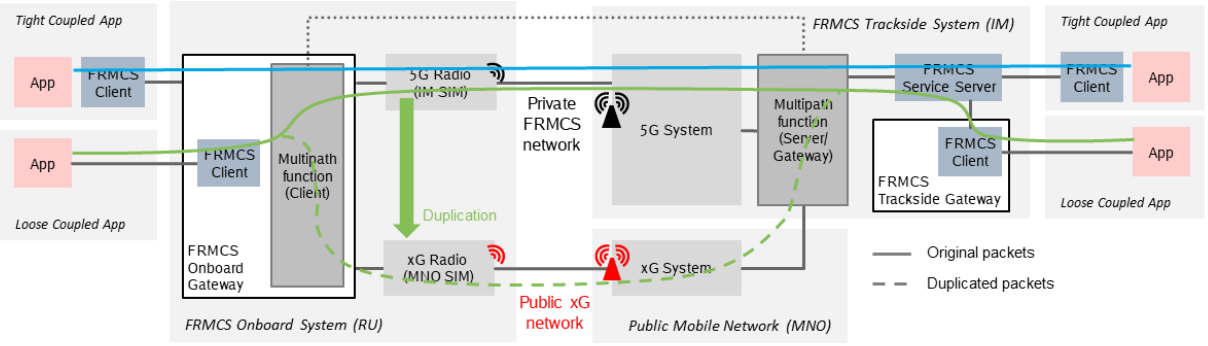

Figure 5: Traffic flow for resilience via packet replication

3.4.1 Description

In this use case, the IP packets of a Data Flow are replicated (duplicated or multiplicated) at the sending MPF and transmitted via additional Data Paths based on criteria defined in the Multipath Policy. The receiving MPF shall sort the received IP packets in the original order and remove duplicates. Criteria for applying replication can include non-fulfilled requirements on reliability, i.e. the packet loss rate is above an acceptable threshold. It’s also possible that for some applications the packets are replicated by default while for other ones replication is not allowed at all.

3.4.2 Resulting Requirements

- Requirements of UC03
- Capability of IP packet replication at the MPF
- Capability of ordering received IP packets, detecting and removing duplicated IP packets at the receiving MPF
- Multipath Policies indicating criteria for enabling packet replication for a specific Data Flow
- Capability of routing replicated IP packets via additional Data Paths

3.4.3 Example Multipath Policy

```
If data flow type == “ETCS”
    If availability (private FRMCS network) == true
        If QoS (private FRMCS network) >= QoS_threshold (“ETCS”)
            Then selected path (data flow type) = private FRMCS network;
        Else if availability (public xG network) ==true
            Then selected path (data flow type) = duplication (private FRMCS network,
            public xG network)
```

3.5 UC05: Coverage Complement (Prio 3)

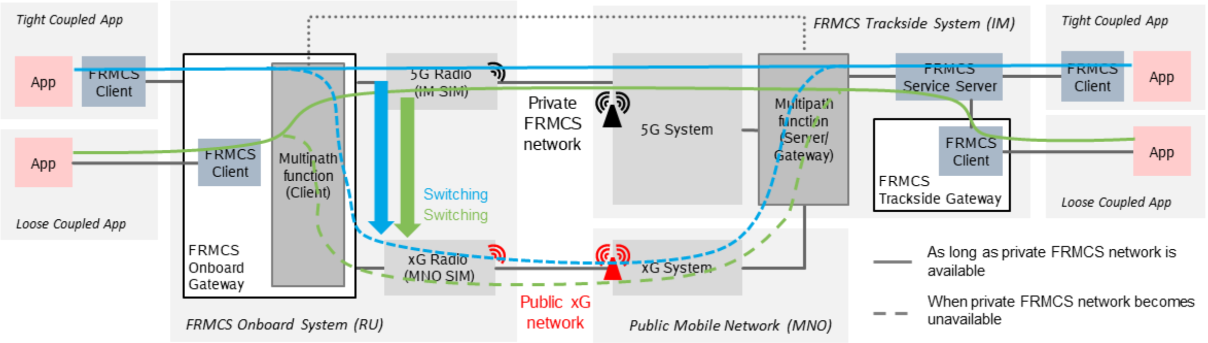

Figure 6: Traffic flow for coverage complement

3.5.1 Description

This use case is quite similar to UC02 “resilience via fallback”, as the used default Data Path (e.g. private FRMCS network) through which the Data Flow is routed becomes unavailable (end of coverage) and therefore the Data Flow is switched (fallback) to an alternative Data Path (e.g. public xG network) if available. The optional extension to UC02 is that the end of the coverage area could be potentially predicted with some probability (e.g. based on inputs from radio planning or measurements) and together with the train position can be taken into account by the MPF for a timely (and potentially more fluent) switching (e.g. smaller interruption times) between the Data Paths (networks).

3.5.2 Resulting Requirements

- Requirements of UC02
- Information on location of coverage end/coverage start (coverage map)
- Instantaneous positioning information of the train (w.r.t. the radio)
- Trigger for switching based on coverage map and train position

3.5.3 Example Multipath Policy

```
If data flow type == “Voice” (same for “ETCS”, “ATO” or “Remote Driving”):
    If availability (private FRMCS network) == true:
            Then selected path (data flow type) = private FRMCS network;
    Else if availability (public xG network) == true
            Then selected path (data flow type) = public xG network;
    Else error (“Voice”, “noNetworkAvailable”)
```

3.6 UC06: Capacity Complement (Prio 3)

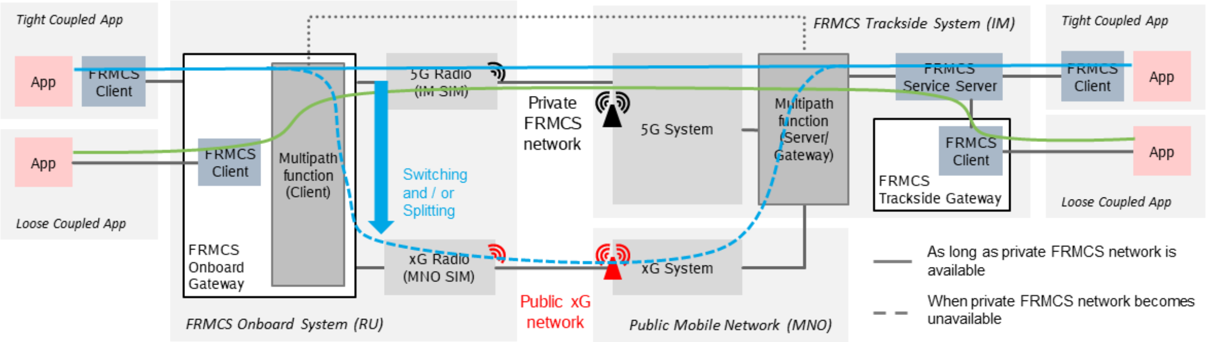

Figure 7: Traffic flow for capacity complement

3.6.1 Description

The objective of this use case is to extend the capacity by serving more (diverse) Data Flows and/or by improving the transmission of a specific Data Flow (e.g. with respect to data rate). This use case is similar to "UC03: Resilience via Best Data Path Selection" that uses switching capability but is extended with the traffic splitting capability.

The traffic of a Data Flow can be offloaded, i.e. switched to an alternative Data Path as soon as the required data rate of the Data Flow cannot be fulfilled with the default Data Path. In addition to the MPF capability of switching the complete Data Flow, this use case also includes the possibility of splitting the Data Flow traffic (on IP packet level) at the sending MPF into subflows and route them via multiple Data Paths in parallel as defined by the Multipath Policy (e.g. sending a junk of subsequent IP packets via the preferred path and the next junk via the alternative path). The receiving MPF should reorder respective IP packets to restore the original Data Flow. This would in allow to aggregate capacity and also to load-balance traffic using two distincct Data Paths.

3.6.2 Resulting Requirements

- Requirements of UC03
- Indication of splitting options via Multipath Policy (e.g. eligible Data Flows for splitting, allowed Data Paths, splitting weights per Data Path)
- Capability to split Data Flow traffic at the sending MPF
- Capability to reorder received IP packets and restore original Data Flow at the receiving MPF
- Capability to route subflows via multiple Data Paths in parallel

3.6.3 Example Multipath Policy

```
If data flow type == "Voice" (same for "ETCS", "ATO" or "Remote Driving"):
    If availability (private FRMCS network) == true:
            Then selected path (data flow type) = private FRMCS network;
            If QoS (data flow type) <= QoS_threshold (data flow type) && (availability (public xG
            network) == true;
                    Then selected path (data flow type) = [private FRMCS network, public xG
                    network];
    Else if availability (public xG network) == true
            Then selected path (data flow type) = public xG network;
    Else error ("Voice", "noNetworkAvailable")
```

3.7 UC07: Network Transition

Note: It has been decided within the 5G-RACOM project consortium that routing capabilities referring to network transitions are not further followed and detailed in the project, as the architecture and functional requirements are quite different compared to the other use cases. Description remains present due to completeness of provided information considering [3].

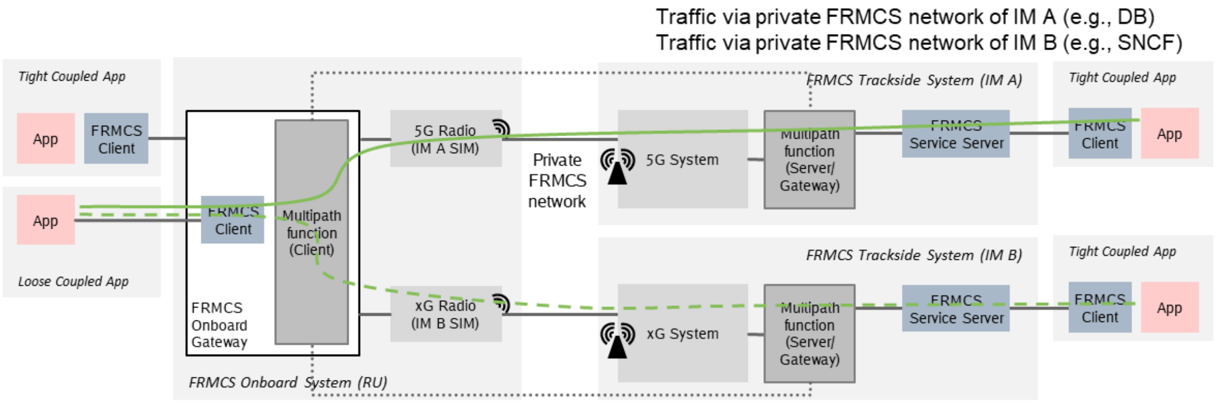
Traffic via private FRMCS network of IM A (e.g., DB)
Traffic via private FRMCS network of IM B (e.g., SNCF)
Tight Coupled App
App
FRMCS Client
App
FRMCS Client
Loose Coupled App
Multipath function (Client)
FRMCS Onboard Gateway
FRMCS Onboard System (RU)
5G Radio (IM A SIM)
xG Radio (IM B SIM)
Private FRMCS network
5G System
xG System
FRMCS Trackside System (IM A)
FRMCS Trackside System (IM B)
Multipath function (Server/ Gateway)
Multipath function (Server/ Gateway)
FRMCS Service Server
FRMCS Service Server
Tight Coupled App
FRMCS Client
App
Tight Coupled App
FRMCS Client
App

Figure 8: Traffic flow for network transition

3.7.1 Description

In this use case, the Data Flow is routed based on the selected endpoint in the trackside as well as based on the FRMCS service server (MCX server) the corresponding client is registered to.

3.7.2 Resulting Requirements

- Routing of a Data Flow based on MCX server registration of the corresponding MCX session
- Mapping of a Data Flow to an MCX session incl. knowledge of the MCX server registration
- MPF client needs to be connected to multiple MPF servers

4 Functional Requirements

High-level requirements for multipath functionality as part of the hybrid FRMCS network approach under 5G-RACOM project have been summarized in WP1 Report [1], based on the high-level use cases defined within the same report.

These high-level requirements include the following:

1) Data Flow Specific Path Management
2) Path Management Capabilities
3) Architectural Requirements
4) Transparency/Decoupling Requirements
5) Availability Requirements

Additional general requirements have been defined in this WP3 report. It shall be noted that the requirements are neither exhaustive nor necessarily complete.

4.1 Detailed Functional Requirements Definitions

In this chapter, we further elaborate on the high-level requirements based on the high level use cases from WP1 and the detailed use case descriptions in chapter 3. These detailed requirements definitions allow for a more precise differentiation of various capabilities and facilitate their prioritization. Requirements are grouped to evaluate the relevance and relative importance of each, ensuring a structured approach to their analysis and implementation.

4.1.1 General Requirements (GEN)

1. MPF shall be capable of supporting IP based packet Data Flows. MPF shall in principle work with IPv4 and IPv6 payload packets.
2. MPF shall ensure in-order received packet delivery to higher layers in both directions. Applications shall be able to rely on correct packet delivery for all receiving packet streams.
3. MPF clients (both onboard and trackside) shall receive operating rules (Multipath Policy) via FS_MPM interface from MPF server located at the trackside.
4. MPF shall be able to provide monitoring capabilities to allow the assessment/measurement of QoS fulfilment. Monitoring can include fault and performance monitoring.
5. MPF shall be able to access feedback on fulfilment of QoS requirements per Data Flow.
6. MPF shall be able to access feedback on fulfilment of QoS requirements per Data Path.
7. Interoperability of MPF onboard and MPF trackside between different vendors shall be ensured.
8. Integration to 5GC networks and its functions shall use standard 5GC interfaces.

4.1.2 Data Flow Specific Path Management (FSPM)

1. MPF shall map the Data Flows (referring to application data or service stratum signalling) to Data Paths (constituted by the combination of an UE and transport network) taking into account the path management capabilities (see next chapter).
2. MPF shall be able to identify a Data Flow and its type (e.g. ETCS, ATO, MCX signalling) based on IP header information (e.g. 5-tuple).
3. MPF shall take into account priorities provided via the Multipath Policy for a specific Data Flow for the path management.
4. MPF shall take into account any operator provided policy given for path management, which might override Multipath Policy inside MPF or provided by applications.
5. MPF shall take into account QoS (data rate, latency, reliability) per Data Flow for the Data Path management i.e. consider QoS requirements obtained via the Multipath Policies and QoS measurements per Data Flow and/or Data Path.

4.1.3 Path Management Capabilities (PMC)

The following MPF capabilities shall be based on the Multipath Policy and quality measurements per Data Path and/or Data Flow available at the MPFs:

1. Steering: the MPF shall be able to select the Data Path (i.e. initial Data Path selection).
2. Switching: the MPF shall be able to switch the mapping/routing of a Data Flow from one Data Path to another one during an active session.
3. Aggregation & Splitting: the MPF shall be able to aggregate/combine multiple Data Paths for a single Data Flow to allow aggregation of bandwidths. Data Flow splitting into subflows is implicit part of aggregation.
4. Replication: the MPF shall be able to use parallel Data Paths to transfer replicated packets in order to increase reliability of packet transfer.
5. Static Data Path routing: Static path routing has to be seen in combination with the above defined Data Path management capabilities.
6. Dynamic Data Path routing: Dynamic Data Path routing has to be seen in combination with the above defined path management capabilities.

4.1.4 Architectural Requirements (ARCH)

1. MPF shall be embedded in the overall FRMCS architecture in a way to respect FRMCS concepts of independence of layers (service layer and transport layer) and shall support various transport layers (including 4G/5G) in parallel.
2. MPF is considered as optional in FRMCS trackside and may be mandatory in FRMCS onboard. A later introduction of MPF shall not break overall service layer and transport layer interfaces, so interfaces to/from service layer and to/from transport layer at the trackside shall be the same as much as possible in case MPF is deployed or not.
3. MPF shall support differentiation between control plane and user plane to allow a kind of distributed architecture at least for the user plane functions and allow a smooth alignment to transport layer user plane functions as well as potential future distributed service layer user plane function.
4. At this time, the user plane is considered as the part of the MPF which is actually providing the data transmission and data reception via one or multiple Data Paths. The MPF user plane function shall be steered via the MPF control plane. The MPF control plane is expected to include provisions to support all control and steering related functions to achieve the multipath functionality. MPF shall support the FRMCS QoS signalling framework.

4.1.5 Transparency/Decoupling Requirements (TRANS)

1. MPF shall support MCX system.
2. MPF shall be independent to the higher layer protocols.
3. MPF shall support connection oriented TCP L4 connections.
4. MPF shall support connection less UDP L4 connections.
5. MPF shall allow the transport layer technique framed routing.
6. MPF shall allow NAT.
7. MPF shall support higher layer security.
8. MPF shall support security mechanisms on the transport layer.
9. MPF shall support tunnelling mechanisms and protocols for the service layer sessions.

4.1.6 Availability Requirements (AVAIL)

1. MPF shall support redundancy mechanism for network failure.
2. MPF shall select bypassing of the MPF communication in case of failure.

4.2 Requirements List, Classification and Prioritization

- Priorities: M – Mandatory, O – Optional, N – Not required
- UC0X: X classifies relevance for the use case
- All requirements are applicable for the general 5G-RACOM MPF specification and testbed implementation. The project will further analyse the requirements and thus it may happen that not even all mandatory requirements may be implemented.

<table>
<tr><th>ID</th><th>MPF Requirement (Short)</th><th>Priority</th><th>UC01</th><th>UC02</th><th>UC03</th><th>UC04</th><th>UC05</th><th>UC06</th></tr>
<tr><td colspan="9"><b>General Requirements (GEN)</b></td></tr>
<tr><td>GEN1</td><td>Support of IP packet Data Flows – IPv4 & IPv6</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>GEN2</td><td>In-order packet delivery</td><td>M</td><td></td><td></td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>GEN3</td><td>MPF clients receive operating rules from MPF server via FS_MPM* interface</td><td>N</td><td colspan="6">X</td></tr>
<tr><td>GEN4</td><td>MPF provides monitoring capabilities on QoS requirements fulfilment – fault & performance</td><td>O</td><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>GEN5</td><td>MPF with access to feedback on QoS requirements fulfilment per Data Flow</td><td>O</td><td></td><td></td><td>X</td><td></td><td></td><td>X</td></tr>
<tr><td>GEN6</td><td>MPF with access to feedback on QoS requirements fulfilment per Data Path</td><td>O</td><td colspan="6">X</td></tr>
<tr><td>GEN7</td><td>Interoperability of MPF Onboard and MPF Trackside</td><td>O</td><td colspan="6">X</td></tr>
<tr><td>GEN8</td><td>Integration to 5GC using standard 5GC interfaces</td><td>M</td><td colspan="6">X</td></tr>
<tr><td colspan="9"><b>Data Flow Specific Path Management (FSPM)</b></td></tr>
<tr><td>FSPM1</td><td>Mapping of Data Flows to Data Path takes PMC into account</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>FSPM2</td><td>Identification of Data Flow and its type based on IP header</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>FSPM3</td><td>Priorities via Multipath Policies for Data Flow for PMC</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>FSPM4</td><td>Apply operator policies for Data Path management, which might override MPF policy or application provided policy</td><td>O</td><td></td><td></td><td></td><td></td><td>X</td><td></td></tr>
<tr><td>FSPM5</td><td>Apply QoS per Data Flow for PMC considering QoS from Multipath Policies per Data Flow or Data Path</td><td>O</td><td></td><td></td><td>X</td><td></td><td></td><td>X</td></tr>
<tr><td colspan="9"><b>Path Management Capabilities (PMC)</b></td></tr>
<tr><td>PMC1</td><td>Steering: initial Data Path selection</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>PMC2</td><td>Switching: switch Data Flow between Data Paths during active session</td><td>M</td><td></td><td>X</td><td>X</td><td></td><td>X</td><td>X</td></tr>
<tr><td>PMC3</td><td>Aggregation & Splitting: aggregate/combine multiple Data Paths for a single Data Flow</td><td>O</td><td></td><td></td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>PMC4</td><td>Replication: replicate packets over parallel Data Paths</td><td>O</td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td>PMC5</td><td>Static Data Path routing – in combination of PMC1 to PMC4</td><td>M</td><td>X</td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td>PMC6</td><td>Dynamic Data Path routing – in combination of PMC1 to PMC-4</td><td>M</td><td></td><td>X</td><td>X</td><td>X**</td><td>X</td><td>X</td></tr>
<tr><td colspan="9"><b>Architectural Requirements (ARCH)</b></td></tr>
<tr><td>ARCH1</td><td>MPF embedded in FRMCS architecture respecting FRMCS concepts (independence of layers)</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>ARCH2</td><td>MPF interfaces to transport layer and service layer to allow later MPF introduction</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>ARCH3</td><td>MPF to support differentiation of control plane and user plane</td><td>O</td><td colspan="6">X</td></tr>
</table>

<table>
<tr><th>ID</th><th>MPF Requirement (Short)</th><th>Priority</th><th>UC01</th><th>UC02</th><th>UC03</th><th>UC04</th><th>UC05</th><th>UC06</th></tr>
<tr><td>ARCH4</td><td>Steering of MPF user plane via MPF control plane, including support of FRMCS QoS framework</td><td>O</td><td colspan="6">X</td></tr>
<tr><td colspan="9"><b>Transparency/Decoupling Requirements (TRANS)</b></td></tr>
<tr><td>TRANS1</td><td>MPF shall support MCX system</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>TRANS2</td><td>MPF shall be independent to the higher layer protocols</td><td>O</td><td colspan="6">X</td></tr>
<tr><td>TRANS3</td><td>MPF shall support connection oriented TCP L4 connections</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>TRANS4</td><td>MPF shall support connection less UDP L4 connections</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>TRANS5</td><td>MPF shall interwork and support with the transport layer technique framed routing</td><td>O</td><td colspan="6">X</td></tr>
<tr><td>TRANS6</td><td>MPF shall allow NAT</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>TRANS7</td><td>MPF shall support higher layer security</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>TRANS8</td><td>MPF shall support security mechanisms on the transport layer</td><td>M</td><td colspan="6">X</td></tr>
<tr><td>TRANS9</td><td>MPF shall support tunnelling mechanisms and protocols for the service layer sessions</td><td>M</td><td colspan="6">X</td></tr>
<tr><td colspan="9"><b>Availability Requirements (AVAIL)</b></td></tr>
<tr><td>AVAIL1</td><td>MPF shall support redundancy mechanism for network failure</td><td>M</td><td></td><td>X</td><td></td><td></td><td>X</td><td></td></tr>
<tr><td>AVAIL2</td><td>MPF shall select bypassing of the communication in case of failure</td><td>O</td><td colspan="6">X</td></tr>
</table>

**Note: FS_MPM not yet specified by standards*

***Note: Dynamic path routing for duplication does not imply a real routing decision as each packet is just duplicated (or not if a 2nd Data Path is not available). Dynamic change can still apply to change this duplication based on availability of the 2nd Data Path. Thus we see limited applicability of this requirement for UC04.*

Table 2: Requirement list with classification and alignment with use cases

5 Assessment Framework

5.1 Methodology and Process

This chapter presents a general methodology and process designed to facilitate the systematic assessment of diverse candidate multipath technologies (see chapter 6). The framework aims to provide the project with a structured approach to evaluating the performance, efficiency, and suitability of different multipath solutions by the requirements given in chapter 4. The methodology proposed herein is structured to encompass key aspects of multipath technologies, including their bandwidth utilization, latency management, fault tolerance mechanisms, and overall scalability. It considers the multifaceted nature of hybrid network structures foreseen in the FRMCS environment.

From the project execution perspective, the assessment will be carried out in two main phases. Phase 1 assessments have already been completed, primarily through theoretical and high-level analysis, as well as a comparative evaluation of all candidates multipath technologies. These assessments were based on compliance with defined general and business criteria, as well as an evaluation of the general compliance of the system architecture with the functional requirements and key performance indications. Outcomes of this phase are summarized in chapter 7. In phase 2, the most promising multipath technologies will be implemented according to the system architecture defined in chapter 2 and practical and in-depth analysis and assessments are being carried out as part of field testing. Based on the use cases in chapter 3, a set of test scenarios accompanied by performance criteria will be used to evaluate the technologies within their intended area of application.

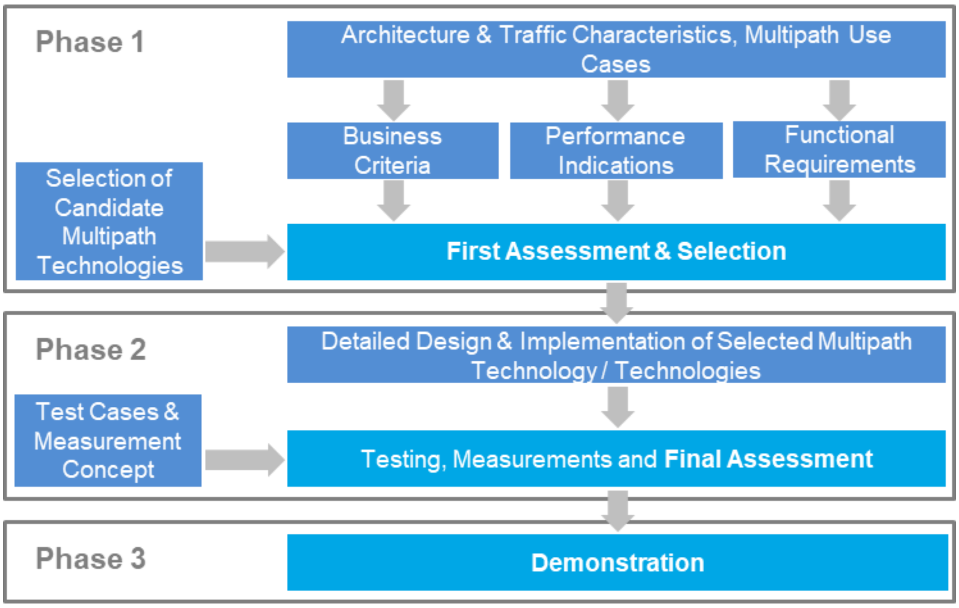
Phase 1
Architecture & Traffic Characteristics, Multipath Use Cases
Business Criteria
Performance Indications
Functional Requirements
Selection of Candidate Multipath Technologies
First Assessment & Selection
Phase 2
Detailed Design & Implementation of Selected Multipath Technology / Technologies
Test Cases & Measurement Concept
Testing, Measurements and Final Assessment
Phase 3
Demonstration

Figure 9: Multipath assessment phases and process

5.2 Phase 1 Assessment Criteria

These non-exhaustive criteria are rather subjective and focus on characteristics that can be estimated/concluded at this phase of the project based on publicly available resources and existing expertise within the project team.

General / Business Criteria

- Standardization – standard availability, specifications maturity, dynamics of standardization, etc.

- Implementation – open-source/commercial implementation availability, implementation maturity, implementation/integration complexity, references/deployments, etc.
- Operation & maintenance – operation & maintenance efforts, backwards compatibility, security impacts, availability & resiliency impacts, lifetime expectation, etc.

Fulfilment of Functional Requirements

The functional requirements are established in chapter 4. The assessment in this phase will focus on meeting some of the key requirements:

- Path management capabilities – Data Flow specific Data Path selection, steering, switching, splitting & aggregation, replication, in-order delivery, prioritization of Data Flows, etc.
- Unstructured – support of IP Data Flows, identification of type of IP Data Flow based on IP header, in-order packet delivery, QoS monitoring capabilities per Data Path and Data Flow, independence on the higher layer protocols, support of connection oriented and connection less TCP/UDP connections, NAT, framed routing, tunnelling, upper layer security, etc.

Note that all candidate multipath technologies and their implementation are considered as compliant with the general system architecture (see chapter 2) and the FRMCS and 3GPP standards.

Performance indications

At this phase, the project will focus only on performance indications in terms of possible additional latency caused by the characteristics of the candidate multipath solutions and the required capabilities. To assess each technology from this perspective, head-of-line blocking issue, ACKs/retransmissions disabling/reducing, additional security procedures, protocol setup time, etc. will be analysed.

Note that other characteristics such as data rates, packet drop/error rate, availability, etc. will be analysed in detail through the testing of selected multipath technology/technologies in phase 2.

5.3 Phase 2 Flavours of Criteria’s

Criteria and related KPIs contained in this chapter are defined to facilitate the assessment of the selected multipath technology/technologies in an objective manner through functional and/or performance testing.

5.3.1 Types of Criteria and KPIs

In this section, the Continuous Monitoring of KPIs and On-Demand KPIs is discussed.

5.3.1.1 Continuous Monitoring KPIs

The parameters described in this section shall be collected in a way, that a continuous monitoring of the connection is possible. These parameters shall be captured on each used modem or connection, separately for UL and DL direction where applicable. The time between two measurements and observation window shall be both configurable. Aim of these measurements shall be a permanent observation of the connection status and general quality of the connection. Those measurements are coupled directly to the modem and shall be available independently from a user data stream initiated by an application.

Criteria	Measurement Method	KPI	Severity
Path Switching Time	Switching time – ping measurement of old and new location IP address or wireshark	Interrupt time	medium
Data Rate Improvement	Total amount of data – median value over time in relation to max theoretical value or previous state of data throughput rate	Data rate improvement	high
Processing Delay	Delay from request of sending data to actual transmit to the network – protocol time stamps are used	Processing delay	medium

Data Rate	Data rate – e.g. iPerf / Netcat	Data throughput rate	high
Latency	Time delay between start and end of data transfer – network time protocol time stamps are used	Latency	high
Reliability	Percentage of packets lost & erroneous	Packet loss & error rate	high
Availability	Percentage of time data connection is available	Connection availability	medium
Radio parameters	SINR, RSRP, RSRQ, CQI, etc. available at the radio modem side and air interface	Air/radio interface KPIs	medium

Table 3: Measurable Criteria

Criteria	Measurement Method	KPI	Severity
Load Balancing Efficiency	Effective distribution of traffic	-	low
Fault Tolerance	General handling of path failures	-	low
Interoperability with the Internet	-	-	low
Open-Source	-	-	low
Encryption and Security	-	-	low
Evolution and Development	-	-	low

Table 4: General Criteria

5.3.1.2 On-Demand KPIs

On demand of a user an application, it shall be possible to capture performance indicators, which are relevant for the functionality of the application. For those KPI measurements, limitations must be defined for each of the identified candidate technologies.

5.3.2 General Measurement / Evaluation of Assessment Criteria

The following figure shows the test setup for the general measurement of assessment criteria.

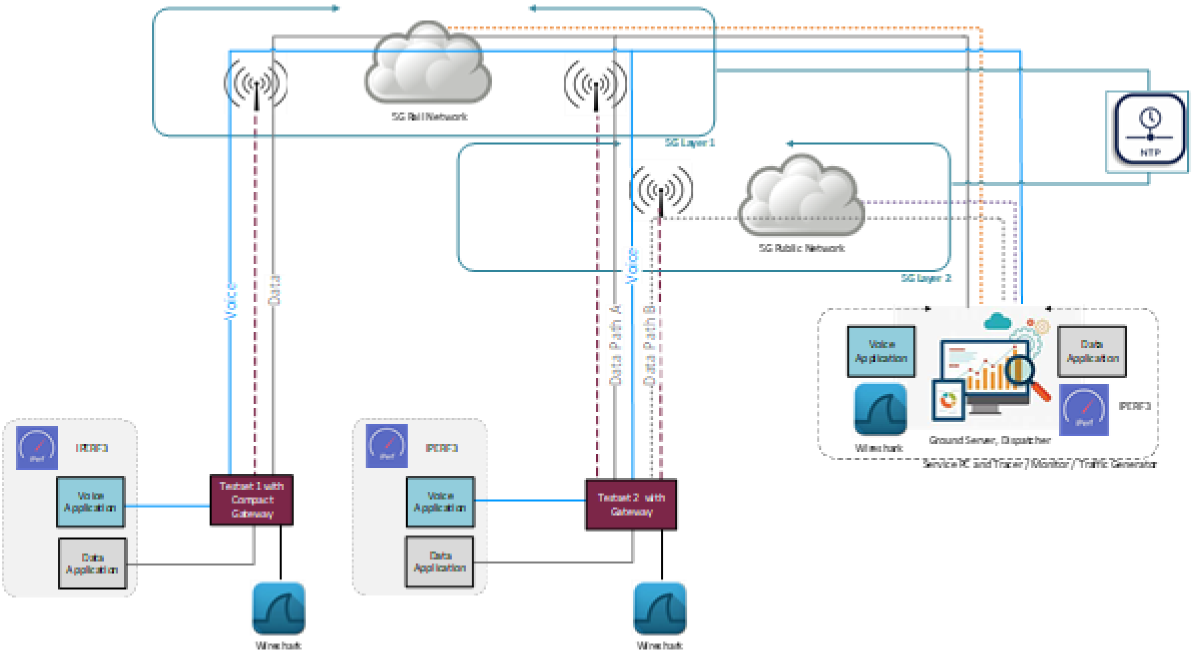

Figure 10: Test Setup for General Measurement of Assessment Criteria

6 Candidate Multipath Technologies

Multipath transport protocols have taken relevance nowadays with the availability of different network interfaces in the same systems and the amount of new applications and services requiring further development of protocols in different layers of the OSI model. This chapter will introduce the main details of multipath protocols, including their characteristics, differences from single path protocols and similarities with single path versions. It will also discuss specified multipath protocols like MPTCP, MP-QUIC, MPUDP, MP-DCCP and MPSCTP.

6.1 Required Capabilities

The concept of multipath is an extension of the single path concept. In this case, the idea is to create different subflows with each of the subflows having its own IP address but both of them belonging to the same connection. Having this in mind, multipath can be seen as a bundling of the network resources of a system to provide better overall performance for a specific connection. Adding additional subflows adds complexity to the systems, therefore concepts such as traffic handling, congestion control, fairness, reliability and others must be discussed to understand how the multipath protocols address them. The main required capabilities are:

- Steering: The ability to select and use one or more specific network interfaces for new Data Flows. In this sense, steering is the feature that makes multipath transport to be aware of the kind of traffic that is incoming and select the network that appropriately fulfils the requirements for the traffic, taking into account the personalized policies that can be set.
- Switching: This feature refers to the ability of the protocol to adjust its parameters to provide an appropriate route for a certain Data Flow. Whenever the main or any of the networks being used for this specific Data Flow becomes unavailable or degrade to a level that affects the service provided, the switching functionality is in charge of keeping the service continuity and moving the data with the available resources to keep the service available or as good as possible. In other words, the switching feature enables hand-over & fallback mechanisms and connection migration for the transport layer.
- Splitting: This functionality is the one that covers the distribution of the traffic of a Data Flow across multiple subflows and thus, different access networks. In other words, is the one in charge of splitting the traffic over the different subflows depending on the user needs. For instance, for the case of reliability the splitting functionality would manage the protocol in order to send the same packet over some or all subflows at the same time, decreasing the overall capacity but ensuring the appropriate handling of critical data.

6.2 Core Functional Blocks

Taking into account the main functionalities that multipath protocols have, the following include the core multipath functional blocks:

- Path management: This functionality oversees starting and maintaining the subflows for a connection. In this sense, this block controls the advertisement and acceptance of new IP's and therefore, the creation of new subflows. In the same way, it can remove flows that will not be part of the connection, due to quality issues, delay problems or any reason that turns a subflow unsuitable for the connection. Taking this into account, this block represents the main part for the steering concept. Note that the exact way of managing the paths depends on the protocol itself thus, the discovery, negotiation, maintenance and closure of the subflows will be independent for different protocols.

- Scheduling: The scheduling is in charge of distributing the packets over different subflows within a connection. Thus, covering the splitting concept of multipath. The scheduling part is one of the most important blocks of as a wrong scheduling decision might result in blocking or receive-window limitations, affecting the performance of the protocol. There are lots of different scheduling algorithms and different studies around them and their performance [4] [5] [6], each of them can serve to a different purpose, the schedulers can be deployed to provide the highest capacity, the lowest delay, the highest reliability or even define the routing according to certain policies agreed between different parties of the network. Some of the algorithms are: Round Robin, Smallest Delay, Priority Delay, Proportional Fair, Persistent/Semi-Persistent Scheduling etc.
- Congestion control: As it is for the single-path transport protocols, congestion control represents a big concern as well for the multipath versions. Multipath protocols also require a way to control the traffic flow depending on the network characteristics. Although it may be tempting to simply extend single-path congestion control protocols to multipath—giving each subflow its own congestion control algorithm—this approach often leads to unfair resource allocation. Fairness among users is a key requirement for multipath systems. The method of assigning each subflow its own congestion control is known as “decoupled congestion control.” An alternative, called “coupled congestion control,” manages congestion for the overall connection, considering information from all links to maintain fairness among different users. According to [7], the main objectives of multipath congestion control are:
    - Obtain at least the same throughput as a single-path flow would on its best sub-path.
    - Not take up more capacity than if it was a single-path flow using the best sub-path.
    - Move as much as possible traffic off its most congested sub-paths.

To serve the mentioned purposes, algorithms like Linked-increase algorithm (LIA) have been developed. LIA is designed to coordinate congestion control across multiple subflows by linking the growth of their congestion windows, thus mitigating the fairness issues typically seen in uncoupled approaches.

The evolution of protocols poses a significant deployment challenge: how can we ensure a smooth transition to multipath? Forcing all users to migrate simultaneously across all services is impractical. Instead, a more effective strategy is to introduce multipath translation mechanisms—such as proxies or gateways in middleboxes—that enable incremental deployment. These solutions allow traffic to be tunnelled through multipath-enabled segments of the network without requiring immediate changes on either the client or server side. This approach ensures compatibility and gradual adoption while aligning with the ETSI FRMCS standards and architecture outlined earlier in the document.

The main challenge of the proxy solution is that the control loop of the end-to-end protocol (TCP, QUIC, etc.) flow will be broken and will be separated into N+1 loops with N being the number of proxies. To preserve the intended behaviour of the connection, it is essential to employ mechanisms that render the presence of proxies transparent to the endpoints. This ensures that critical functions like congestion control remain effective and are not adversely impacted by latency or variability introduced within the multipath segment.

6.3 Additional Requirements

- IP compatibility: The selected multipath technology shall be able to transport IP packets and not make any assumptions on which transport protocol is encapsulated.
- Support for unreliable traffic: The multipath technology should provide support for transporting unreliable traffic, such as QUIC or UDP based flows. Therefore, unreliable transmission should be supported.

- Support for flexible re-ordering: The multipath technology should support flexible re-ordering of user traffic, including no re-ordering at all. This requirement is important to support low latency traffic, where the re-creation of packet order may negatively impact delivery latency.
- Support for flexible congestion control: The multipath technology should support flexible congestion control, including the disabling of the congestion control, if the inner traffic is known to be congestion controlled.
- Support for flexible packet scheduling: The multipath technology should support different packet scheduling mechanisms, which should be configurable from the control plane. Examples are cheapest path first, or other more sophisticated schedulers.
- Support for disabling acknowledgements: With the multipath gateway function running as a middlebox between the client and AS, an inner congestion control loop will be established which can impact the outer control loop between the client and AS. This would need disabling of acknowledgements along with retransmissions at the MPF.
- Lightweight: The multipath technology should be lightweight in computational resources and limit the encapsulation overhead.

Note that the information provided in chapters 6.1, 6.2 and 6.3 complements information provided in chapters 4 and 5.

6.4 High-Level Descriptions of Candidate Technologies

For details refer to Annex 1.

6.5 Assessment of Candidate Technologies

The following is the assessment summary of the explored protocols.

6.5.1 MPTCP

Standardization: MPTCP has been evolving for around 10 years and is currently proposed as a standard in RFC 8684. It extends the widely used TCP protocol, ensuring a standardized approach to multipath transport with support for various interfaces.

Implementation: MPTCP is implemented in Linux kernels from version 5.4 onwards, and it is included in Ubuntu image 22.04 (LTS). Commercial products and open-source versions are available, contributing to its widespread implementation.

Operation & Maint.: MPTCP offers improved network reliability, reduced head-of-line blocking, and seamless fallback to TCP when needed. However, deploying MPTCP in the middle of the network poses challenges, particularly when gateways or proxies are involved, requiring careful attention to maintain control loops.

Data Flow Specific Path Selection: MPTCP allows the usage of different interfaces under a single TCP connection, enabling path selection based on network conditions, capacity, and reliability. It offers the ability to distribute traffic according to link possibilities, traffic characteristics, and internal policies.

Steering: In the latest Linux implementations (kernel 5.4 and onwards), MPTCP supports steering through a conjunction of the path manager, congestion control, and scheduler. This allows dynamic decisions on the suitability of paths, adjusting traffic based on policies and changing paths when necessary.

Switching: MPTCP includes switching capabilities in its latest Linux implementations. The path management entity, congestion control, and scheduler work together to facilitate switching between paths when needed.

Aggregation & Splitting: MPTCP supports capacity aggregation and splitting capabilities. The path management, scheduler, and congestion control collaborate to optimize traffic distribution among multiple paths, addressing network congestion and adapting to policies.

Replication: MPTCP does not inherently support replication due to the TCP nature, if one package is lost it will automatically re-transmit it, even if the packet arrives through another interface. Even though some implementations have it (specific scheduler), in the latest versions this was removed due to the mentioned reasons.

In-order Delivery: MPTCP ensures in-order delivery through its unique approach to data sequence mapping. It maintains a separation between subflows, managing a connection or data sequence number space and a subflow sequence number space for reliable data transmission.

Prioritization: MPTCP allows changing the priorities of paths, managed by the path management entity. This feature enables adapting to different network conditions and traffic characteristics for optimized performance.

Per Data Flow & Per Path Flow: MPTCP provides connection-level acknowledgments for overall data and path-level acknowledgments for specific flow chunks. This dual acknowledgment mechanism contributes to effective data flow management.

L4 Independence: MPTCP is designed to extend the TCP semantic to a "bundling" of TCP subflows under the same TCP connection, providing layer 4 independence for applications utilizing multipath transport.

Disabling Acks: MPTCP cannot disable ACK’s in the same way as TCP can't.

Additional Security Proc.: MPTCP supports secure transport by extending TCP semantics to bundle subflows under the same TCP connection. The protocol negotiates keys during connection setup for authenticating new flows, ensuring data integrity. It does not have a inherent security like TLS and that layer would need to be added.

Protocol Setup Time: MPTCP follows a standard 3-way handshake for connection setup, incorporating "MP CAPABLE" options to signal MPTCP capability and negotiate keys. The protocol provides additional options like "MP JOIN" and "MP ADD" for subflow creation, addition, and path advertising, contributing to efficient protocol setup.

6.5.2 MP-QUIC

Standardization: MP-QUIC, an evolution of the QUIC protocol, is not yet an official standard but is detailed in the internet-draft “Multipath Extension for QUIC". The protocol is expected to standardize the draft in the first h|alf of 2024, demonstrating potential alignment with future standards.

Implementation: MP-QUIC is available as open-source projects, with at least three implementations: MP-QUIC, XQUIC, PicoQUIC, and later available TQUIC. Implementations are available in Go, C and RUST and maintained by different organizations, contributing to the protocol's adaptability and adoption.

Operation & Maint.: As of January 2024, MP-QUIC is in good development stages of development, and the available implementations, though still not having all the required for the project, are being updated and maintained for performance. Potential issues include dependency problems and the protocol's application layer nature.

Data Flow Specific Path Selection: MP-QUIC allows explicit constraints on the number of paths through the "active connection id limit," providing flexibility in selecting suitable paths for data flow.

Steering: MP-QUIC theoretically supports steering capabilities through its path manager, which defines path suitability, manages new paths, and handles path addition or removal. However, the protocol lacks regulation on the scheduler, impacting full steering functionality.

Switching: MP-QUIC can switch between paths through its path management entity, and it has congestion control embedded. However, full switching capabilities might require coordination with the scheduler, which is not explicitly regulated.

Aggregation & Splitting: MP-QUIC supports aggregation and splitting capabilities through its path manager, scheduler, and congestion control. However, the protocol relies on the scheduler for full functionality, and some implementations like may lack splitting support.

Replication: Depending on the scheduler implementations, MP-QUIC could provide replication possibilities since ACK’s can be ignored with a specific working mode.

In-order Delivery: MP-QUIC achieves in-order delivery by numbering packets per path and using a sequence number+connection ID pair for reordering at the higher layer. An "ACK MP frame" is introduced to accommodate connection ID information in acknowledgments.

Prioritization: MP-QUIC lacks a fixed method for selecting preferred paths, as the protocol does not prioritize any path explicitly. The flexibility in schedulers, such as minRTT and Round Robin, offers room for customized prioritization strategies.

Per Data Flow & Per Path Flow: MP-QUIC uses the concept of "connections" for each path, bundling them under the MP-QUIC connection. Acknowledgments are structured using the ACK MP frame, contributing to effective management of data flow per path.

L4 Independence: MP-QUIC, like its base QUIC protocol, provides layer 4 independence by extending the QUIC semantic to bundle multiple paths under the same MP-QUIC connection.

Disabling Acks: It supports disabling acknowledgments, enhancing efficiency and reducing acknowledgment overhead.

Add. Security Proc.: MP-QUIC incorporates TLS for security, making it suitable for secure transport over HTTP. The protocol ensures encrypted communication, and connection setup involves authentication**.**

Protocol Setup Time: MP-QUIC follows a process similar to QUIC for initial connection establishment, but with additional options like "enable multipath." The use of "PATH_CHALLENGE" and "PATH_RESPONSE" for subflow creation adds efficiency to the protocol setup.

6.5.3 SCTP, CMT+SCTP, MPSCTP

Standardization: SCTP (Stream Control Transmission Protocol) is standardized by RFC9260, providing a connection-oriented message-switched protocol. CMT+SCTP and MPSCTP are extensions of SCTP designed to offer multipath capabilities.

Implementation: Pure SCTP has been commercially used and implemented in various operating systems, including AIX, NetBSD, Cisco IOS, FreeBSD, Linux kernel, and others. CMT+SCTP and MPSCTP are research-driven extensions, with fewer deployment instances.

Operation & Maint.: Pure SCTP ensures error-free, non-duplicated data transfer, optional bundling of messages, and network-level fault tolerance. It is commercially deployed in various operating systems, showcasing reliability. CMT+SCTP and MPSCTP face limitations in terms of widespread development and deployment, impacting their operational status.

Data Flow Specific Path Selection: SCTP supports multi-homing with different IP addresses under the same association. However, it does not send over all streams simultaneously. Specific path selection occurs through application-defined "SET_PRIMARY" or default criteria.

Steering: Pure SCTP does not have explicit steering functionality during association initiation. The selection of the primary address, used as the main path, is generally defined by the application or through "SET_PRIMARY." CMT+SCTP supports steering, selecting the main path based on scheduling policies.

Switching: Pure SCTP can handle switching characteristics in case of duplicated packets or heartbeat absence, leading the system to switch to another path. CMT+SCTP supports switching through the path manager, automatically transitioning to an alternative path if the primary one fails.

Aggregation & Splitting: SCTP does not use all paths simultaneously, employing other connections only when the main path fails. CMT+SCTP supports aggregation through load balancing, failover switching, and bandwidth aggregation, maximizing network resource utilization.

Replication: SCTP provides network-level fault tolerance through multi-homing, allowing the use of another path for retransmission in case of primary path failure.

In-order Delivery: SCTP ensures sequenced delivery of user messages within multiple streams, offering order-of-arrival delivery options. CMT+SCTP can face issues with out-of-order packets, but it manages retransmission policies to address this.

Prioritization: SCTP does not have a fixed method for selecting a preferred path, relying on application-defined criteria. CMT+SCTP incorporates scheduling policies for prioritizing the main path.

Per Data Flow & Per Path Flow: SCTP organizes connections into associations, with each path represented by different IP addresses. CMT+SCTP maps streams to different paths, enabling parallel transmission over each path.

L4 Independence: SCTP provides layer 4 independence, bundling different paths under the same association.

Disabling Acks: SCTP does not explicitly mention disabling acknowledgments. The concept of acknowledgments in SCTP is used for reliability.

Add. Security Proc.: SCTP, CMT+SCTP, and MPSCTP inherit security features from SCTP's base design. They do not introduce additional security procedures.

Protocol Setup Time: SCTP follows an association initiation process, with an INIT message. CMT+SCTP and MPSCTP have similar initiation processes, negotiating parameters and forming associations for data exchange.

High-level architecture incl. supported architecture options: The architecture of SCTP involves multihoming with different IP addresses under the same association. CMT+SCTP supports load balancing, failover, and bandwidth aggregation.

References to standards: SCTP is standardized by RFC9260. CMT+SCTP is referenced in an Internet Engineering Task Force draft, and MPSCTP extends SCTP with a different approach.

References to papers/studies: Various studies explore the evolution of SCTP with CMT, including issues related to out-of-order packets. MPSCTP papers highlight the use of two number spaces for accurate RTT calculation and congestion control.

References to use/deployments: Pure SCTP is commercially used and deployed in several operating systems. CMT+SCTP and MPSCTP have not seen actual deployments, primarily existing in research and simulation environments.

Support of steering/switching/splitting capabilities: Pure SCTP supports switching but lacks explicit support for steering and splitting. CMT+SCTP supports steering, switching, and splitting capabilities.

Integration with transport network infrastructure: SCTP's integration with transport network infrastructure depends on the implementation of the scheduler. CMT+SCTP follows similar considerations as MP-QUIC or MPTCP, relying on the scheduler for functionality.

Availability of commercial products and/or as open-source: Pure SCTP is commercially used, and open-source implementations are available in various operating systems. CMT+SCTP and MPSCTP are more research-driven, lacking actual deployments.

Assessment phase considerations (Pros/Cons, risks, issues, limitations, requirements compliancy, etc.): Pure SCTP is reliable but does not inherently increase throughput. CMT+SCTP addresses throughput aggregation but faces challenges with out-of-order packets and limited development. MPSCTP's approach with two numbering spaces aims to resolve issues with reordering but lacks extensive development and deployment.

In conclusion, SCTP stands as a reliable protocol, while CMT+SCTP and MPSCTP address throughput limitations but face challenges and limited adoption. The assessment should consider specific use cases and requirements for effective deployment.

6.5.4 MP-DCCP

Standardization: DCCP is a standardized transport layer protocol (RFC 4340) designed for applications requiring real-time, multimedia communication. MP-DCCP builds upon DCCP, extending its capabilities and being worked in the draft DCCP Extensions for Multipath Operation with Multiple Addresses [https://datatracker.ietf.org/doc/draft-ietf-tsvwg-multipath-dccp/].

Implementation: DCCP and MP-DCCP are implemented in open-source projects, making them accessible for research and development. Commercial networking products may also incorporate MP-DCCP.

Operation & Maint.: DCCP provides built-in congestion control, including Explicit Congestion Notification (ECN) support. MP-DCCP extends capabilities with multipath features, supporting load balancing, failover, and bandwidth aggregation.

Data Flow Specific Path Selection: MP-DCCP operates on a client-server architecture, establishing multiple paths to the receiver. It supports path steering, enabling dynamic selection of the most efficient paths for data transmission.

Steering: MP-DCCP supports path steering, allowing dynamic selection of the best paths for data transmission. It utilizes a scheduler to define the optimal way to distribute traffic.

Switching: MP-DCCP provides switching capabilities, allowing seamless path change in case of path failure or congestion. The scheduler plays a crucial role in determining the most efficient path.

Aggregation & Splitting: MP-DCCP supports bandwidth aggregation, combining the available bandwidth of all paths. Splitting capabilities depend on the scheduler, which determines the best way to distribute traffic.

Replication: It does support replication over all the available paths when the redundant scheduler is used.

In-order Delivery: DCCP provides unreliable data delivery, and MP-DCCP extends this by offering the possibility to reorder data upon arrival.

Prioritization Per Data Flow MP-DCCP supports scheduling policies, and prioritization could be implemented within the scheduler.

Per Path Flow: MP-DCCP operates by establishing multiple paths to the receiver, and the scheduler plays a role in managing flows over these paths.

L4 Independence: MP-DCCP, like its base DCCP protocol, provides layer 4 independence by extending the DCCP to bundle multiple paths under the same MP-DCCP connection.

Disabling Acks: DCCP ACK packets inform congestion control rather than re-transmission. MP-DCCP may disable acknowledgments selectively.

Additional Security Proc.: There is no built-in cryptographic security for MP-DCCP like TLS. Nonetheless, there is a security feature to authenticate new paths.

Protocol Setup Time: It follows a 3-way DCCP handshake.

6.5.5 MPUDP

Standardization: MPUDP is not a standardized protocol. The draft proposing "MPUDP" based on MP-DCCP has expired, and there is no specific deployment of MPUDP. Unofficial attempts, such as MPUDP implementations is available on GitHub, are more experimental and lack standardization.

Implementation: MPUDP lacks a specific deployment as a standalone protocol. Unofficial implementations, like the ones on GitHub (e.g., mp-tunnel, MLVPN), attempt to create multipath functionality for UDP by forwarding packets using tunnels or bonding several networks. An implementation of MPUDP with session creation for managing UDP packets has been developed.

Operation & Maint.: MPUDP, lacking a standardized deployment, has experimental implementations, and operational aspects may vary. Unofficial attempts, like mp--tunnel and MLVPN, involve configuring gateways or bonding networks. The implementation [2] introduces session creation to manage UDP packets.

6.5.6 SD-WAN

Standardization: SD-WAN is a technology that has become prevalent, yet standardization may vary as different vendors provide proprietary solutions. Standards are essential for interoperability and ensuring a common framework.

Implementation: SD-WAN implements a separation of the data plane and control plane, offering virtualized routing functionality. It is employed by vendors like Cisco and Fortinet. The implementation aims to reduce network costs, enhance speed through simplified management, improve security and visibility, and optimize overall network performance.

Operation & Maint.: SD-WAN simplifies network operations and maintenance by centralizing control plane decisions, reducing complexity at individual nodes. The separation of planes enables more straightforward management and faster failover, contributing to operational efficiency.

Data Flow Specific Path Selection: SD-WAN provides control over data flow through policies defined in the orchestration plane, allowing for specific path selections based on business requirements and Quality of Service (QoS) needs.

Steering: SD-WAN can facilitate traffic steering, allowing administrators to adjust policies for traffic balancing.

Switching: SD-WAN enables fast failover, enhancing availability by quickly adapting to changes in network conditions or failures. The control plane centrally manages switching decisions.

Aggregation & Splitting: N/A

Replication: N/A

In-order Delivery: N/A

Prioritization: SD-WAN allows administrators to define policies for specific businesses, implying the potential for prioritization.

Per Data Flow & Per Path Flow: SD-WAN's orchestration plane allows for policies to be defined based on business requirements, suggesting support for per-data-flow configuration.

L4 Independence: Yes, it is a layer 3 implementation and therefore, fully independent of the layer 4.

Disabling Acks: N/A

Add. Security Proc.: SD-WAN enhances security through deep analytics and troubleshooting implementation

Protocol Setup Time: N/A

6.5.7 Load Balancing Based IP Routing

Standardization: Load Balancing Based IP Routing operates at the IP layer and involves techniques for multipath routing. Although specific standardization details are not mentioned, it emphasizes the use of IP layer for faster routing compared to transport layer approaches.

Implementation: Implementation of load balancing based IP routing, highlighting the need for a scheduler to manage traffic based on network parameters. Various routing algorithms and frameworks, such as OSPF version 2 and the one presented in references [4], [5], and [6], demonstrate different approaches to implementation.

Operation & Maint.: Load balancing in IP networks involves concurrent multipathing or backup configurations. The operation includes dynamic adaptation, failovers, and a scheduler making decisions on routing packets through different networks connected to a router. Maintenance involves assessing the trade-offs between the number of paths and computational needs for optimal performance.

Data Flow Specific Path Selection: The approach involves distributing traffic through different networks connected to a router. The scheduler, acting at the network layer, decides how to route packets, contributing to data flow-specific path selection.

Steering: A scheduler approach is used, which implies that an organisation is responsible for scheduling traffic based on network parameters. This scheduler efficiently directs traffic along various network routes.

Switching: The concept of fault tolerance is applied with emphasis on multipath preservation strategy in case of failure in the main path. This indicates a switching capability to ensure uninterrupted data transmission.

Aggregation & Splitting: Load balancing includes the concept of flow splitting, allowing the concurrent usage of links to aggregate capacity. The scheduler approach can be configured for either simultaneous usage or as backups, addressing both aggregation and splitting.

Replication: N/A

In-order Delivery: Not supported

Prioritization: Partially supported depending on the implementation.

Per Data Flow & Per Path Flow: The scheduler decides how to route packets through different networks, indicating a per data flow and per path flow management capability.

L4 Independence: Load balancing is performed at the IP layer, emphasizing independence from Layer 4 protocols. This enables faster routing compared to transport layer approaches.

Disabling Acks: N/A

Additional Security Proc.: N/A

Protocol Setup Time: N/A

7 Conclusions and Multipath Technology Selection

MPTCP, MP-QUIC, SCTP, and MP-DCCP stand as robust multipath transport protocols, each boasting its distinctive strengths and grappling with inherent weaknesses. However, a comprehensive examination unveils key insights:

- **MPTCP and MP-QUIC**: These protocols emerge as the flag bearers of feature-rich multipath transport, presenting a diverse array of functionalities. The nuanced comparison places them at the forefront, showcasing their versatility in addressing various networking demands.
- **MP-QUIC's**: Notably, MP-QUIC gains precedence over MPTCP, thanks to a pivotal feature—disabling acknowledgments as a gateway solution. This strategic advantage positions MP-QUIC as a frontrunner in scenarios where minimizing acknowledgment overhead is critical for efficient data transmission.
- **MP-DCCP's**: In contrast, MP-DCCP, while trailing behind MPTCP and MP-QUIC in overall features, carves a unique niche by providing support for unreliable traffic without the burden of acknowledgments. However, its Achilles' heel lies in the limited resources and implementations.
- **Load Balancing Based IP Routing**: Load balancing based IP routing enhances transmission capabilities through multipath routing at the IP layer. Key considerations include:
  - Flow Splitting: Concurrent usage of links for aggregated capacity.
  - Traffic Engineering: Adjusting Data Paths to optimize data flows.

Configurations involve concurrent usage or backups, with a trade-off between performance and computational needs.

- **SD-WAN:** SD-WAN separates the data and control planes, offering benefits like reduced costs, increased speed, enhanced security, and improved availability. It provides a flexible solution for WAN networks with proprietary implementations by companies like Cisco and Fortinet. In the context of Multipath Transport Protocols, SD-WAN contributes to traffic balancing but operates at the IP layer without explicit details on aggregation methods or per-flow QoS. In conclusion, while SD-WAN offers advantages for WAN networks, the lack of clarity on certain aspects and its proprietary nature makes it distinct from Multipath Transport Protocols like MPTCP, MP-QUIC, SCTP, and MP-DCCP.

The contributions of Load Balancing Based IP Routing and SD-WAN come to the forefront, introducing additional dimensions to network optimization and traffic management. These technologies, with their distinct capabilities, enrich the discourse on multipath transport, ushering in new paradigms that warrant careful consideration in the evolving realm of network architecture.

Assessment Criteria		MPTCP	MP-QUIC	SCTP	DCCP	MPUDP	SD-WAN	Load-B.
Business	Standardization	🟩	🟩	🟥	🟥	🟥	🟥	🟥
	Implementation	🟩	🟧	🟥	🟧	🟥	🟧	🟥
	Operation & Maint.	🟩	🟧	🟥	🟧	🟥	🟩	🟨
Path Management	Data Flow Specific Path Selection	🟩	🟩	🟩	🟥	🟥	🟨	🟧
	Steering	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Switching	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	Aggregation & Splitting	🟩	🟩	🟥	🟩	🟥	🟨	🟨
	Replication	🟩	🟩	🟥	🟩	🟥	🟨	🟨
	In-order Delivery	🟩	🟩	🟥	🟥	🟥	🟨	🟥
	Prioritization	🟩	🟧	🟩	🟩	🟥	🟨	🟧
QoS Monitoring	Per Data Flow	🟩	🟩	🟩	🟥	🟥	🟨	🟥

	Per Path Flow	🟩	🟩	🟩	🟥	🟥	🟨	🟩
Perf. Indication	L4 Independence	🟧	🟩	🟧	🟧	🟧	🟨	🟩
	Disabling Acks	🟥	🟩	🟥	🟧	🟩	🟨	🟨
	Add. Security proc.	🟩	🟧	🟧	🟧	🟩	🟨	🟨
	Protocol setup time	🟧	🟧	🟧	🟧	🟩	🟨	🟨

🟩 Supported 🟥 Not supported 🟧 Partially supported 🟨 Unknown

Table 5: Multipath Feature Support

The project conducted an analysis of the MP-QUIC based MPF implementation feasibility. Several existing MP-QUIC libraries and own MP implementation on top of the standard QUIC library were analysed and subjected to basic testing to evaluate overall maturity and MP feature support. The analysis shown various levels of maturity, configuration options and MP feature support. It was concluded that further development would be necessary for any library under the project.

Selected implementations/libraries were compared based on assessment criteria outlined by the project. The outcome of the analysis is that it is indeed feasible to perform MP-QUIC based implementation within the project and specific library has been selected. Another outcome is that the first high-level assessment of MP candidate technologies remains valid. A more detailed analysis will be conducted as part of the implementation and testing phase. **The project team has agreed to implement both MPTCP and MP-QUIC protocols and will explore possibilities for multi-protocol support**.

Below is the table that further compares the three available open-source solutions of MP-QUIC which offer slightly different features because of their implementation. xQUIC provides a better solution compared to the other two.

Assessment Criteria		MP-QUIC	xQUIC	PicoQUIC
Business	Standardization	🟩	🟩	🟩
	Implementation	🟧	🟩	🟧
	Operation & Maint.	🟧	🟩	🟧
Path Management	Data Flow Specific Path Selection	🟩	🟩	🟩
	Steering	🟩	🟩	🟩
	Switching	🟩	🟩	🟩
	Aggregation & Splitting	🟩	🟩	🟧
	Replication	🟩	🟩	🟩
	In-order Delivery	🟩	🟩	🟩
	Prioritization	🟧	🟧	🟧
QoS Monitoring	Per Data Flow	🟩	🟩	🟩
	Per Path Flow	🟩	🟩	🟩
Perf. Indication	L4 Independence	🟧	🟩	🟩
	Disabling Acks	🟧	🟩	🟥
	Add. Security proc.	🟧	🟩	🟧
	Protocol setup time	🟧	🟧	🟧

🟩 Supported 🟥 Not supported 🟧 Partially supported 🟨 Unknown

Table 6: MP-QUIC Assessment of the Open-source Solutions

As a conclusion, it can be observed MPTCP and MP-QUIC offer the most features in terms of Multipath functionality and hence are the strongest contenders among the rest of the protocols. With disabling the acknowledgements being a critical feature of MPF as a gateway solution, MP-QUIC takes precedence over MPTCP. Although MP-DCCP features fare less in comparison with MPTCP and MP-QUIC, its inherent support of unreliable traffic (without Acks) can be in contention. The only drawback is a lower interest in general, leading to less research and implementations.

8 Annexes

Annex 1 - High-Level Descriptions of Candidate Technologies

9 Definitions

5-tuple	A set of five values that uniquely identify an UDP/TCP session. It includes the source IP address, source port, destination IP address, destination port and transport protocol. Note: A subset of these parameters may be sufficient to identify certain applications (i.e. a specific Type of Data Flow). Alternatively, an “any-to-any” configuration can be used to match all traffic.
Data Flow	A sequence of IP packets transmitted to and/or from the Multipath Function (MPF), where routing decisions are applied based on the Multipath Policy. Data Flows can refer to application data as well as to FRMCS service stratum signalling. A Data Flow refers to a transport-layer session and is characterized by Data Flow attributes (such as type of Data Flow: ETCS, Voice, TCMS, FRMCS signalling and QoS requirements (e.g. latency, data rate). A Data Flow is identified via one or more 5-tuples.
Data Path	A logical or physical route (network connection) between a specific MPF Client and MPF Server, used to transmit a Data Flow or Subflow. Data Path is typically associated with a transport network accessed via a UE/modem and its network interface. A Data Path can be configured as or associated with the following states: • Active - Data Path that carries one or more Data Flows or Subflows. • Default – The preferred Data Path for a Data Flow, used whenever available. • Alternative – A secondary or backup Data Path for a Data Flow, may be used in addition to or instead of the Default, depending on the Multipath Policy and Quality Thresholds. • Available – The Data Path meets the minimum Quality Threshold requirements for the Data Flow. • Unavailable – The Data Path does not meet the minimum Quality Threshold requirements for the Data Flow(s) or is out of service (outage/shutdown/etc.). Note: Data Path states are evaluated independently for each Data Flow, a Data Path may be available for one application and unavailable for another. A Data Path may also simultaneously hold multiple states, e.g., Available and Alternative.
Duplication/Replication	The capability to replicate packets of a Data Flow and transmit them over multiple Subflows over multiple Active Data Paths. At the receiver MPF, the original Data Flow is reassembled from the associated Subflows.
MPF	The Multipath Function (MPF) is a function responsible for managing the efficient transmission of Data Flows across multiple Data Paths between an MPF Client and an MPF Server/Gateway. It dynamically selects, switches, aggregates, or replicates traffic based on the Multipath Policy and Quality Thresholds, ensuring seamless, adaptive, and resilient communication.

	The MPF acts as a proxy or gateway, positioned between endpoints to provide multipath capabilities without requiring modifications to end-user applications. It acts as an intermediary, utilizing multipath transport protocols such as MPTCP and MP-QUIC to optimize performance and reliability while maintaining compatibility with traditional transport and application protocols.
Multipath	A functionality provided by the MPF that enables the utilization of multiple independent Data Paths (network connections) simultaneously and/or dynamically to improve performance, reliability, and resilience.
Multipath Policy	A set of rules for mapping Data Flows to Data Paths (in terms of steering decisions) and associated conditions (e.g. Quality Threshold(s), use of multipath capabilities such as switching, splitting, replication). The policy may contain static rules for which dynamic evaluation is not needed (e.g. Default Data Path per Application, Alternative Data Path per application) and/or rules which need to be evaluated dynamically (e.g. QoS/continuity requirements assessment based on link quality measurements). The Multipath Policy is provided by the MPF server of the FRMCS infrastructure.
Quality Threshold	A performance criterion that determines whether a Data Path is suitable for a given Data Flow(s). It is based on measurable network quality parameters, such as throughput, latency, packet loss, ensuring that the selected Data Path meets the requirements of the application or service. Network quality parameters shall be measured continuously and event-based.
Splitting (Aggregation)	A capability where a Data Flow is divided into Subflows, which are transmitted over multiple Available Data Paths. When splitting is applied to a Data Flow, a part of the Data Flow is transferred over one Data Path while the remaining part of the Data Flow is transferred over one or more other Data Paths. At the receiver MPF, the original Data Flow is reassembled (aggregated and reordered) from the associated Subflows. Aggregation is inherently part of Splitting, and may occur in both outbound and inbound directions.
Steering	The initial selection of one or more Default or Alternative Data Paths to direct a specific Data Flow. It is assumed that this is performed during "initial" Data Path selection, e.g. after startup/restart/outage.
Subflow	A transport-layer segment flow (QUIC, TCP, etc.) operating over an individual Data Path, forming part of a larger Multipath connection (MP-QUIC, MPTCP, etc.). A Subflow is established and terminated similarly to a regular single-path connection. While each Subflow is typically mapped 1:1 to a Data Path, a Data Path can carry multiple Subflows from different applications or sessions.
Switching	The redirection of an ongoing Data Flow from one Active Data Path to an Alternative Data Path, or vice versa, without disrupting the connection. Switching shall not result in a dropped connection (which would cause re-initiation). Temporary QoS degradation may occur but should be tolerated.

10 Abbreviations

2G	2nd Generation of mobile communications aka GSM/EDGE
3GPP	3rd Generation Partnership Project
4G	4th Generation of mobile communications aka LTE
5G	5th Generation of mobile communications
5GS	5G System
APS	Advanced Protection System
ATO	Autonomous Train Operation
ATSSS	Access Traffic Steering, Switching and Splitting protocol
BMWK	Federal Ministry for Economic Affairs and Climate Action
CCS	Command, Control and Signalling
COTS	Commercial Off The Shelf
DB	Deutsche Bahn i.e. DB InfraGO (former DB Netz AG)
DL	Downlink
DNN	Data Network Name
DTB	Digital Rail Testbed
E2E	End To End
EC	European Commission
(e)DECOR	(Enhanced) Dedicated Core Networks
ERA	European Railway Agency
ERJU	Europe's Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
FRMCS	Future Railway Mobile Communication System
GoA	Grade of Automation
GSM-R	Global System for Mobile Communications – Rail
HR	Home Routed roaming
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Infrastructure Manager
IMS	IP Multimedia Subsystem
IPv6	Internet Protocol version 6
ISD	Inter-Site Distance
LBO	Local BreakOut roaming
MA	Movement Authority
MAMS	Multi-Access Management Services
MCX	Mission Critical Services
MEFR	Ministère de l’Economie et des Finances et de la Relance
MNO	Mobile Network Operator
MPF	MultiPath Function
MP-DCCP	MultiPath Datagram Congestion Control Protocol
MP-QUIC	MultiPath Quick UDP Internet Connections protocol
MPTCP	MultiPath Transmission Control Protocol
NSA	Non-Standalone Access

N3G	Non-3GPP Access
N77/N78	3GPP 5G bands in 900 and 1900 MHz
NSA	Non-Standalone 5G network architecture
PoC	Proof of Concept
QUIC	Quick UDP Internet Protocol
RACOM	Resilient and Green RAil COMmunications
RAN	Radio Access Network
RAT	Radio Access Type
RBC	Radio Block Center
REC	Railway Emergency Communication
RMR	Rail Mobile Radio
RU	Railway Undertaking
SA	Standalone 5G network architecture
SD-WAN	Software Defined WAN
SNCF	Société Nationale des Chemins de fer Français i.e. SNCF Réseau
TC RT	Technical Committee for Railway Telecommunications
TCMS	Train Control and Monitoring System
TSI	Technical Specification of Interoperability
TU	Technical University i.e. Chemnitz, Ilmenau
UE	User Equipment
UIC	International Union of Railways
UL	Uplink
WLAN	Wireless LAN i.e. WiFi
WP	Work-Package

11 References

[1] 5G-RACOM, “Work Package 1: Use Cases, Requirements and Assumptions – Final Report,” 2023.

[2] UIC, “FRMCS System Requirements Specification”.

[3] UIC, FRMCS Multipath use cases, Doc. No. FW-AT 7324

[4] Bruno YL Kimura, Demetrius CSF Lima, and Antonio AF Loureiro, “Packet scheduling in multipath TCP: Fundamentals, lessons, and opportunities,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 1445–1457, 2020.

[5] P. Rengaraju, C.-H. Lung, and A. Srinivasan, “Adaptive admission control and packet scheduling schemes for QoS provisioning in multihop WiMAX networks,” in *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2012, pp. 866–871.

[6] [Ros19-3] Marc Mollà Roselló, “Multi-path scheduling with deep reinforcement learning,” in *2019 European Conference on Networks and Communications (EuCNC)*, pp. 400–405, 2019.

[7] De Coninck, Q., & Bonaventure, O. (2017, November). Multipath quic: Design and evaluation. In *Proceedings of the 13th international conference on emerging networking experiments and technologies* (pp. 160-166).

[8] “ATSSS Emulated“ https://www.etsi.org/deliver/etsi_tr/103400_103499/103459/01.02.01_60/tr_103459v010201p.pdf

[9] 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)

[10] H. Wu, S. Ferlin, G. Caso, Ö. Alay and A. Brunstrom, "A Survey on Multipath Transport Protocols Towards 5G Access Traffic Steering, Switching and Splitting," in IEEE Access, vol. 9, pp. 164417-164439, 2021, doi: 10.1109/ACCESS.2021.3134261.

[11] M. Boucadair et al., “3GPP Access Traffic Steering Switching and Splitting (ATSSS) – Overview for IETF Participants”, proposed RFC “draft-bonaventure-quic-atsss-overview”.

[12] Y. Kang and C. Kim, "A Multi-Access Session Management for ATSSS Support in 5G Network," 2019 25th Asia-Pacific Conference on Communications (APCC), Ho Chi Minh City, Vietnam, 2019, pp. 409-412, doi: 10.1109/APCC47188.2019.9026504.

[13] C. Barjau, D. Gomez-Barquero, H. Jung, S. -I. Park and N. Hur, "Limitations of ATSSS technology in ATSC 3.0 – 5G convergent systems," 2021 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Chengdu, China, 2021, pp. 1-5, doi: 10.1109/BMSB53066.2021.9547016.c

[14] https://www.telekom.com/en/company/details/deutsche-telekom-demonstrates-multipath-for-fixed-mobile-convergence-on-campus-625838

[15] https://www.tessares.net/solutions/5g-atsss-solution/

[16] RFC 8743 Multi-Access Management Services (MAMS)

[17] Alan Ford, Costin Raiciu, Mark J. Handley, Olivier Bonaventure, and Christoph Paasch, *TCP Extensions for Multipath Operation with Multiple Addresses*, RFC 8684, RFC Editor, March 2020. Available: https://www.rfc-editor.org/info/rfc8684. DOI: 10.17487/RFC8684.

[18] https://arxiv.org/abs/1801.05168

[19] Q. D. Coninck, M. Baerts, B. Hesmans, and O. Bonaventure, ‘‘A first analysis of multipath TCP on smartphones,’’ in Passive and Active Measurement. Cham, Switzerland: Springer, 2016, pp. 57–69.

[20] B. Y. L. Kimura, D. C. S. F. Lima and A. A. F. Loureiro, "Packet Scheduling in Multipath TCP: Fundamentals, Lessons, and Opportunities," in *IEEE Systems Journal*, vol. 15, no. 1, pp. 1445-1457, March 2021, doi: 10.1109/JSYST.2020.2965471.

[21] GitHub - multipath-tcp/mptcp_net-next

[22] T. Li, L. Li, X. Wang, X. Zhang, F. Zhang and K. Wan, "An In-depth Analysis of Subflow Degradation for Multi-path TCP on High Speed Rails," *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Belfast, United Kingdom, 2022, pp. 231-240, doi: 10.1109/WoWMoM54355.2022.00042.

[23] I. Lopez, M. Aguado and C. Pinedo, "A Step Up in European Rail Traffic Management Systems: A Seamless Fail Recovery Scheme," in *IEEE Vehicular Technology Magazine*, vol. 11, no. 2, pp. 52-59, June 2016, doi: 10.1109/MVT.2016.2519540.

[24] Yanmei Liu, Yunfei Ma, Quentin De Coninck, Olivier Bonaventure, Christian Huitema, and Mirja Kühlewind, “Multipath Extension for QUIC”, Internet-Draft draft-ietf-quic-multipath-04, Internet Engineering Task Force, Mar. 2023, Work in Progress.

[25] Tommy Pauly, Eric Kinnear, & David Schinazi. (2022). An Unreliable Datagram Extension to QUIC. https://datatracker.ietf.org/doc/rfc9221/

[26] https://datatracker.ietf.org/doc/draft-ietf-quic-multipath/

[27] De Coninck, Q., & Bonaventure, O. (2019, June). Multipathtester: Comparing mptcp and mpquic in mobile environments. In *2019 Network Traffic Measurement and Analysis Conference (TMA)* (pp. 221-226). IEEE.

[28] J. S. Wejin, J. A. Badejo, O. Jonathan and F. Dahunsi, "A Brief Survey on the Experimental Application of MPQUIC Protocol in Data Communication," *2022 5th Information Technology for Education and Development (ITED)*, Abuja, Nigeria, 2022, pp. 1-8, doi: 10.1109/ITED56637.2022.10051479.

[29] Stewart, R., Tüxen, M., & Nielsen, K. (2022). RFC 9260: Stream Control Transmission Protocol. https://datatracker.ietf.org/doc/html/rfc9260

[30] Yuan, Y., Zhang, Z., Li, J., Shi, J., Zhou, J., Fang, G., & Dutkiewicz, E. (2010, April). Extension of SCTP for concurrent multi-path transfer with parallel subflows. In *2010 IEEE Wireless Communication and Networking Conference* (pp. 1-6). IEEE.

[31] Verma, L. P., Sharma, V. K., Kumar, M., Kanellopoulos, D., & Mahanti, A. (2022). DB-CMT: A new concurrent multi-path stream control transport protocol. *Journal of Network and Systems Management*, *30*(4), 67.

[32] S. Shailendra, R. Bhattacharjee and S. K. Bose, "MPSCTP: A Simple and Efficient Multipath Algorithm for SCTP," in *IEEE Communications Letters*, vol. 15, no. 10, pp. 1139-1141, October *2011, doi: 10.1109/LCOMM.2011.080811.110866.*

[33] Tomar, P., Kumar, G., Verma, L. P., Sharma, V. K., Kanellopoulos, D., Rawat, S. S., & Alotaibi, Y. (2022). Cmt-sctp and mptcp multipath transport protocols: A comprehensive review. Electronics, 11(15), 2384.

[34] Iyengar, J. R. (2006). End-to-end concurrent multipath transfer using transport layer multihoming. University of Delaware.

[35] Iyengar, J. R., Amer, P. D., & Stewart, R. (2006). Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths. IEEE/ACM Transactions on networking, 14(5), 951-964.

[36] Verma, L. P., Sharma, V. K., Kumar, M., Kanellopoulos, D., & Mahanti, A. (2022). DB-CMT: A new concurrent multi-path stream control transport protocol. *Journal of Network and Systems Management*, *30*(4), 67.

[37] Y. Yuan *et al*., "Extension of SCTP for Concurrent Multi-Path Transfer with Parallel Subflows," *2010 IEEE Wireless Communication and Networking Conference*, Sydney, NSW, Australia, 2010, pp. 1-6, doi: 10.1109/WCNC.2010.5506559.

[38] Dreibholz, T., "Evaluation and Optimisation of Multi-Path Transport using the Stream Control Transmission Protocol", Habilitation Treatise, 13 March 2012, https://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-29737/Dre2012_final.pdf

[39] https://multipath-dccp.org/intro.html

[40] https://datatracker.ietf.org/doc/html/draft-amend-tsvwg-multipath-framework-mpdccp-01

[41] https://datatracker-ietf-org.lucaspardue.com/doc/draft-ietf-tsvwg-multipath-dccp/

[42] https://datatracker.ietf.org/doc/draft-amend-tsvwg-multipath-framework-mpdccp/]

[43] Kandula, S., Lin, K. C. J., Badirkhanli, T., & Katabi, D. (2008, April). FatVAP: Aggregating AP Backhaul Capacity to Maximize Throughput. In *NSDI* (Vol. 8, pp. 89-104).

[44] K. G. Yalda, D. J. Hamad and N. Ţăpuş, "A survey on Software-defined Wide Area Network (SD-WAN) architectures," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-5, doi: 10.1109/HORA55278.2022.9799862.

[45] Rajagopalan, S. (2020, November). An Overview of SD-WAN Load Balancing for WAN Connections. In 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1-4). IEEE.

[46] Singh, A. K., & Srivastava, S. (2018). A survey and classification of controller placement problem in SDN. International Journal of Network Management, 28,

[47] https://www.mef.net/resources/mef-70-2-sd-wan-service-attributes-and-service-framework/

[48] Qadir, J., Ali, A., Yau, K. L. A., Sathiaseelan, A., & Crowcroft, J. (2015). Exploiting the power of multiplicity: a holistic survey of network-layer multipath. IEEE Communications Surveys & Tutorials, 17(4), 2176-2213.

[49] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in Proc. IEEE INFOCOM, 2003,vol. 1, pp. 270–280.

[50] P. Sambasivam, A. Murthy, and E. M. Belding-Royer, "Dynamically adaptive multipath routing based on AODV," in Proc. 3rd Annu. Mediterranean Ad Hoc Netw. Workshop, 2004, pp. 1–12

[51] J. Zhang, K. Xi and H. J. Chao, "Load Balancing in IP Networks Using Generalized Destination-Based Multipath Routing," in IEEE/ACM Transactions on Networking, vol. 23, no. 6, pp. 1959-1969, Dec. 2015, doi: 10.1109/TNET.2014.2348176.

[52] [Ste20.1-5] Sterca, A., Bufnea, D., & Niculescu, V. (2020, September). IP Multihoming Throughput Maximization based on Passive RTT Measurements. In 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-6). IEEE.

[53] A. Sterca, D. Bufnea and V. Niculescu, "Bandwidth Aggregation over Multihoming Links," 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020, pp. 1-7, doi: 10.1109/ISCC50000.2020.9219714.