International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2029

(06/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

A multi-path transmission control in multi-connection

Recommendation ITU-T Y.2029

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2029

A multi-path transmission control in multi-connection

Summary

The objective of Recommendation ITU-T Y.2029 is to describe the multi-path transmission control in multi-connection. This Recommendation also covers scenarios, requirements, mechanisms, information flows, and provides consideration to topics on security.

Multi-path transmission control is a mechanism in the multi-connection network, which is provided based on requirements, such as congestion control and traffic transmission adjustment, retransmission scheme, service flow separation, energy efficiency and management.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2029	2015-06-29	13	11.1002/1000/12510

Keywords

Multi-connection, multi-path, transmission control.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2029

A multi-path transmission control in multi-connection

1 Scope

This Recommendation describes the scenarios and requirements of multi-path transmission control in multi-connection and provides the mechanisms of multi-path transmission control. The descriptions cover aspects related to capability requirements, information flows and security.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection*.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[ITU-T Y.2027] Recommendation ITU-T Y.2027 (2012), *Functional architecture of Multi-connection Requirements*.

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and Capabilities for ITU-T NGN*.

[ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

[ITU-T Y.2251] Recommendation ITU-T Y.2251 (2011), *Multi-connection requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 multi-connection [ITU-T Y.2251]: The functionality which provides capability to the user equipment (UE) and network to maintain more than one access network connection simultaneously.

3.1.2 multi-connection user equipment [ITU-T Y.2027]: A user equipment which can support two or more network connections simultaneously under the control of a network enhanced for multi-connection capability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 multi-path connection: A set of one or more sub-transmission flows, over which the application in a multi-path transmission enhanced multi-connection user equipment can communicate with the corresponding application.

3.2.2 multi-path transmission enhanced multi-connection policy control function entity: A multi-connection policy control function entity [ITU-T Y.2027] with enhanced capabilities of multi-path transmission control within the transport layer.

3.2.3 multi-path transmission enhanced multi-connection user equipment: A multi-connection user equipment [ITU-T Y.2027] with enhanced capabilities of multi-path transmission control within the transport layer.

3.2.4 multi-path transmission enhanced service control function: A service control function [ITU-T Y.2027] with enhanced capabilities of multi-path transmission control within the transport layer.

3.2.5 path: The route taken by the multi-path transmission packets between two associated multi-path transmissions enhanced multi-connection user equipment. If the user equipment is not enhanced with multi-path transmission capability, the multi-path transmission enhanced service control function can be used as a proxy. A path can be uniquely identified by the associated IP addresses and port number pairs.

3.2.6 sub-transmission flow: A unidirectional logical channel established from one multi-path transmission enhanced multi-connection user equipment to another, which forms part of a larger multi-path connection.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACK	Acknowledgement
Cwnd	Congestion Window
ICV	Integrity Check Value
MPC-FE	Multi-connection Policy Control Function Entity
MPTCP	Multi-Path TCP
MPT-enhanced MPC-FE	Multi-Path Transmission enhanced Multi-connection Policy Control Function Entity
MPT-enhanced MUE	Multi-Path Transmission enhanced Multi-connection User Equipment
MPT-enhanced SCF	Multi-Path Transmission enhanced Service Control Function
MUE	Multi-connection User Equipment
PLR	Packet Loss Rate
QoS	Quality of Service
RTO	Retransmission Timeout
RTT	Round-Trip Time
SCF	Service Control Function
SCTP	Stream Control Transmission Protocol
SCTP-CMT	Stream Control Transmission Protocol-Concurrent Multi-path Transfer

SSThresh	Slow Start Threshold
UE	User Equipment
WLAN	Wireless Local Area Network

5 Conventions

In this Recommendation:

The keyword "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keyword "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keyword "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement is not present to claim conformance.

The keyword "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keyword "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Scenarios and requirements

6.1 Scenarios

The general scenarios in [b-ITU-T Y Suppl.9] are required to be taken into consideration in multi-path transmission control. Typical scenarios are derived based on scenario C of [b-ITU T Y Suppl.9] where a multi-connection user equipment (MUE) can establish multiple connections to heterogeneous access networks controlled by different access control functions, but the same service control function for a specific service. According to the relationship among the multiple service flows, these scenarios can be further classified into:

1) Scenario I

   In scenario I, an MUE establishes multiple connections to heterogeneous access networks, for example, in a video conference: voice is transmitted by 2G, 3G or long term evolution (LTE) to assure real-time service, and video is transmitted by wireless local area network (WLAN) which has higher bandwidth and may be cost efficient for a large number of network flows. In the transport layer, the flows can be transported in multiple paths.

   In this scenario, the multiple service data flows may have a native coupled relationship, but some mechanisms are required to guarantee the aggregation of the service. Cache and synchronization are the necessary mechanisms for service aggregation.

2) Scenario II

   In scenario II, an MUE is required for access to heterogeneous access networks simultaneously, such as 2G, 3G or WLAN. For example, to achieve greater bandwidth when downloading a multimedia file with a large volume of data, the MUE chooses a WLAN connection for download. When time is limited, to achieve a higher transmission rate, the multimedia file will be split and transferred to both the WLAN and 3G paths in the transport layer.

In this scenario, the multiple data flows are split and aggregation is simply based on the service separation policy and data scheduling mechanism.

6.2 Requirements

In [ITU-T Y.2251] IP flows are identified and bound to the proper connections. Because the connection status and service flows change dynamically, some connections may become overloaded and the lost data packets will be retransmitted frequently, thus reducing data transmission efficiency. Occasionally, data transmission through a single path cannot meet a user's service requirements such as real-time demand for large amounts of data. In multi-path transmission control, based on the requirements in [ITU-T Y.2251], the following requirements are to be considered:

1) Congestion control and traffic transmission adjustment

Congestion avoidance and reliability can be achieved directly at the transport layer. Changes in the congestion window (Cwnd) can reflect the degree of congestion on each path. As each path has its own features, it can avoid or relieve congestion occurrences using multi-path transmission. In multi-path transmission, the available paths can be treated as independent paths with independent congestion control decisions, or all the paths can be coupled to each other to perform congestion control.

As the total session Cwnd equals the Cwnd summation of each available path, it is required to consider balancing the rapid increase or decrease of the total Cwnd.

For example, Alice is connected to WLAN and 3G access networks. The WLAN access is used for web browsing, and the 3G access is used for downloading high definition movies. A voice call is received leading to congestion on the 3G path. To enhance the user experience, the download flow can be adjusted to go through the WLAN path.

2) Retransmission scheme

In multi-path transmission, there may be several available paths for retransmission. The continuous retransmission using the initial path may be inefficient. Therefore, the transmission may be enhanced using non-congested paths during the duration of the session.

If several non-congested paths are available, an appropriate path may be chosen according to the service. For example, a service requiring low delay is required to choose a minimum delay path, likewise a service requiring large throughput or low packet loss rate (PLR) is required to choose appropriate path(s). However, if the user is only capable of connecting with two access networks, retransmission can be done using the non-congested path.

In a dynamic scenario, if the user is connected to the WLAN and 3G access networks, and the services transmitted through WLAN retransmit frequently, the retransmission packets may be adjusted to utilize the 3G path.

3) Service flow separation

Just as a file can be split into a number of small file blocks, likewise a real-time service flow may be divided into several sub-transmission flows to be transmitted using different paths; these sub-transmission flows in turn may be reassembled into a complete service flow at the receiving end. Since the original numbered packets are separated and transmitted through multiple paths, the sub-transmission flow sequence numbers are required to be added to each sub-transmission flow. For example, in a certain path, a sub-transmission flow sequence number is used for transmission control, and a data sequence number is used for data recovery at the receiving end.

The simultaneous use of multiple paths in data transmission can enhance the overall bandwidth, and ensure a high transmission rate, low PLR and low transmission delay for a mobile user. And the sub-transmission flows can be transmitted through different paths for better quality of service (QoS) and achieving sharing resources.

For example, when a user is watching a high-definition video, several sub-transmission flows transmitting through different paths can improve the user experience. When the user is maintaining multiple connections and downloading a file with a large volume of data, to improve the transmission rate and to balance the data downloading, the data file can be separated and transmitted through several paths.

4) Energy efficiency and management

In the transport layer, congestion control and traffic transmission adjustment are related to the issue of energy consumption. According to the network performance and traffic load information (such as the Cwnd) of each path, policies to reduce energy consumption are required to be considered as well as in multi-path transmission control. If it is unnecessary to maintain too many paths, sub-transmission flows can be adjusted or transferred to fewer paths for energy savings, and the idle connections can be released.

For example, if a user listens to online music through 3G access and browses the web using WLAN, the audio stream can be adjusted to go through WLAN, and the 3G connection can be released to save energy.

7 A multi-path transmission mechanism

7.1 Overview

As described in [ITU-T Y.2027], an MUE can maintain more than one access network connection simultaneously. A multi-path transmission enhanced MUE (MPT-enhanced MUE) can distribute the service flows into different connections, based on the service requirements and the network conditions. The MPT-enhanced MUE may also divide a service flow into several sub-transmission flows and transmit them in different paths for higher aggregated bandwidth if necessary. Different IP addresses are configured by each access network, thus there exists one or several transmission paths simultaneously over a terminal device.

In order to avoid or relieve congestion in the multi-path transmission, specific congestion control mechanisms are required. Multi-path transmission control is required to take all paths' performance into account when a service flow is transmitted through several paths simultaneously in the NGN network. In addition, parallel transmissions through multiple paths removes the restriction of a single network not meeting the requirements of the high-bandwidth service. The packets of a service transmitted through multiple paths simultaneously may lead to out-of-order packets at the receiving end; packet scheduling is imperative for in-order delivery. At the same time, multi-path transmission control is required to take energy efficiency into consideration.

In the NGN network, users within the paths acting as direct initiators of the paths can obtain information about the end-to-end transmissions of current paths. The network can obtain and control the overall performance of the related accesses. Multi-path transmission control can be initiated by either the user side or the network side.

Connection information, access network performance parameters and policies are required to be sent to the related functional entity for performing multi-path transmission control. In order to complete the multi-path transmission control, the following enhancements are required to be supported in the multi-connection architecture:

1) MUE can optionally be enhanced for the multi-path transmission support, such as comprehensive path assessment, path status maintenance, adjustment decision and implementation (e.g., retransmission path selection, transmission rate adjustment, service separation/aggregation and sub-transmission flow mobility);

2) Multi-connection policy control function entity (MPC-FE) is required to support a specific multi-path transmission policy decision algorithm to provide adaptive decisions, such as decomposed service transmission adjustment and service separation decision. The MPC-FE

is required to provide the information and adjustment policies of the end hosts to the multi-path transmission proxy (i.e., service control function (SCF));

3) SCF is required to be enhanced as a multi-path transmission proxy to transparently provide multi-path capability to multi-path unaware hosts, such as the multi-path transmission traffic separation/aggregation and path status maintenance. It may interact with the MPT-enhanced MUE by the multi-path transmissions and interact with the MUE/user equipment (UE) by single-path transmissions when necessary.

The related functional entities are shown in Figure 7-1.

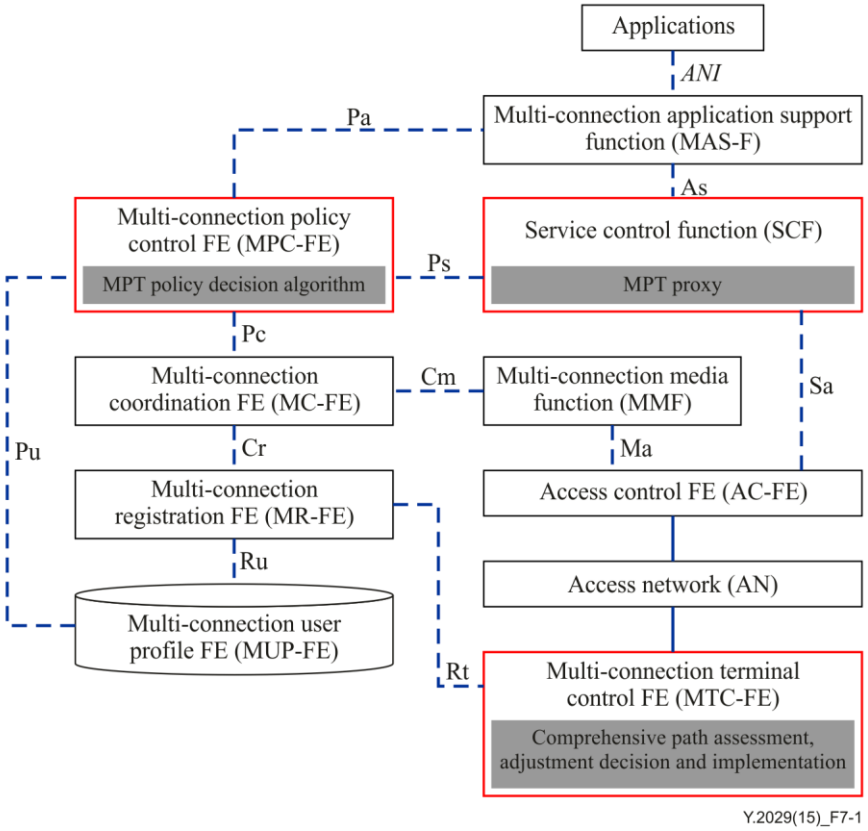

Figure 7-1 – Functional entities associated with multi-path transmission

A multi-path transmission adjustment policy may include the following information:

– access network ID related to the specific service;

– data transmission rate of each path for a specific service.

7.2 Initialization of the mechanism

7.2.1 A multi-path transmission control initiated by MPT-enhanced MUE

For congestion control and retransmission path selection, it is required to collect the congestion signals and network performance parameters. The signals and parameters are required to include, at least, the following information:

– congestion control parameters of each path used for comprehensive path evaluation, such as Cwnds, PLR, round-trip time (RTT) and slow start threshold (SSThresh);

– access type of each access network, which reflects the bandwidth, time delay, and reliability (i.e., QoS) level;

– total throughput and transmission rate of each sub-transmission flow.

In order to avoid or relieve congestion, the MPT-enhanced MUE can adjust the traffic according to specific policies installed in the MPT-enhanced MUE; the various path adjustment algorithms are transparent to the users.

7.2.2 A multi-path transmission control initiated by the network

It is required to collect the access network performance parameters and connection information and to facilitate the adjustment policy decision by the multi-path transmission enhanced multi-connection policy control function entity (MPT-enhanced MPC-FE). Afterwards, the updated policy can be sent to the multi-path transmission proxy (i.e., multi-path transmission enhanced service control function (MPT-enhanced SCF)) so that overall network performance improvement can be achieved.

The following metrics are used to evaluate the performance of access networks:

– network throughput;

– response time;

– network bandwidth capacity;

– PLR.

In addition, for the MUEs/UEs without multi-path transmission capability, network-based methods can be used to support the functionality.

7.3 Description of the mechanism

7.3.1 Packet delivery mechanism

In multi-path transmission, packets can be routed over multiple paths simultaneously to increase the network utilization by balancing the traffic load over the networks. Different numbers of packets from the same service may appear in different paths, and so the packet sequence number cannot be used for transmission control of each path. The multi-path transmission control is not only ensures in-order data delivery, but also guarantees the reliability of the path transmission.

In the multi-path transmission control, the following aspects of service flow separation are required to be considered:

1) In-order delivery

   To ensure in-order delivery, a connection level receive buffer is required to be maintained at the receiving end, where packets of a service are placed until they are in order and can be read by the application. Hence, a data sequence number is necessary for traffic aggregation. For instance, stream control transmission protocol (SCTP) uses stream sequence number (SSN), and multi-path TCP (MPTCP) uses connection-level sequence for in-order delivery.

2) Reliable delivery

   To ensure reliable delivery, multi-path transmission control is required to detect and retransmit any missed data, if necessary. In order to identify the packets on a specific path that may be retransmitted, a sub-transmission flow sequence number is necessary for reliable delivery. For instance, SCTP uses transmission sequence number (TSN), and MPTCP uses sub-transmission flow-level sequence number for reliable delivery.

7.3.2 Path selection and management mechanism

7.3.2.1 Path selection mechanism

Different types of services often have different requirements for transmission performance. Path selection is required to take both the performance parameters of each path (e.g., bandwidth, latency, reliability, energy consumption) and the services' requirements into consideration. MUEs with multi-path transmission capability can choose one or more paths for service transmission. In multi-path transmission control, path selection can be divided into the following two cases:

1) Select multi-path transmission

Generally, services with high bandwidth requirements can be split and routed over multiple paths simultaneously. A multi-path transmission can increase the network utilization by balancing the traffic load over the networks, which removes the restriction of a single network not satisfying the high bandwidth requirement.

For a service with high interactivity and small throughput, it would be preferable to use the lowest latency path to transfer traffic and retain one or more additional paths for resilience and fault recovery purposes. For other services, the reserved path can also be used to balance traffic load and traffic retransmission.

2) Select single-path transmission

If only a single specific path can meet the service requirements, it is unnecessary to split the service among several paths. In this case, although using multi-path to transfer the service packets can possibly improve throughput or accelerate the transmission speed, it may lead to operational complexity, high energy consumption or low resource utilization. Considering the processing overhead, if only a single path can meet the requirements of the service, parallel transmission is unnecessary.

A multi-path transmission can also be used for concurrent multi-service transmissions. For two concurrent download services, belonging to the same application or different applications, the traffic of each service can be transferred through different paths and do not have to be split. At the same time, the paths' energy consumption cannot be ignored for longer battery life. For energy savings, low energy consumption path(s) would be selected with higher priority.

7.3.2.2 Path management mechanism

A multi-path transmission control is required to have the abilities to automatically adjust the paths according to the current available paths' abilities and services requirements. For example, a path(s) is required to be added or deleted based on the received reachability state of destination transport addresses and service requirements. For energy savings, paths in multi-path transmission are required to be properly suspended or activated. At the same time, the mechanism of path failure detection and recovery is also essential.

In multi-path transmission, the following mechanisms are required to be considered:

1) Path update

In the communication process, path state is required to be updated in real time. There are many factors that can lead to path addition or deletion, such as the reachability state of destination transport addresses, service requirements and the possibility of unused path(s) with better performance than the current path(s) in use.

2) Path failure detection and recovery

Network failure may lead to path interruption or unavailability in a multi-path transmission. Hence, the mechanism of path failure detection and recovery is necessary in a multi-path transmission control. For instance, SCTP uses heartbeat messages to monitor the reachability of peer addresses, and judges whether the path has failed or not. The MPTCP sender will declare a path failed after a predefined upper bound on retransmissions is reached, or on the receipt of an ICMP error. If the predefined time installed for the failure path is exceeded, the failed path will be deleted. When a path has failed, the sub-transmission traffic transmitted on the failed path should be transferred to other paths.

3) Path suspending and path activation

If fewer paths meet the requirements of the services, part of the available paths can be kept in an idle state. In this case, a path suspending mechanism can save energy, since it can reduce the number of the transmission paths used simultaneously. When the used path(s) cannot

satisfy the requirements of the current service, a path activation mechanism to increase the available path(s) is required.

7.3.3 Congestion control and traffic transmission adjustment mechanism

7.3.3.1 Load balance mechanism with fairness consideration

In multi-path transmission control, MPT-enhanced MUE attaches to the Internet through several interfaces simultaneously for higher aggregated bandwidth, while MPT-enhanced MUE and MUE/UE share the network resources. Multi-path transmission improves the service experience, but it is required that the service using only a single-path for transmission dose not compromise the performance. The multi-path transmission is required to be fair to the existing single-path transmission.

To ensure fairness to a single-path transmission, multi-path transmission control is required to determine which sub-transmission flows share a point of congestion and which sub-transmission flows do not. Sub-transmission flows of a service that share a bottleneck link are required to be coupled for congestion control. In terms of the detection mechanism, the sender may inject probe packets as active detection techniques or employ application and/or transport data and acknowledgement (ACK) packets for measurement purposes as passive detection techniques. In addition, loss-based techniques rely on loss characteristics within and across sub-transmission flows as signals of congestion, and similarly, delay-based techniques use delay characteristics and changes within and across sub-transmission flows. The sub-transmission flows that share a common or separate bottleneck are required to be considered regarding which of the packets from these two flows are likely to be dropped or delayed in close time.

In contrast to single-path transmission, services can be separated and transmitted simultaneously so that the sub-transmission flows of a service transmitted through distinct paths are required to be coordinated. With the aid of multi-path transmission control, some of the traffic can be shifted from more congested paths to less congested ones, thus compensating for lost bandwidth on some paths by moderately increasing transmission rates on others. The congestion control mechanism of multi-path transmission is required to couple the paths in order to shift traffic from more congested to less congested paths, and thus standard TCP congestion control mechanisms are not applicable.

Therefore, alternate congestion control mechanisms are necessary, such as, fully coupled congestion control, coupled congestion control or semi-coupled congestion control, which take the sub-transmission flows of a service into consideration. In case of path loss, path failure detection is necessary, and the traffic on the failed path should be scheduled and transferred according to the available paths.

7.3.3.2 Throughput guarantee mechanism

In multi-path transmission, if the end-to-end delay and bottleneck bandwidth are not properly addressed, there may be many packets along multiple paths, which can arrive late and can lead to a large number of out-of-order packets at the receiver, and can eventually cause serious degradation to QoS.

In order to solve the above-mentioned problem, a buffer is required to be used to execute packet reordering at the receiver. At the same time, packet delivery order on each path is required to take both bandwidth aggregation and end-to-end delay into account in order to obtain the optimal transmission throughput. Several mechanisms can be used according to the available bandwidth and end-to-end delay on each path, such as the earliest delivery path first (EDPF) mechanism.

Duplicate ACKs or retransmission timeout (RTO) are two methods for triggering retransmission. The retransmission timer is adjusted dynamically, based on the measured RTTs. In multi-path transmission, packet reordering or other events that bring a sudden change of the RTT may lead to unnecessary retransmissions, which would cause the sender to wait a longer time for an

acknowledgment. In order to avoid unnecessary retransmission, RTO of a path is required to be calculated appropriately; refer to [b-IETF RFC 5682].

In standard TCP, every lost packet is recovered through retransmissions at the transport layer without coding techniques. In multi-path transmission, reliability can be achieved by introducing redundancy in the form of copies of each packet sent through multiple paths. However, network coding can recover original packets from receiving packets even if there is partial information loss in the packets. In addition, the application of network coding can improve network throughput, reduce energy consumption, reduce transmission delay, and the encoded data is secured in transmission. In general, network coding schemes can be divided into linear coding and nonlinear coding.

7.3.3.3 Efficient retransmission mechanism

In standard TCP, a single-path algorithm is adopted with traffic retransmission for packet loss. However, to ensure the delivery of packets on time with acceptable quality, there are several retransmission paths available other than the original one in multi-path transmission environment. In some cases, retransmission through the original path is inefficient, especially when the original path is in a state of high load. In multi-path transmission control, retransmission through the original path is not a strict constraint, and choosing the retransmission path mainly depends on the QoS requirements of the retransmission traffic.

If all available paths are uncongested, the retransmission traffic can be scheduled through the reserved path (e.g., RTX-SAME) or chose one retransmission path randomly (e.g., RTX-ASAP).

If the path is in a state of congestion, some indicators, such as the RTO occurs, are used to trigger the retransmission scheme. In multi-path transmission control, the following retransmission aspects are required to be considered:

– In order to ensure the timely delivery of retransmitted packets, retransmitted traffic from the sending end can be scheduled through a path that has Cwnd space available at that time (e.g., RTX-ASAP), or a path that has the largest Cwnd (e.g., RTX-CWND). In order to guarantee the reliable delivery of retransmitted packets, the minimum packet loss or retransmission path is required to be selected so that the retransmission traffic can be scheduled through the paths with the lowest PLR (e.g., RTX-LOSSRATE) or the largest SSThresh (e.g., RTX-SSTHRESH).
– The receiving end can choose the shortest RTT path or the path with the highest reliability for packet acknowledgement messages transmission. This may reduce the sending side's requirements for buffering, and prevent unnecessary retransmission from a different path.

8 Capability requirements

8.1 MPT-enhanced MUE requirements in the sending side

In order to highlight the benefits of multi-path transmission, the following capabilities are required for the MPT-enhanced MUE at the sending end:

1) identify and maintain all the paths' information, e.g., path failure detection;
2) provide service separation for bandwidth aggregation, if necessary;
3) properly select and timely adjust the path(s) for service transmission in a multi-path transmission control;
4) analyse the path performance parameters, e.g., PLR, RTT, SSThresh and the available bandwidth;
5) adjust the congestion control parameters of each path, e.g., Cwnd and RTO;
6) adopt an appropriate manner to improve the network transmission efficiency, e.g., network coding technology or retransmission policy;

7) address verification before adding a new path;

8) maintain the mapping information between a service and its path(s);

9) provide path failure detection and path recovery;

10) provide packet delivery mechanisms for service separation.

8.2 MPT-enhanced MUE requirements in the receiving side

In order to highlight the benefits of the multi-path transmission, the following capabilities are required for the MPT-enhanced MUE in the receiving end:

1) analyse the path performance parameters, e.g., PLR, RTT;

2) select an appropriate path for ACK transmission;

3) provide packet caching and reordering for the separated service and delivery to the upper layer;

4) provide network decoding and lost packet recovery if possible;

5) ensure data confidentiality and integrity verification;

6) maintain the mapping information between a service and its path(s);

7) provide packet delivery mechanisms for service aggregation.

8.3 MPT-enhanced MPC-FE requirements

In a multi-path transmission control initiated by the network, MPT-enhanced MPC-FE is responsible for making adjustment policy decisions by obtaining and analysing access network performance parameters and the capability of the corresponding end. The policy decision will be pushed to MPT-enhanced SCF to make the related MPT decisions periodically. The MPT-enhanced functions of the MPC-FE are as follows:

1) obtain the information of each access network's performance parameters (e.g., network throughput, response time, network bandwidth capacity and PLR) and determine the capability of the corresponding end (MPT-enhanced MUE, or not);

2) analyse the entire network status based on the information obtained above;

3) make MPT policy decisions based on the overall network performance;

4) push the overall network performance parameters to the related MPT-enhanced SCF periodically.

8.4 MPT-enhanced SCF requirements

In a multi-path transmission initiated by the network, the multi-path transmission proxy functions extended in SCF can transparently provide multi-path transmission capabilities to multi-path unaware hosts. Depending on the multi-path transmission capabilities of the sending end and the receiving end, MPT-enhanced SCF can act as a sender proxy or a receiver proxy to:

1) intercept the service request message for proxy initialization;

2) interact with the MPT-enhanced MPC for proxy decision;

3) act as a sender proxy to provide multi-path transmission capability in place of the sender;

4) act as a receiver proxy to provide multi-path transmission capability in place of the receiver;

5) accept the overall network performance parameters from the MPT-enhanced MPC periodically as a multi-path transmission proxy.

9 Information flow

9.1 Path selection mechanism

In a multi-path transmission, services with high bandwidth requirements can be routed over multiple paths simultaneously to increase the network utilization by balancing the traffic load over the networks, which removes the restriction of a single network not satisfying high bandwidth services. However, if only a single path can satisfy the service requirements, it is unnecessary to split the service into several paths, and the most appropriate path should be selected.

The path or paths selection is required to take the service requirements, the paths' performance and the paths' energy consumption into consideration, and the most appropriate path is required to be selected as described in [b-IETF RFC 6897] or [b-IETF RFC 4960]. In order to select the most appropriate path or paths, the status of each available path is required to be assessed and analysed.

To ensure the reliable, in-order delivery of a separated service, a connection level receive buffer is required to be maintained at the receiving end. A sequence of numbers to indicate connection level is necessary for traffic aggregation, and a sequence of numbers for sub-transmission flow is necessary for reliable delivery in order to identify the retransmission traffic of a specific path.

Path selection can be executed by the MPT-enhanced MUE or the network proxy entity (i.e., MPT-enhanced SCF which supports multi-path transmission proxy functions). The high-level information flow is described separately as follows.

9.1.1 Path selection mechanism initiated by MPT-enhanced MUE

Suppose that MUE_A is an MPT-enhanced MUE with two interfaces and is accessing the 3G (IF (1)) and WLAN (IF (2)) access networks simultaneously. Consider the example scenario where MPT-enhanced MUE_A initializes an FTP service request to establish the control connection with an FTP server through the 3G interface. In this scenario, the FTP server is MPT-enhanced MUE_B. After the establishment of control connection, MPT-enhanced MUE_A decides to establish two data transmission paths using the 3G path and the WLAN path.

The detailed information flow of this example scenario is shown in Figure 9-1.

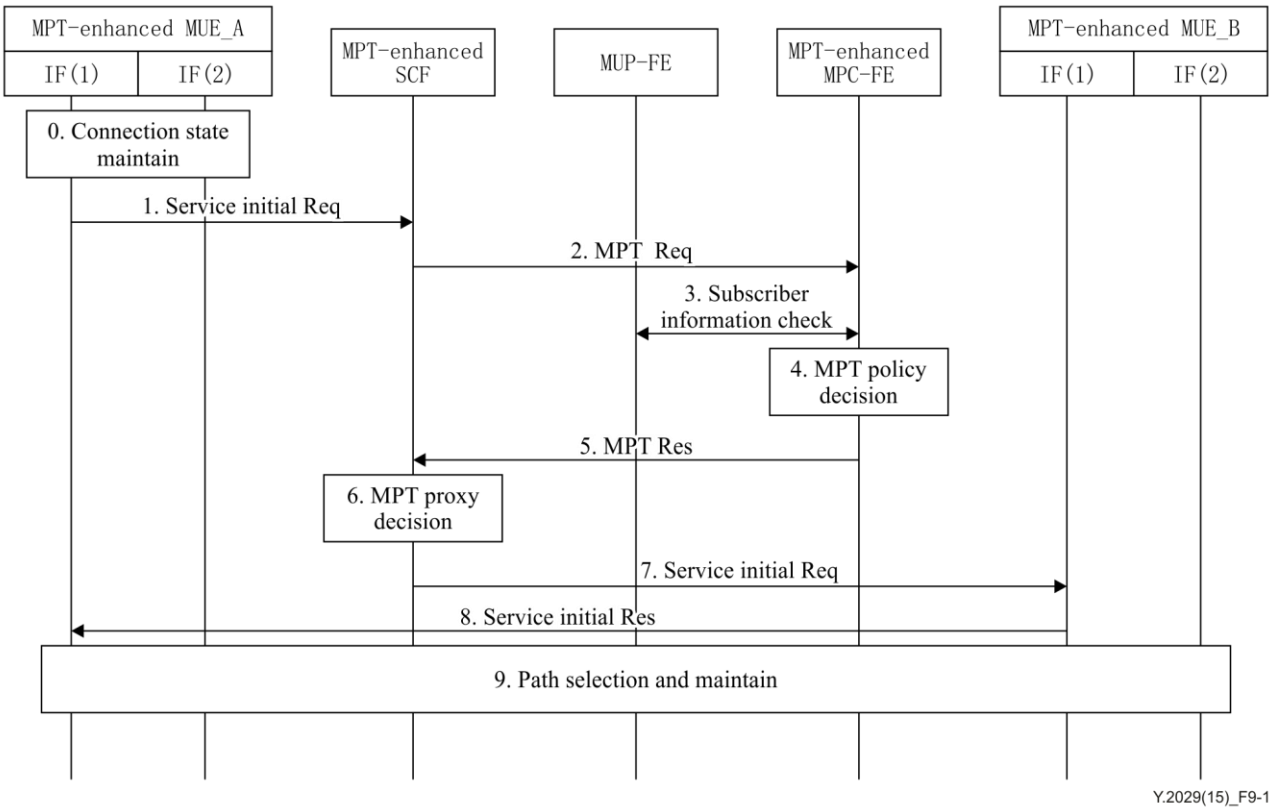

Figure 9-1 – Path selection procedure initiated by MPT-enhanced MUE

0) MPT-enhanced MUE_A maintains the connection status of each available access network for the incoming services;

1) MPT-enhanced MUE_A launches an FTP service request to MPT-enhanced MUE_B to establish an MPT connection. This service request will be intercepted by MPT-enhanced SCF of the corresponding node;

2) MPT-enhanced SCF initiates an MPT request to MPT-enhanced MPC-FE to query whether the corresponding node and corresponding networks' performance allow multi-path transmission;

3) after receiving the MPT request from MPT-enhanced SCF, MPT-enhanced MPC-FE obtains the profile information of the FTP server from MUP-FE and judges whether the FTP server is MPT enhanced;

4-5) MPT-enhanced MPC-FE makes MPT policy decisions, and returns an MPT responds message to the MPT-enhanced SCF indicating that the FTP server is an MPT-enhanced MUE and the corresponding networks' performance is able to support MPT;

6) as the FTP server can support the multi-path transmission, the MPT-enhanced SCF will not act as a multi-path transmission proxy for the FTP server;

7) MPT-enhanced SCF forwards the service initial request to the IF(1) of MPT-enhanced MUE_B;

8) MPT-enhanced MUE_B accepts the FTP service request and sends a service initial response message to the IF(1) of MPT-enhanced MUE_A;

9) after the establishment of control connection, MPT-enhanced MUE_A establishes two data transmission paths with MPT-enhanced MUE_B using the IF(1) and IF(2), respectively.

After the above steps, the download traffic would be separated to transmit through two paths according to the paths' performance, and the traffic transmitted through different paths will be aggregated and delivered to the upper layer at the receiving end.

9.1.2 Path selection mechanism initiated by the network proxy entity

Suppose that UE_A is unaware of multi-path transmission and accesses only the WLAN access network, in contrast to clause 9.1.1, and the FTP server (MUE_B) is an MPT-enhanced MUE. When UE_A initiates an FTP service to MPT-enhanced MUE_B, the MPT proxy of UE_A decides whether to initiate the MPT connection for UE_A based on the MPT support situation of corresponding node and network performance.

The detailed information flow of this example scenario is shown in Figure 9-2.

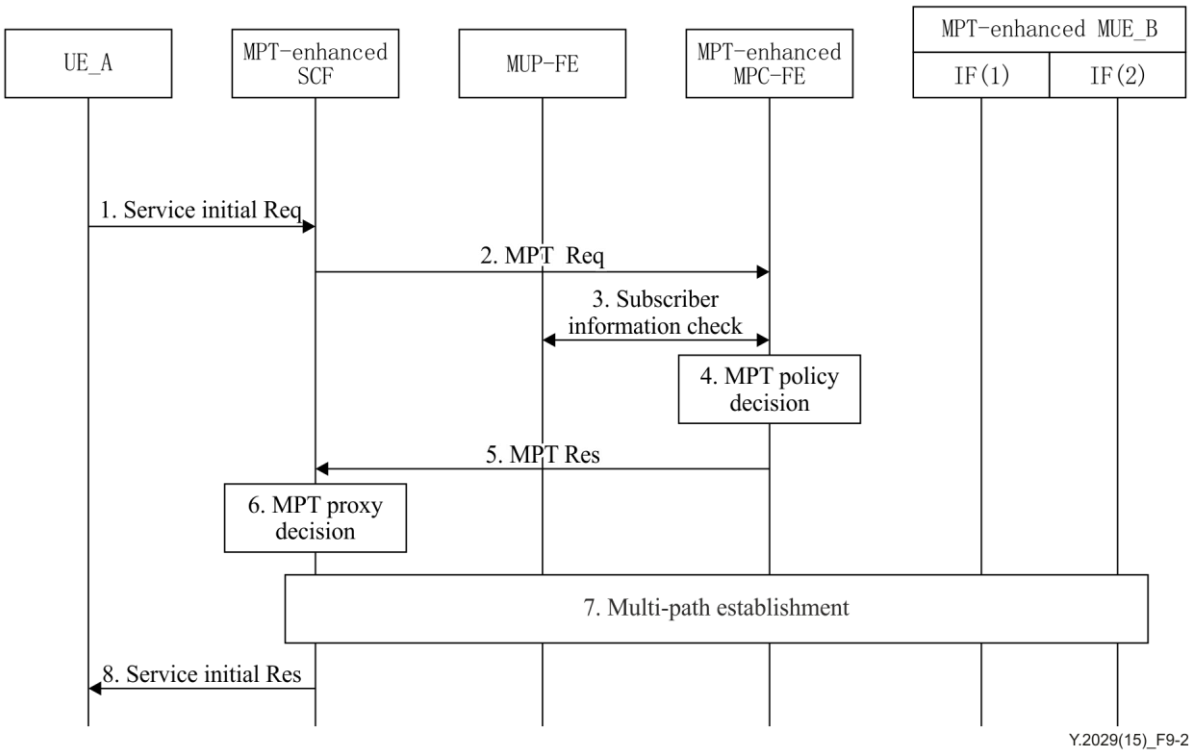

Figure 9-2 – Path selection procedure in network-based scenario

1-2) UE_A launches an FTP service request to an FTP server (MPT-enhanced MUE_B). MPT-enhanced SCF intercepts the service request and sends an MPT request to MPT-enhanced MPC-FE to decide whether to act as a proxy for UE_A;

3) after receiving the MPT request, MPT-enhanced MPC-FE obtains the profile information of the FTP server from MUP-FE and judges whether the FTP server, MUE_B, is MPT-enhanced. In this scenario, MUE_B is MPT-enhanced;

4-5) MPT-enhanced MPC-FE makes MPT policy decisions based on the overall network performance and the service requirements., It then forwards the policy to the MPT-enhanced SCF. During the process of data packets transmissions, MPT-enhanced MPC-FE pushes the parameters for network performance to the MPT-enhanced SCF periodically;

6) the MPT-enhanced SCF makes the MPT proxy decision to decide to act as an MPT proxy for the sending end;

7) MPT-enhanced SCF establishes two transmission paths with MPT-enhanced MUE_B instead of UE_A;

8) when the process of multi-path establishment has finished, MPT-enhanced SCF sends a service initial respond message to inform UE_A to communicate with MPT-enhanced MUE_B.

For UE_A, the multi-path transmission between MPT-enhanced SCF and MPT-enhanced MUE_B is transparent, but UE_A can enjoy the benefit of multi-path transmission control.

9.2 Traffic adjustment mechanism

In a multi-path transmission, the MPT-enhanced MUE and MUE/UE share the network resources. In contrast to single-path transmission, services with large bandwidth requirements can be separated for parallel transmission. It must be considered that the separated service is transmitted through distinct paths and should be coordinated based on a path scheduler algorithm, which may refer to [b-IETF RFC 6356] or [b-IETF RFC 4960].

In addition, there are several retransmission paths available rather than (just) the original one, i.e., single-path is less efficient, especially when the original path is under high load. According to the performance of each path available, retransmission traffic can be enhanced to transmit through a different path depending on the QoS requirements of the retransmission traffic. In order to avoid unnecessary retransmission, RTO of a path should be carefully calculated as described in [b-IETF RFC 5682].

Moreover, packet scheduling takes both bandwidth aggregation and end-to-end delay into account to obtain the optimal transmission throughput, and network coding can recover original packets from receiving packets even if partial information is lost in the packets. The application of packet scheduling and network coding can also improve the network throughput, reduce energy consumption and reduce transmission delay.

Traffic adjustment can be initiated by the MPT-enhanced MUE or the network (MPT-enhanced SCF as a multi-path transmission). The high level information flow is described separately as follows.

9.2.1 Traffic adjustment mechanism initiated by MPT-enhanced MUE

Suppose that MUE_A and MUE_B are both MPT-enhanced MUEs with two interfaces simultaneously accessing WLAN (IF (1)) and 3G (IF (2)) access networks. Consider the example scenario where MUE_A initiates a large file transfer service to MUE_B. To achieve a larger bandwidth for time savings, MUE_A splits the file transfer to go through both the WLAN path and the 3G path simultaneously.

After a period of time, the 3G path becomes congested due to the increased traffic load. MUE_A would then shift some of the traffic from the 3G path to the WLAN path, which is less congested based on the paths' performance parameters such as Cwnd and RTT. The traffic adjustment of each path is required to take path conditions into consideration in a fully coupled, coupled or semi-coupled way. At the same time, the packets transmitted by each path are required to be adjusted according to the available bandwidth and end-to-end delay of each path for in-order delivery. Thereafter, when detecting that data packets in WLAN path retransmit frequently, MUE_A could decide to adjust part of the retransmitted traffic to go through the 3G path for better retransmission efficiency.

The detailed information flow of this example scenario is shown in Figure 9-3.

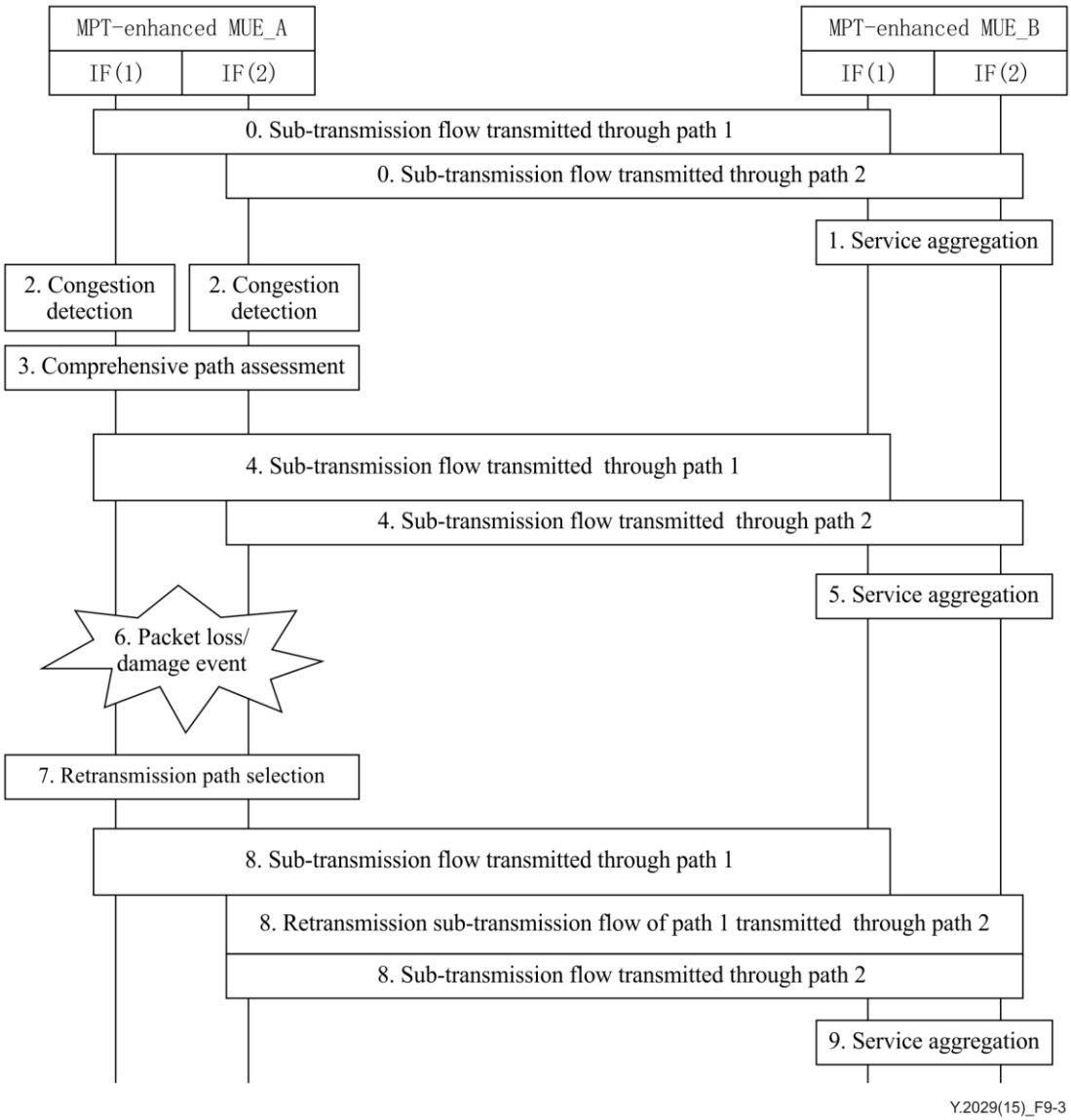

Figure 9-3 – Traffic adjustment procedure initiated by MPT-enhanced MUE

0-1) data packets of a large file are transferred from MPT-enhanced MUE_A to MPT-enhanced MUE_B through the WLAN path and the 3G path simultaneously for a larger aggregated bandwidth;

2) MUE_A collects and analyses path performance parameters of the WLAN path and the 3G path, and finds that the 3G path access becomes more congested;

3) MUE_A decides to shift some of the traffic from the 3G path to the WLAN path according the comprehensive path assessment;

4-5) after the above procedures, the WLAN path balances some traffic of the 3G path for resource optimization and timely delivery;

6) MUE_A detects the packet loss or damage event such as retransmission acknowledgment or the RTO occurs of the WLAN path;

7) MUE_A decides to adjust the retransmitted traffic to the 3G path for better retransmission efficiency based on a specific retransmission policy;

8-9) after the above procedures, MUE_A turns on the retransmission scheme. The service flow still transmits through the WLAN path, but part of the retransmitted traffic is adjusted to the 3G path. Data packets from the WLAN path and the 3G path are aggregated at the receiving end for upper layer delivery.

9.2.2 Traffic adjustment mechanism initiated by the network

Suppose that UE_A is an ordinary UE accessing only the WLAN access network, and MUE_B is an MPT-enhanced MUE with two interfaces simultaneously accessing to the WLAN (IF (1)) and 3G (IF (2)) access networks. Consider the example scenario where UE_A initiates a large file transfer service to MPT-enhanced MUE_B. To achieve a larger bandwidth for time savings, the MPT-enhanced SCF splits the file transfer to go through the WLAN path and the 3G path simultaneously to MPT-enhanced MUE_B on behalf of UE A.

During the transmission, MPT-enhanced SCF communicates with UE_A by single path but communicates with MPT-enhanced MUE_B by multi-path, simultaneously, as a multi-path transmission proxy for UE_A. If necessary, the MPT-enhanced MPC-FE may push the access networks' performance parameters to the MPT-enhanced SCF as the traffic adjustment reference periodically.

The detailed information flow of this example scenario is shown in Figure 9-4.

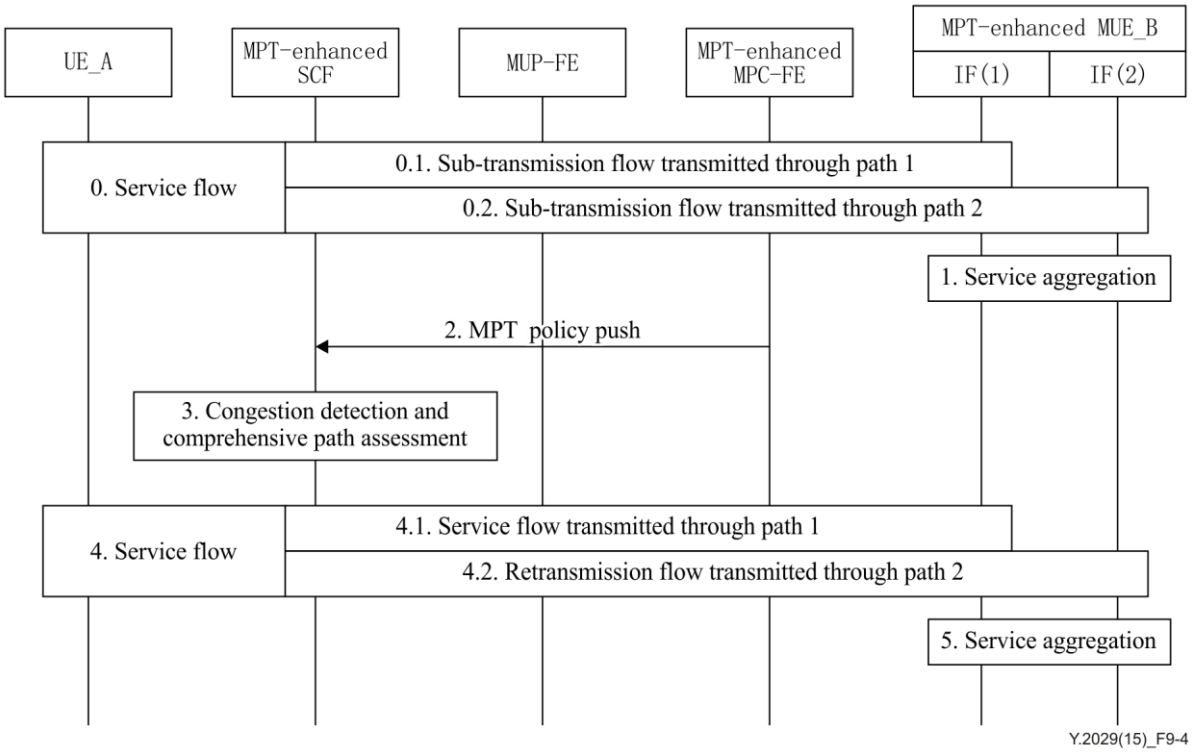

Figure 9-4 – Traffic adjustment procedure initiated by the network

0-1) data packets of a large file are transferred from UE_A to MPT-enhanced MUE_B through the WLAN path and the 3G path simultaneously for a larger aggregated bandwidth;

2) MPC-FE collects and analyses the access networks' performance parameters, and periodically pushes them to the MPT-enhanced SCF as the traffic adjustment reference when necessary;

3) MPT-enhanced SCF collects and analyses path performance parameters of the WLAN path and the 3G path on behalf of UE_A, and finds that the 3G path becomes more congested than earlier;

4-5) considering both path conditions and performances of each access network, the MPT-enhanced SCF adjusts the traffic transmission ratio of each, and the WLAN path balances some traffic of the 3G path.

10 Security considerations

10.1 Security requirement

10.1.1 General requirement

The security goal for MPT is to provide a service with greater security than regular single-path transmission. This is achieved through a combination of existing security mechanisms (potentially modified to align with the MPT) and of protection against identified new multipath threats. From the threat analysis and security goal of the MPT, three key security requirements can be identified. The MPT is required to do the following:

– provide a mechanism to confirm that the entities in an MPT control are the same as the original connection setup;

– provide verification that the peer can receive traffic at a new address being added;

– provide replay protection, i.e., ensure that a request to add/remove a sub-transmission flow is 'fresh'.

10.1.2 Authentication security

Authentication is the process that verifies the validity of some data attributes or entities and it is a basic security service that is required to be implemented whether in single-path transmission control or in multi-path transmission control. These services are provided for the authentication of a communication peer entity and a source of data as described below.

1) Peer entity authentication

   Peer entity authentication is used for validating the identities of one or more communication session entities of the same transport layer connection. It can be implemented at the initiation or the duration of a transport layer connection. Peer entity authentication can avoid, to a degree, the masquerade or unauthorized replay of a previous transport layer connection. A one-way/mutual peer entity authentication scheme with or without liveness checks can provide different protection levels. Peer entity authentication service is provided by an appropriate combination of cryptographically-derived or protected authentication exchanges, protected password exchanges and signature mechanisms.

2) Data origin authentication

   Data origin authentication provides the corroboration of the source of a data unit. The service can enable the data recipient of MPT to verify whether the incoming messages originated from a legitimate or specific MPT sender, so as to prevent a malicious attack that poses as a legitimate MPT sender and sends falsified massages. It can be also used for non-repudiation purposes, preventing the MPT sender from denying that it has performed a particular action related to data. But it cannot prevent duplication or modification of data units. This data origin authentication service can be provided by encryption protection or signature mechanism.

3) Access control

   Access control provides protection against unauthorized usage of resources that are accessible via the multi-path transmission model. This protection service may be applied to various or all types of access to a resource (e.g., the use of a communications resource; the reading, the writing, or the deletion of an information resource; the execution of a processing resource).

   The access control service can be provided through the appropriate use of specific access control mechanisms, such as one based on access control information where the access rights of peer MPT-enhanced MUE are maintained, or one where security labels bound to a resource may be used to grant or deny access. In order to determine and enforce the access rights of

an MPT user entity, these mechanisms may use the authenticated identity or capabilities of the entity, or information about the entity (such as membership in a known set of entities). If the MPT user entity attempts to use an unauthorized resource or use an authorized resource with an improper type of access, the access control function rejects the attempts and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail.

10.1.3 Data security

In traditional single-path transmission control, data security mainly includes data confidentiality and data integrity. To provide a service with higher security than regular single-path transmission, data security is required to be considered in multi-path transmission control. Data security is used to protect data from malicious attacks, such as: intercept, unauthorized disclosure, duplication, modification. The data security is described in detail in this clause.

1) Data confidentiality

Data confidentiality protects data from unauthorized disclosure. Some private data are of great importance in a multi-path transmission model, such as addresses of an MPT-enhanced MUE or other attribute information of one or more transport paths. Once they are disclosed, it results in security threats such as identity imitation of attackers or data falsification and modification. Therefore, data confidentiality mechanisms are necessary. Encryption is an important method to provide data confidentiality. It ensures that only the session entity with the correct key can read the data. Encryption algorithms such as DES and RSA can be deployed optionally. Enforcing file permissions and the use of access control lists to restrict access to sensitive data also contribute to data confidentiality.

2) Data integrity

Data integrity aims to maintain the consistency, accuracy, and trustworthiness of data over their entire life cycle. It ensures that data have not been altered or destroyed in an unauthorized or undetected manner. Since data are sensitive to modification, it is necessary to ensure data integrity. For example, modification or destruction of the signaling data used for path control may lead to unpredictable communication consequences.

Data integrity can be provided by integrity check value (ICV) processing. ICV processing may be used to detect unauthorized modification of MPT user data and security control information while the data is in transit between communicating transport entities. Hashing algorithms such as MD5 and SHA1 can also be used for checking data integrity.

10.2 Attack defence

10.2.1 Flooding attacks

Flooding attacks, also known as bombing attacks, mean that with the help of a third party, an MPT-enhanced MUE transmits large amounts of data to the target. Flooding attacks send a large amount of data which exceeds the service ability of the victim, consumes the limited resources of available to the victim, such as network bandwidth, CPU processing power, memory and network connections, and which result in the denial of service of the victim.

Before launching an attack, the attacker initiates a session to a source, S, and establishes the first path from S. The attacker then starts downloading a great amount of traffic from source S. Next, the attacker impersonates the victim and sends a signalling packet conveying the address of the victim to establish another path belonging to the existing transport layer connection with S. Now, two paths have been established between the attacker and the victim. In this case, one path is actually between S and the attacker, and the other path is between S and the victim. However, source S believes that the two paths are both between itself and the attacker.

After completing the above, the attacker can send some mendacious information to notify S to transmit traffic to the victim through the path between the attacker and the victim.

If the attacker can successfully make the attack, source S falsely transmits a large amount of traffic to the victim. The amount of traffic is often beyond the resources available to the victim and results in the victim suffering a serious attack. In this process, source S always thinks that it is sending data to the attacker.

For the victim, some countermeasures can be taken to avoid this type of attack. When receiving packets from an unknown path, the victim can issue reset (RST) packets to the peer MPT node, which is the source of these packets. RST packets can interrupt the multi-path transmission connection. Thus, after source S receives the RST packets, it terminates the data transmission to the victim, or at least it can reduce the number of data transmissions. Therefore, to a certain degree, this method can prevent the flooding attacks.

In addition, to deal with this type of attack, reachability should be checked before the MPT sender sends data through a new path of an existing multi-path transmission connection. In this solution, before transmitting packets, the source S sends a request message to ask if the victim is willing to accept packets from the path identified by source S's own IP address and the victim's IP address. Since there is no such path belonging to the victim, the victim would reject the request from source S. Source S then would not to send packets to the victim. These and other methods can prevent the flooding attacks described in this clause.

10.2.2 Hijacking attacks

Hijacking attacks occur when an attacker takes over a path belonging to the multi-path transmission connection between a victim and its peer node, and then intercepts the packets from the victim.

Before a hijack attack begins, a multi-path transmission connection is established between the victim and the peer. After the attacker learns the 4-tuple that identifies the transport layer connection between the victim and its peer, the attacker poses as the peer but uses its own IP address to establish another path with the victim. After completing this step, the attacker is naturally participating in the communication between the victim and the peer. When the victim transmits data packets through the two paths, perhaps not all, but at least part of the packets from the victim are sent to the attacker.

In the communication process, the victim of the hijacked path believes that it is sending data packets to its peer; it is in fact communicating with the attacker and the peer simultaneously. At the same time, the peer does not receive all of the packets sent by the victim, which may lead to some negative effects. For example, this may result in a denial of service (DoS) attack since the partial data sent to the peer will stop waiting for the missing data sent to the attacker. The following are some available approaches for preventing hijacking attacks to a degree.

1) Cookie-based solution

   During the establishment of the first path between the victim and its peer, a cookie can be agreed on by each party. This cookie is added in every control packet used to establish other paths in the future. In order to initiate hijacking attacks, the attackers must obtain the cookie. Thus the cookie-based approach prevents off-path attackers from launching hijacking attacks; it cannot prohibit on-path attackers.

2) Shared secret exchanged in plain text

   This protection process is similar to that of the cookie-based approach, but is more secure. The difference is the exchange of a key in plaintext during the establishment of the first path. Subsequent establishment requests of other paths again validate the new path by using a keyed hashed message authentication code (HMAC) signature using the shared key. Since the shared key only transmits during the establishment of the first path, attackers that sniff (record) packets after the first path has already been established would not successfully launch an attack. However, for attackers sniffing or modifying the messages exchanged

during the establishment of the first path, this solution can hardly provide effective protection.

3) Strong crypto anchor exchange

To achieve more effective protection, in this approach, the communication endpoints would exchange some strong crypto anchor, other than a key in plaintext, while establishing the first path. A public key or a hash-chain anchor can be the strong crypto anchor. After the communication endpoints agree on the anchor, they can exchange packets which are encrypted by the shared crypto anchor through the first path. Actually, if the attacker wants to launch a hijacking attack, it would be necessary to change the crypto anchor exchanged in the path establishment phase. But, if the endpoints communicate directly, the modify operations can be detectable.

Bibliography

[b-ITU-T Y Suppl.9] ITU-T Y-series Recommendations – Suppl.9 (2010), *ITU-T Y.2000-series – Supplement on multi-connection scenarios*.

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[b-IETF RFC 5682] IETF RFC 5682 (2009), *Forward RTO-Recovery (F-RTO) : An Algorithm for Detecting Spurious Retransmission Timeouts with TCP*.

[b-IETF RFC 6356] IETF RFC 6356 (2011), *Coupled Congestion Control for Multipath Transport Protocols.*

[b-IETF RFC 6897] IETF RFC 6897 (2013), *Multipath TCP (MPTCP) Application Interface Considerations*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015