

INTAREA
Internet Draft
Intended status: Standards Track
Expires: September 4,2020

J. Zhu
Intel
S. Seo
Korea Telecom
S. Kanugovi
Nokia
S. Peng
Huawei
March 4, 2020

User-Plane Protocols for Multiple Access Management Service
draft-zhu-intarea-mams-user-protocol-09

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on September 4,2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in

Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Abstract

Today, a device can be simultaneously connected to multiple communication networks based on different technology implementations and network architectures like WiFi, LTE, and DSL. In such multi-connectivity scenario, it is desirable to combine multiple access networks or select the best one to improve quality of experience for a user and improve overall network utilization and efficiency. This document presents the u-plane protocols for a multi access management services (MAMS) framework that can be used to flexibly select the combination of uplink and downlink access and core network paths having the optimal performance, and user plane treatment for improving network utilization and efficiency and enhanced quality of experience for user applications.

Table of Contents

1.	Introduction.....	3
2.	Terminologies.....	3
3.	Conventions used in this document.....	3
4	MAMS User-Plane Protocols.....	4
4.1	MX Adaptation Sublayer.....	4
4.2	GMA-based MX Convergence Sublayer.....	5
4.3	MPTCP-based MX Convergence Sublayer.....	6
4.4	GRE as MX Convergence Sublayer.....	6
4.4.1	Transmitter Procedures.....	7
4.4.2	Receiver Procedures.....	8
4.5	MX Adaptation and Convergence Co-existence.....	8
5.	MX Convergence Control Message.....	8
5.1	Keep-Alive Message.....	9
5.2	Probe Message.....	9
5.3	Acknowledgement (ACK) Message.....	10
5.4	Packet Loss Report (PLR) Message.....	10
5.5	First Sequence Number (FSN) Message.....	11
5.6	Coding Coefficient Update (CCU) Message.....	12
5.7	Coded MX SDU (CMS) Message.....	13
5.8	Traffic Splitting Update (TSU) Message.....	14
5.9	Traffic Splitting Acknowledgement (TSA) Message.....	14

6	Security Considerations.....	15
7	IANA Considerations.....	15
8	Contributing Authors.....	16
9	References.....	16
9.1	Normative References.....	16
9.2	Informative References.....	16

[1](#). Introduction

Multi Access Management Service (MAMS) [[MAMS](#)] is a programmable framework to select and configure network paths, as well as adapt to dynamic network conditions, when multiple network connections can serve a client device. It is based on principles of user plane interworking that enables the solution to be deployed as an overlay without impacting the underlying networks.

This document presents the u-plane protocols for enabling the MAMS framework. It co-exists and complements the existing protocols by providing a way to negotiate and configure the protocols based on client and network capabilities. Further it allows exchange of network state information and leveraging network intelligence to optimize the performance of such protocols. An important goal for MAMS is to ensure that there is minimal or no dependency on the actual access technology of the participating links. This allows the scheme to be scalable for addition of newer access technologies and for independent evolution of the existing access technologies.

[2](#). Terminologies

Anchor Connection: refers to the network path from the N-MADP to the Application Server that corresponds to a specific IP anchor that has assigned an IP address to the client.

Delivery Connection: refers to the network path from the N-MADP to the C-MADP.

"Network Connection Manager" (NCM), "Client Connection Manager" (CCM), "Network Multi Access Data Proxy" (N-MADP), and "Client Multi Access Data Proxy" (C-MADP) in this document are to be interpreted as described in [[MAMS](#)].

[3](#). Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

The terminologies "Network Connection Manager" (NCM), "Client Connection Manager" (CCM), "Network Multi Access Data Proxy" (N-MADP), and "Client Multi Access Data Proxy" (C-MADP) in this document are to be interpreted as described in [[MAMS](#)].

4 MAMS User-Plane Protocols

Figure 1 shows the MAMS u-plane protocol stack as specified in [[MAMS](#)].

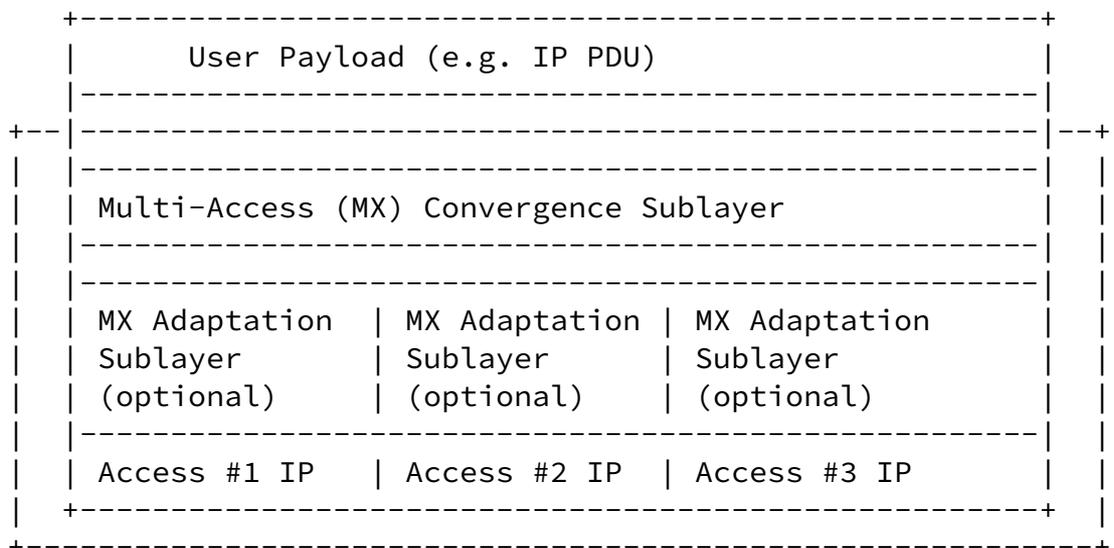


Figure 1: MAMS U-plane Protocol Stack

It consists of the following two Sublayers:

- o Multi-Access (MX) Convergence Sublayer: This layer performs multi-access specific tasks, e.g., access (path) selection, multi-link (path) aggregation, splitting/reordering, lossless switching, fragmentation, concatenation, keep-alive, and probing etc.
- o Multi-Access (MX) Adaptation Sublayer: This layer performs functions to handle tunneling, network layer security, and NAT.

The MX convergence sublayer operates on top of the MX adaptation sublayer in the protocol stack. From the Transmitter perspective, a User Payload (e.g. IP PDU) is processed by the convergence sublayer first, and then by

the adaptation sublayer before being transported over a delivery access connection; from the Receiver perspective, an IP packet received over a delivery connection is processed by the MX adaptation sublayer first, and then by the MX convergence sublayer.

[4.1](#) MX Adaptation Sublayer

The MX adaptation sublayer supports the following mechanisms and protocols while transmitting user plane packets on the network path:

- o UDP Tunneling: The user plane packets of the anchor connection can be encapsulated in a UDP tunnel of a delivery connection between the N-MADP and C-MADP.

Zhu

Expires September 4, 2020

[Page 4]

Internet-Draft

MAMS u-plane protocols

March 2020

- o IPsec Tunneling: The user plane packets of the anchor connection are sent through an IPsec tunnel of a delivery connection.
- o Client Net Address Translation (NAT): The Client IP address of user plane packet of the anchor connection is changed, and sent over a delivery connection.
- o Pass Through: The user plane packets are passing through without any change over the anchor connection.

The MX adaptation sublayer also supports the following mechanisms and protocols to ensure security of user plane packets over the network path.

- o IPsec Tunneling: An IPsec [[RFC7296](#)] tunnel is established between the N-MADP and C-MADP on the network path that is considered untrusted.
- o DTLS: If UDP tunneling is used on the network path that is considered "untrusted", DTLS (Datagram Transport Layer Security) [[RFC6347](#)] can be used.

The Client NAT method is the most efficient due to no tunneling overhead. It SHOULD be used if a delivery connection is "trusted" and without NAT function on the path.

The UDP or IPsec Tunneling method SHOULD be used if a delivery connection has a NAT function placed on the path.

[4.2](#) GMA-based MX Convergence Sublayer

Figure 2 shows the MAMS u-plane protocol stack based on trailer-based encapsulation [[GMA](#)]. Multiple access networks are combined into a

single IP connection. If NCM determines that N-MADP is to be instantiated with GMA as the MX Convergence Protocol, it exchanges the support of GMA convergence capability in the discovery and capability exchange procedures [[MAMS](#)].

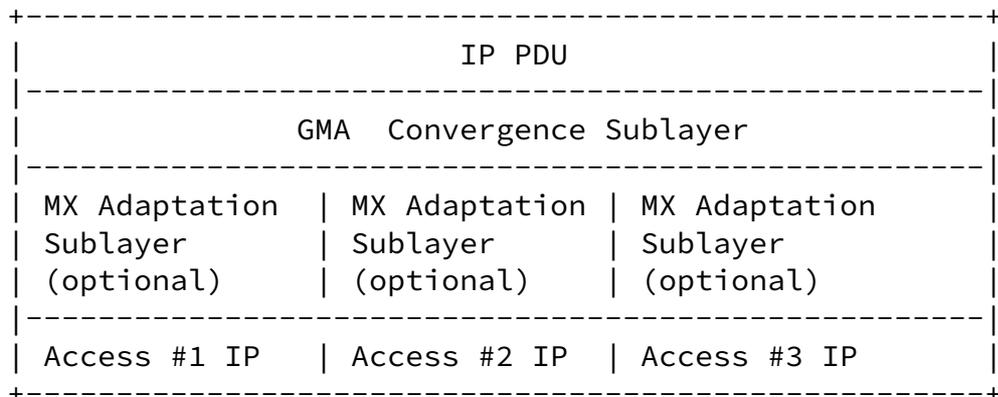


Figure 2: MAMS U-plane Protocol Stack with GMA as MX Convergence Layer

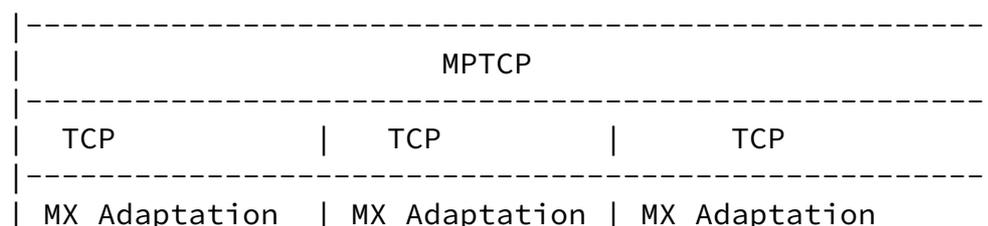
Figure 3 shows the trailer-based Multi-Access (MX) PDU (Protocol Data Unit) format [[GMA](#)]. If the MX adaptation method is UDP tunneling and "MX header optimization" in the "MX_UP_Setup_Configuration_Request" message [[MAMS](#)] is true, the "IP length" and "IP checksum" header fields of the MX PDU SHOULD remain unchanged. Otherwise, they should be updated after adding or removing the GMA trailer in the convergence sublayer.



Figure 3: GMA PDU Format

[4.3](#) MPTCP-based MX Convergence Sublayer

Figure 4 shows the MAMS u-plane protocol stack based on MPTCP. Here, MPTCP is reused as the "MX Convergence Sublayer" protocol. Multiple access networks are combined into a single MPTCP connection. Hence, no new u-plane protocol or PDU format is needed in this case.



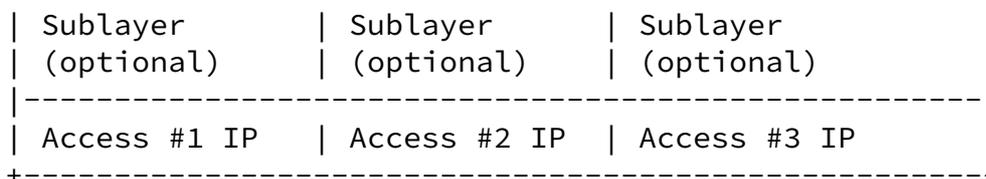


Figure 4: MAMS U-plane Protocol Stack with MPTCP as MX Convergence Layer

If NCM determines that N-MADP is to be instantiated with MPTCP as the MX Convergence Protocol, it exchanges the support of MPTCP capability in the discovery and capability exchange procedures [MAMS]. MPTCP proxy protocols [MPProxy][MPPlain] SHOULD be used to manage traffic steering and aggregation over multiple delivery connections.

4.4 GRE as MX Convergence Sublayer

Figure 5 shows the MAMS u-plane protocol stack based on GRE (Generic Routing Encapsulation) [GRE2784]. Here, GRE is reused as the "MX Convergence sub-layer" protocol. Multiple access networks are combined

into a single GRE connection. Hence, no new u-plane protocol or PDU format is needed in this case.

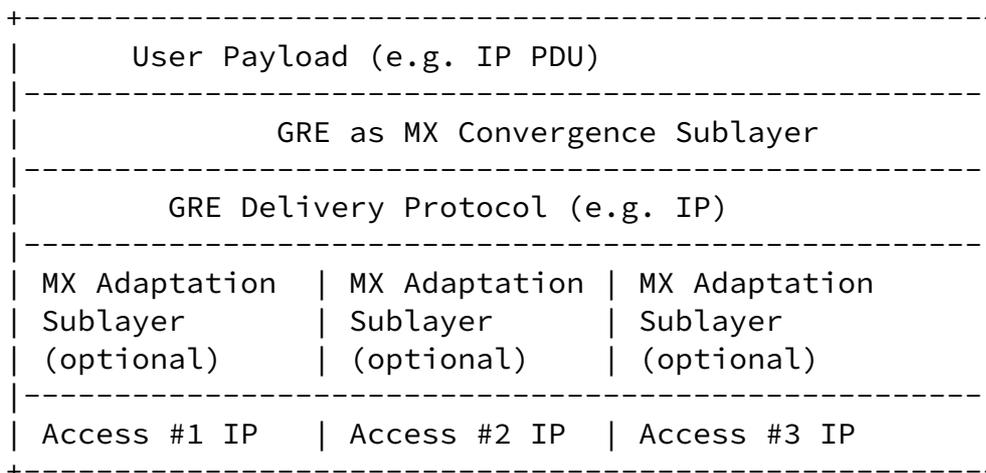


Figure 5: MAMS U-plane Protocol Stack with GRE as MX Convergence Layer

If NCM determines that N-MADP is to be instantiated with GRE as the MX Convergence Protocol, it exchanges the support of GRE capability in the

discovery and capability exchange procedures [[MAMS](#)].

[4.4.1](#) Transmitter Procedures

Transmitter is the N-MADP or C-MADP instance, instantiated with GRE as the convergence protocol that transmits the GRE packets. The Transmitter receives the User Payload (e.g. IP PDU), encapsulates it with a GRE header and Delivery Protocol (e.g. IP) header to generate the GRE Convergence PDU.

When IP is used as the GRE delivery protocol, the IP header information (e.g. IP address) can be created using the IP header of the user payload or a virtual IP address. The "Protocol Type" field of the delivery header is set to 47 (or 0X2F, i.e. GRE)[[IANA](#)].

The GRE header fields are set as specified below,

- If the transmitter is a C-MADP instance, then sets the LSB 16 bits to the value of Connection ID for the Anchor Connection associated with the user payload or sets to 0xFFFF if no Anchor Connection ID needs to be specified.
- All other fields in the GRE header including the remaining bits in the key fields are set as per [[GRE_2784](#)][[GRE_2890](#)].

[4.4.2](#) Receiver Procedures

Receiver is the N-MADP or C-MADP instance, instantiated with GRE as the convergence protocol that receives the GRE packets. The receiver processes the received packets per the GRE procedures [[GRE_2784](#), [GRE_2890](#)] and retrieves the GRE header.

- If the Receiver is an N-MADP instance,
 - o Unless the LSB 16 Bits of the Key field are 0xFFFF, they are interpreted as the Connection ID of Anchor Connection for the user payload. This is used to identify the network path over which the User Payload (GRE Payload) is to be transmitted.
- All other fields in the GRE header, including the remaining bits in the Key fields, are processed as per [[GRE_2784](#)][[GRE_2890](#)].

The GRE Convergence PDU is passed onto the MX Adaptation Layer (if present) before delivery over one of the network paths.

4.5 MX Adaptation and Convergence Co-existence

MAMS u-plane protocols support multiple combinations and instances of user plane protocols to be used in the MX Adaptation and the Convergence sublayers.

For example, one instance of the MX Convergence Layer can be MPTCP Proxy [[MPProxy](#)][MPPlain] and another instance can be Trailer-based. The MX Adaptation for each can be either UDP tunnel or IPsec. IPsec may be set up for network paths considered as untrusted by the operator, to protect the TCP subflow between client and MPTCP proxy traversing that network path.

Each of the instances of MAMS user plane, i.e. combination of MX Convergence and MX Adaptation layer protocols, can coexist simultaneously and independently handle different traffic types.

5. MX Convergence Control Message

A UDP connection may be configured between C-MADP and N-MADP to exchange control messages for keep-alive or path quality estimation. The N-MADP end-point IP address and UDP port number of the UDP connection is used to identify MX control PDU. A MX control PDU consists of the following fields:

- o Type (1 Byte): the MX control message type
- o CID (1 Byte): an unsigned integer to identify the anchor and delivery connection of the MX control message
 - + Anchor Connection ID (MSB 4 Bits): an unsigned integer to identify the anchor connection

Zhu

Expires September 4, 2020

[Page 8]

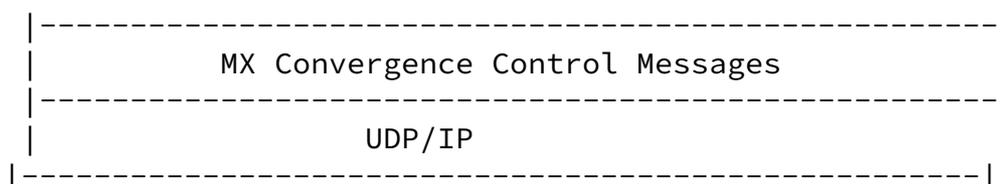
Internet-Draft

MAMS u-plane protocols

March 2020

- + Delivery Connection ID (LSB 4 Bits): an unsigned integer to identify the delivery connection
- o MX Control Message (variable): the payload of the MX control message

Figure 6 shows the MX convergence control protocol stack, and MX control PDU goes through the MX sublayers the same way as MX data PDU.



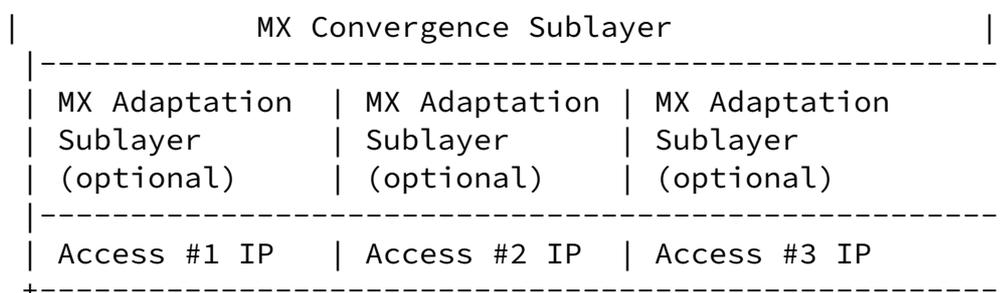


Figure 6: MX Convergence Control Protocol Stack

5.1 Keep-Alive Message

The "Type" field is set to "0" for Keep-Alive messages. C-MADP may send out Keep-Alive message periodically over one or multiple delivery connections, especially if UDP tunneling is used as the adaptation method for the delivery connection with a NAT function on the path.

A Keep-Alive message is 6 Bytes long, and consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the keep-alive message
- o Timestamp (4 Bytes): the current value of the timestamp clock of the sender in the unit of 100 microseconds.

5.2 Probe Message

The "Type" field is set to "1" for Probe messages.

N-MADP may send out the Probe message for path quality estimation. In response, C-MADP may send back the ACK message.

A Probe message consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the Probe REQ message
- o Probing Flag (1 Byte):
 - + Bit #0: a ACK flag to indicate if the ACK message is expected (1) or not (0);
 - + Bit #1: a Probe Type flag to indicate if the Probe message is sent during the initialization phase (0) when the network path is not included for transmission of user data or the active

phase (1) when the network path is included for transmission of user data;

- + Bit #2~7: reserved
- o Reverse Connection ID (1 Byte): the connection ID of the delivery connection for sending out the ACK message on the reverse path
- o Timestamp (4 Bytes): the current value of the timestamp clock of the sender in the unit of 100 microseconds.
- o Padding (variable)

The "R-CID" field is valid only if Bit #0 of the "Probing Flag" field is set to "1". If the "R-CID" field is set to all "1"s, the ACK message SHOULD be sent over the same delivery connection as the Probe message.

The "Padding" field is used to control the length of Probe message.

[5.3](#) Acknowledgement (ACK) Message

The "Type" field is set to "2" for ACK messages. The ACK message consists of the following fields:

- o Acknowledgment Number (2 Bytes): the sequence number of the received message.
- o Timestamp (4 Bytes): the current value of the timestamp clock of the sender in the unit of 100 microseconds.

[5.4](#) Packet Loss Report (PLR) Message

The "Type" field is set to "3" for PLR messages.

C-MADP may send out the PLR messages to report lost MX SDU for example during handover. In response, C-MADP may retransmit the lost MX SDU accordingly.

A PLR message consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the PLR message
- o Flow ID (1 Byte): an unsigned integer to identify the traffic flow;
- o ACK number (4 Bytes): the next (in-order) sequence number (SN) that the sender of the PLR message is expecting

- o Number of Loss Bursts (1 Byte)
 - For each loss burst, include the following
 - + Sequence Number of the first lost MX SDU in a burst (4 Bytes)

+ Number of consecutive lost MX SDUs in the burst (1 Byte)

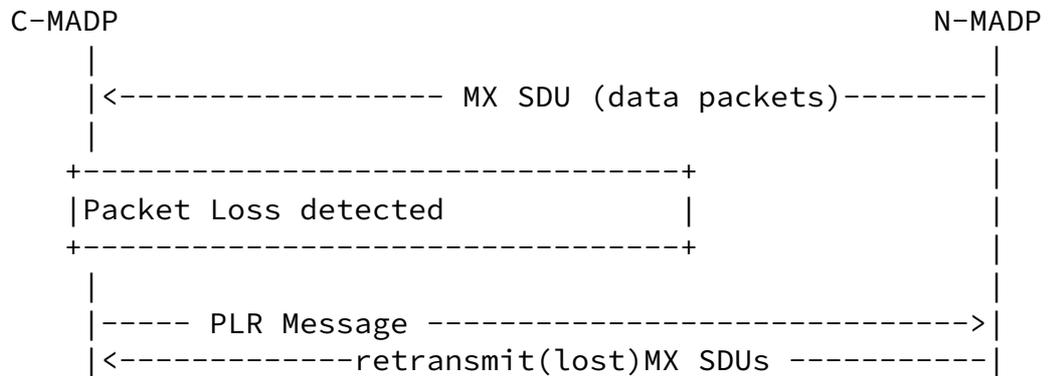


Figure 7: MAMS Retransmission Procedure

Figure 7 shows the MAMS retransmission procedure in an example where the lost packet is found and retransmitted.

5.5 First Sequence Number (FSN) Message

The "Type" field is set to "4" for FSN messages.

N-MADP may send out the FSN messages to indicate the oldest MX SDU in its buffer if a lost MX SDU is not found in the buffer after receiving the PLR message from C-MADP. In response, C-MADP SHALL only report packet loss with SN not smaller than FSN.

A FSN message consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the FSN message
- o Flow ID (1 Byte): an unsigned integer to identify the traffic flow;
- o First Sequence Number (4 Bytes): the sequence number (SN) of the oldest MX SDU in the (retransmission) buffer of the sender of the FSN message.

Figure 8 shows the MAMS retransmission procedure in an example where the lost packet is not found.



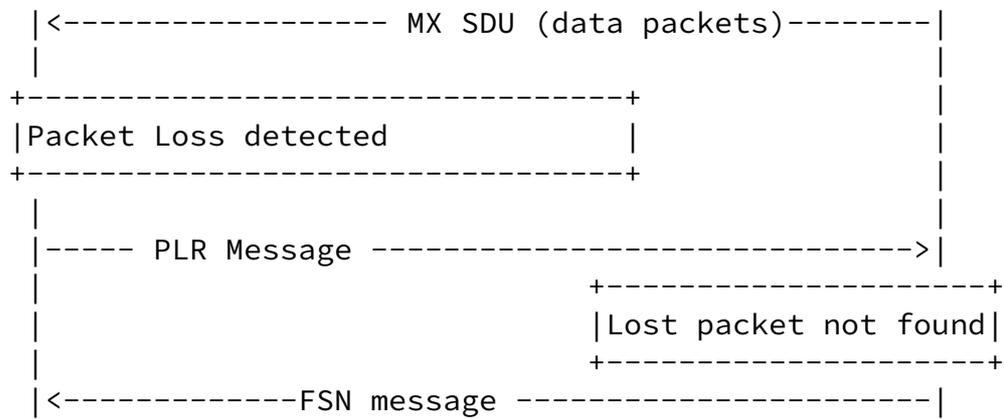


Figure 8: MAMS Retransmission Procedure with FSN

5.6 Coding Coefficient Update (CCU) Message

The "Type" field is set to "5" for CCU messages.

N-MADP (or C-MADP) may send out the CCU message to support downlink (or uplink) packet loss recovery through coding, e.g. [CRLNC], [CTCP], [RLNC]. In response, C-MADP (or N-MADP) SHALL send out the ACK message to indicate the successful reception. A CCU message consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the CCU message
- o Flow ID (1 Byte): an unsigned integer to identify the traffic flow
- o Fragmentation Control (FC) (1 Byte): to provide necessary information for re-assembly
 - + Bit #7: a More Fragment (MF) flag to indicate if the fragment is the last one (0) or not (1)
 - + Bit #0~#6: Fragment Offset (in units of fragments) to specify the offset of a particular fragment relative to the beginning of the SDU
- o Type (1 Byte): the coding coefficient generation method type
 - + 0: none (if XOR is used for coding)
 - + 1: deterministic
 - + 2: random
 - + Others: reserved
- o L (1 Bytes): the length of coding coefficient (in Bytes), included only if "Type" is 1 or 2
- o K (4 Bytes): the total number of coding coefficients, included only if "Type" is 1
- o Coding Coefficients (K x L Bytes): the list of coding coefficients, included only if "Type" is 1
- o Random Seed (8 Bytes): the random seed to generate coding coefficients, included only if "Type" is 2

If the CCU message is too long, it can be fragmented and transported by multiple MX control PDUs. Only the first MX control PDU carries Type, K, and L.

[5.7](#) Coded MX SDU (CMS) Message

The "Type" field is set to "6" for CMS messages.

N-MADP (or C-MADP) may send out the CMS message to support downlink (or uplink) packet loss recovery through coding, e.g. [[CRLNC](#)], [[CTCP](#)], [[RLNC](#)]. A coded MX SDU is generated by applying a network coding algorithm to multiple consecutive (uncoded) MX SDUs, and it is used for fast recovery without retransmission if any of the MX SDUs is lost.

A Coded MX SDU message consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the CMS message
- o Flow ID (1 Byte): an unsigned integer to identify the traffic flow
- o Flag (1 Byte)
 - + Bit #0: to indicate if the CMS message uses the same set of coding coefficients as its previous CMS message or not. This bit is flipped whenever a new set of coding coefficients is used
 - + Bit #1: to indicate if the FC field is present or not
 - + Bit #2: to indicate if the SDU-SN field is present or not
 - + Bit #3: to indicate if the K field is present or not
 - + Bit #4~7: reserved
- o Fragmentation Control (FC) (1 Byte): to provide necessary information for re-assembly
 - + Bit #7: a More Fragment (MF) flag to indicate if the fragment is the last one (0) or not (1)
 - + Bit #0~#6: Fragment Offset (in units of fragments) to specify the offset of a particular fragment relative to the beginning of the SDU
- o SDU-SN (4 Bytes): the sequence number of the first (uncoded) MX SDU used to generate the coded MX SDU
- o K (4 Bytes): with linear network coding, this field indicates the coding coefficient index for the first MX SDU; with XOR, this field is not included.
- o N (1 Byte): the number of consecutive MX SDUs used to generate the coded MX SDU
- o Coded MX SDU (variable): the coded MX SDU

If the CMS message is too long, it can be fragmented and transported by multiple MX control PDUs. SDU-SN, N and K are only included in the MX PDU carrying the first fragment of the coded MX SDU.

Internet-Draft

MAMS u-plane protocols

March 2020

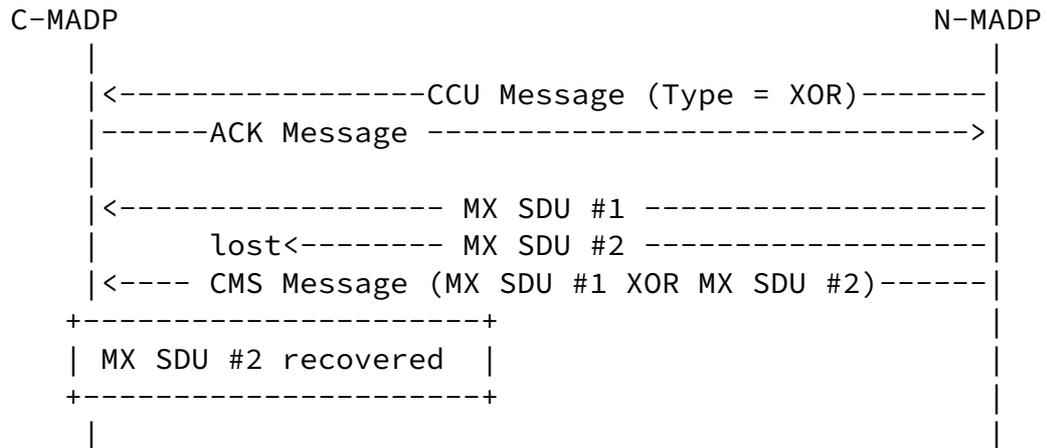


Figure 9: MAMS Packet Recovery Procedure with XOR Coding

[5.8](#) Traffic Splitting Update (TSU) Message

The "Type" field is set to "7" for TSU messages.

N-MADP (or C-MADP) may send out a TSU message to change the traffic splitting configuration of the reverse path.

A TSU message consists of the following fields:

- o Sequence Number (2 Bytes): the sequence number of the TSU message;
- o Flow ID (1 Byte): an unsigned integer to identify the flow;
- o N (1 Byte): number of delivery connections;
- o Traffic Splitting Parameters (N Bytes): the traffic splitting threshold $K(i)$ of the i -th delivery connection, where connections are ordered according to their Connection ID, where $i=1, 2, \dots, N$, and N is the number of delivery connections.

Let's use $f(x)$ to denote the traffic splitting function, which maps a MX SDU Sequence Number "x" to the i -th delivery connection, and $f(x)$ MAY be given by

$$f(x)=i, \text{ if } K[i-1] \cdot \text{mod}(x - \text{StartSN}, K[N]) < K[i]$$

Wherein, $i=1,2,\dots,N$ and $K[0]=0$. Please refer to 5.9 for the definition of "StartSN".

[5.9](#) Traffic Splitting Acknowledgement (TSA) Message

The "Type" field is set to "8" for TSA messages. N-MADP (or C-MADP) SHALL send out a TSC message in response to a received TSU message. A TSA message consists of the following fields:

- o SN Number (2 Bytes): the sequence number of the corresponding TSU message;
- o StartSN (4 Bytes): the sequence number of the first MX SDU using the traffic splitting configuration provided by the corresponding TSU message.

Figure 10 shows the traffic splitting update procedure for downlink traffic, where C-MADP performs path quality measurement based on received packets and determines traffic splitting parameters. Once update is needed, C-MADP will send the TSU message carrying the new traffic splitting parameters to N-MADP. N-MADP will send back the TSA message in response, and perform traffic splitting accordingly. The TSA message carries the "StartSN" parameter to indicate the first packet using the new configuration so that C-MADP can perform measurements accordingly.

For uplink traffic, N-MADP performs measurements, determines traffic splitting parameters, and sends out the TSU message. C-MADP sends back the TSA message and performs traffic splitting.

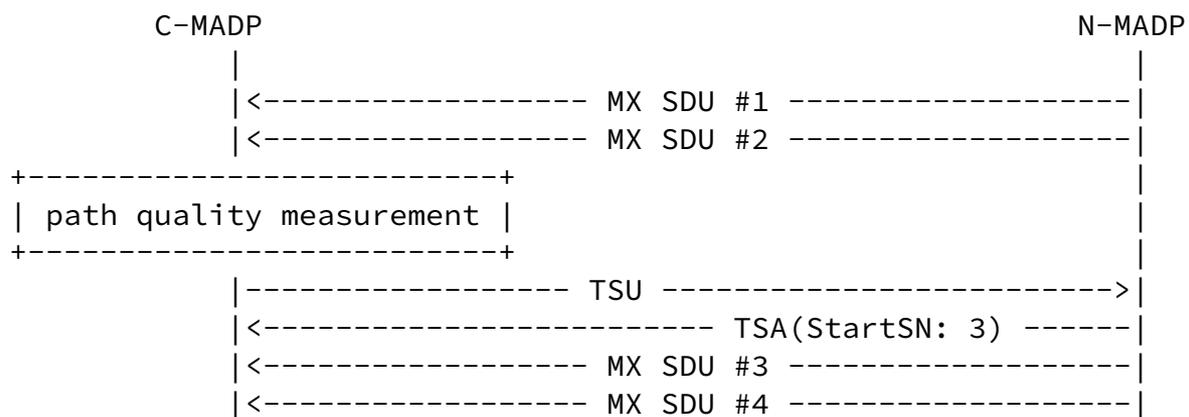


Figure 10: Downlink Traffic Splitting Update Procedure

6 Security Considerations

User data in MAMS framework rely on the security of the underlying network transport paths. When this cannot be assumed, NCM configures use of appropriate protocols for security, e.g. IPsec [[RFC4301](#)] [[RFC3948](#)], DTLS [[RFC6347](#)].

[7](#) IANA Considerations

This draft makes no requests of IANA.

Zhu

Expires September 4, 2020

[Page 15]

Internet-Draft

MAMS u-plane protocols

March 2020

[8](#) Contributing Authors

The editors gratefully acknowledge the following additional contributors in alphabetical order: Salil Agarwal/Nokia, Wei Mao/Intel, Hema Pentakota/Nokia, and Menglei Zhang/Intel.

[9](#) References

[9.1](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.

[9.2](#) Informative References

- [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), January 2012, <<http://www.rfc-editor.org/info/rfc6347>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](#), DOI 10.17487/RFC7296, October 2014, <<http://www.rfc-editor.org/info/rfc7296>>.
- [RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", [RFC 3948](#), DOI 10.17487/RFC3948, January 2005, <<http://www.rfc-editor.org/info/rfc3948>>.
- [MPProxy] X. Wei, C. Xiong, and E. Lopez, "MPTCP proxy mechanisms", <https://tools.ietf.org/html/draft-wei-mptcp-proxy-mechanism-02>

[MPPlain] M. Boucadair et al, "An MPTCP Option for Network-Assisted MPTCP", <https://www.ietf.org/id/draft-boucadair-mptcp-plain-mode-09.txt>

[MAMS] S. Kanugovi, S. Vasudevan, F. Baboescu, and J. Zhu, "Multiple Access Management Protocol", <https://tools.ietf.org/html/draft-kanugovi-intarea-mams-protocol-03>

Zhu

Expires September 4, 2020

[Page 16]

Internet-Draft

MAMS u-plane protocols

March 2020

[GMA] J. Zhu, "Trailer-based Encapsulation Protocols for Generic Multi-Access Convergence", <https://tools.ietf.org/html/draft-zhu-intarea-gma-01>

[GRE2784] D. Farinacci, et al., "Generic Routing Encapsulation (GRE)", [RFC 2784](https://www.rfc-editor.org/info/rfc2784) March 2000, <<http://www.rfc-editor.org/info/rfc2784>>.

[GRE2890] G. Dommety, "Key and Sequence Number Extensions to GRE", [RFC 2890](https://www.rfc-editor.org/info/rfc2890) September 2000, <<http://www.rfc-editor.org/info/rfc2890>>.

[IANA] <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>

[LWIPEP] 3GPP TS 36.361, "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE-WLAN Radio Level Integration Using Isec Tunnel (LWIP) encapsulation; Protocol specification"

[RFC791] Internet Protocol, September 1981

[CRLNC] S Wunderlich, F Gabriel, S Pandi, et al. Caterpillar RLNC (CRLNC): A Practical Finite Sliding Window RLNC Approach, IEEE Access, 2017

[CTCP] M. Kim, et al. Network Coded TCP (CTCP), eprint arXiv:1212.2291, 2012

[RLNC] J. Heide, et al. Random Linear Network Coding (RLNC)-Based Symbol Representation, <https://www.ietf.org/id/draft-heide-nwcrp-rlnc-00.txt>

Authors' Addresses

Jing Zhu

Intel

Email: jing.z.zhu@intel.com

SungHoon Seo

Korea Telecom

Email: sh.seo@kt.com

Satish Kanugovi

Zhu

Expires September 4, 2020

[Page 17]

Internet-Draft

MAMS u-plane protocols

March 2020

Nokia

Email: satish.k@nokia.com

Shuping Peng

Huawei

Email: pengshuping@huawei.com

