INTAREA
Internet Draft
Intended status: Standards Track
Expires: September 27, 2017
March 27, 2017
J. Zhu
Intel
S. Seo
Korea Telecom

User-Plane Protocols for Multiple Access Management Service
draft-zhu-intarea-mams-user-protocol-01

Status of this Memo

Copyright Notice

Abstract

Today, a device can be simultaneously connected to multiple communication networks based on different technology implementations and network architectures like WiFi, LTE, 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 best combination of uplink and downlink access and core network paths, and user plane treatment for improving network efficiency and enhanced application quality of experience.

Table of Contents

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 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 accesses and for independent technology evolution of the existing accesses.

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 client.

"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_CP].

```
             +-----------------------------------------------------+
             |      User Payload (e.g. IP PDU)                     |
             |-----------------------------------------------------|
          +--|-----------------------------------------------------|--+
          |  |-----------------------------------------------------|  |
          |  | Multi-Access (MX) Convergence Sublayer              |  |
          |  |-----------------------------------------------------|  |
          |  |-----------------------------------------------------|  |
          |  | MX Adaptation   | MX Adaptation | MX Adaptation     |  |
          |  | Sublayer        | Sublayer      | Sublayer          |  |
          |  | (optional)      | (optional)    | (optional)        |  |
          |  |-----------------------------------------------------|  |
          |  | Access #1 IP    | Access #2 IP  | Access #3 IP      |  |
```

```
          |  +-------------------------------------------------------+  |
          +-------------------------------------------------------------+
                 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, etc.
o Multi-Access (MX) Adaptation Sublayer: This layer performs functions to handle tunnelling, network layer security, and NAT.

4.1 MX Adaptation Layer

The MX adaptation layer 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.
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): change the Client IP address of user plane packet of the anchor connection, and send it over a delivery connection.
o Pass Through: The user plane packets are passing through without any change over the anchor connection.

The MX adaptation layer 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 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 Tunnelling method SHOULD be used if a delivery connection has a NAT function on the path.

4.2 Trailer-based MX Convergence Layer

Trailer based MX convergence integrates multiple connections into a single e2e IP connection. It operates between Layer 2 (L2) and Layer 3 (network/IP).

```
<-------- MX PDU Payload ---------------->
+--------------------------------------------------------+
| IP (v4 or v6) header |  IP payload     | MX Trailer  |
+--------------------------------------------------------+
```

Figure 2: Trailer-based Multi-Access (MX) PDU Format

Figure 2 shows the trailer-based Multi-Access (MX) PDU (Protocol Data Unit) format. A MX PDU MAY carry multiple IP PDUs in the payload if concatenation is supported, and MAY carry a fragment of the IP PDU if fragmentation is supported.

The MX trailer may consist of the following fields:

- o Next Header (e.g. 1 byte): the IP protocol type of the (first) IP packet in a MX PDU
- o Connection ID (e.g.1 byte): an unsigned integer to identify the anchor connection of the IP packets in a MX PDU
- o Traffic Class ID (e.g. 1 byte): an unsigned integer to identify the traffic class of the IP packets in a MX PDU, for example Data Radio Bearer (DRB) ID for a cellular connection
- o Sequence Number (e.g. 2 bytes): an auto-incremented integer to indicate order of transmission of the IP packet, needed for lossless switching or multi-link (path) aggregation.
- o Packet Length (e.g. 2 bytes): the length of the first IP packet, only included if a MX PDU contains multiple IP packets, i.e. concatenation
- o Fragmentation Control (e.g. 1 Byte): to provide necessary information for re-assembly, only needed if a MX PDU carries fragments, i.e. fragmentation
  - o Bit #7: a More Fragment (MF) flag to indicate if the fragment is the last one or not
  - o Bit #0~#6: Fragment Offset (in units of fragments) to specify the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram

Moreover, the following fields of the IP header of the MX PDU are changed as follows:

o Protocol Type: "114" to indicate that the presence of MX trailer (i.e. the trailer based MAMS u-plane protocol is a "0-hop" protocol, not subject to IP routing)

o IP length: add the length of "MX Trailer" to the length of the original IP packet
o IP checksum: recalculate after changing "Protocol Type" and "IP Length"

The MX u-plane protocol can support multiple Anchor connections simultaneously, each of which is uniquely identified by Connection ID. It can also support multiple traffic classes per connection, each of which is identified by Traffic Class ID.

Moreover, the MX trailer format MAY be negotiated dynamically between NCM and CCM. For example, NCM can send a control message to indicate which of the above fields SHOULD be included for individual delivery connection, on downlink and uplink, respectively.

4.3 MPTCP-based MX Convergence Layer

TBD

4.4 Co-existence of MX Adaptation and MX Convergence Layers

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

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 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 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 protocols, like IPsec [RFC4301] [RFC3948], for security.

6 IANA Considerations

TBD

7 Contributing Authors

The editors gratefully acknowledge the following additional contributors in alphabetical order: Hema Pentakota/Nokia, Satish Kanugovi/Nokia.

8 References

8.1 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>.

8.2 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

[MAMS_CP] S. Kanugovi, et al., "Control Plane Protocols and Procedures for Multiple Access Management Services"

Authors' Addresses

Jing Zhu

Intel

Email: jing.z.zhu@intel.com

SungHoon Seo

Korea Telecom

Email: sh.seo@kt.com