IPPM
Internet-Draft
Intended status: Standards Track
Expires: 3 January 2026

G. Fioccola
T. Zhou
Huawei
Y. Zhu
W. Zhang
China Telecom
K. Zhu
Huawei Technologies

2 July 2025

On-Path Telemetry YANG Data Model
draft-ietf-ippm-on-path-telemetry-yang-01

Abstract

This document proposes a YANG data model for monitoring On-Path network performance information to be published in YANG notifications. The Alternate-Marking Method and In-situ Operations, Administration, and Maintenance (IOAM) are the On-Path hybrid measurement methods considered in this document.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 3 January 2026.

Copyright Notice

Table of Contents

1. Introduction

Alternate-Marking Method [RFC9341] [RFC9342] (AltMark) is a technique used to perform packet loss, delay, and jitter measurements on in-flight packets. In-situ Operations, Administration, and Maintenance (IOAM) is a method to produce operational and telemetry information that may be exported using the in-band or out-of-band method. The data types and data formats for IOAM data records have been defined in [RFC9197] [RFC9326].

This document defines a YANG data model for monitoring On-Path telemetry information of Alternate Marking Method and IOAM. It provides YANG data models with performance monitoring parameters that can be subscribed to for monitoring and telemetry via YANG-Push specified in [RFC8639], [RFC8640] and [RFC8641].

This document uses the existing mechanisms of [RFC9341], [RFC9342], [RFC9197], [RFC9326] to monitor the performance of the network and connectivity services.

Section 3 includes the tree diagram, while Section 5 includes the data model. Also, an example is reported in Appendix A.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Conventions

The following terms are defined in [RFC7950] and are used in this specification:

* augment

* data model

* data node

The terminology for describing YANG data models is found in [RFC7950].

2. Use Case

Some applications may use the subscription model specified in [RFC8641] to subscribe to the On-Path telemetry network performance data. For example, Network Telemetry [RFC9232] updates may be subscribed to YANG-Push on-change notifications [RFC8641] for state changes. YANG-Push periodic notifications [RFC8641] can be subscribed to obtain real-time performance data.

There is a need for real-time traffic monitoring of the network to optimize the network performance. The next figure shows an example of a high-level workflow for dynamic network control based on traffic monitoring that could use the mechanism described in this document.

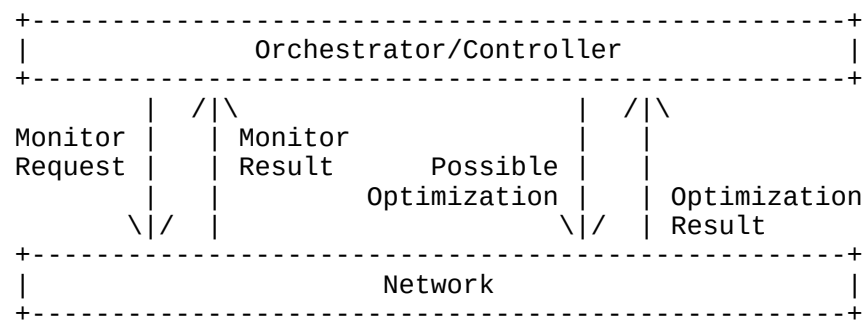

Figure 1: Workflow for dynamic network control based on traffic monitoring

The Controller sends a Monitor Request and receive Monitor Result. Because of this Closed-Loop approach, the controller can take Optimization actions, that can be related to forwarding path modification or performance measurements variation ([I-D.ietf-ippm-alt-mark-yang]), as also described in [RFC9342] with regard to the flexible and adaptive performance measurements.

3. On-Path Telemetry Tree Diagram

Tree diagrams used in this document follow the notation defined in [RFC8340].

The On-Path Telemetry model is organized as shown in the following figure. This model complements the AltMark model in [I-D.ietf-ippm-alt-mark-yang] and the IOAM model in [RFC9617].

```
  module: on-path-telemetry

    +--ro on-path-telemetry-data
       +--ro interface*                       [if-name]
          +--ro if-name                       if:interface-ref
          +--ro profile-name                  string
          +--ro filter
          |  +--ro filter-type?               telemetry-filter-type
          |  +--ro ace-name?                -> /acl:acls/acl/aces/ace/name
          +--ro protocol-type?                telemetry-protocol-type
          +--ro node-action                   telemetry-node-action
          +--ro measurement-period?           uint64
          +--ro measurement-period-number?    uint64
          +--ro flow-mon-id?                  uint32
          +--ro method-type?                  altmark-method-type
          +--ro altmark-loss-measurement?
          |  +--ro in-traffic-pkts?           yang:counter64
          |  +--ro out-traffic-pkts?          yang:counter64
          |  +--ro in-traffic-bytes?          uint64
          |  +--ro out-traffic-bytes?         uint64
          +--ro altmark-delay-measurement?
          |  +--ro pkts-timestamps?
          |     +--ro pkt-timestamp?          yang:date-and-time
          |     +--ro pkt-seq-num?            yang:counter32
          +--ro path-delay?
          |  +--ro path-delay-mean            uint32
          |  +--ro path-delay-min             uint32
          |  +--ro path-delay-max             uint32
          |  +--ro path-delay-sum             uint64
          +--ro ioam-incremental-tracing?
          |  +--ro incremental-tracing*       ioam-trace-data
          +--ro ioam-preallocated-tracing?
          |  +--ro preallocated-tracing*      ioam-trace-data
          +--ro ioam-direct-export?
          |  +--ro direct-export*             ioam-trace-data
          +--ro ioam-proof-of-transit?
          |  +--ro proof-of-transit*          ioam-pot-data
          +--ro ioam-edge-to-edge?
             +--ro edge-to-edge*              ioam-e2e-data
```

4. On-Path Telemetry Data

The "on-path-telemetry-data" contains detailed information for the AltMark telemetry data and IOAM telemetry data. The information includes:

* interface: indicates the list of interface where the On-Path Telemetry is applied.

The "interface" contains the detailed information for the each interface. The information includes:

* if-name: is the interface name as in ifName [RFC2863]

* profile-name: is the unique identifier for each profile

* filter: is used to identify the monitored flow

* protocol-type: is used to indicate the protocol where the On-path telemetry is applied

* node-action: indicates the operation applied to the flow.

* measurement-period: indicates the period. Note that it is different from the period defined in [RFC8641].

* measurement-period-number: indicates the period number (for AltMark see [I-D.ietf-ippm-alt-mark-deployment]).

* flow-mon-id: is used to identify the monitored flow and to correlate the exported data of the same flow from multiple nodes and from multiple packets.

* altmark-loss-measurement: indicates loss counters.

* altmark-delay-measurement: indicates packet timestamps.

* ioam-incremental-tracing: indicates IOAM incremental tracing data.

* ioam-preallocated-tracing: indicates IOAM preallocated tracing data.

* ioam-direct-export: indicates direct export data.

* ioam-proof-of-transit: indicates proof of transit data.

* ioam-edge-to-edge: indicates edge-to-edge data.

The "altmark-loss-measurement" contains:

* in-traffic-pkts: indicates the inbound packets of the period.

* out-traffic-pkts: indicates the outbound packets of the period.

* in-traffic-bytes: indicates the inbound bytes of the period.

* out-traffic-bytes: indicates the outbound bytes of the period.

The "altmark-delay-measurement" contains:

* pkts-timestamps: indicates the list of packet timestamps for delay measurement in the period (pkt-timestamp) and the corresponding sequence numbers (pkt-seq-num).

The "path-delay" in introduced in [I-D.ietf-opsawg-ipfix-on-path-telemetry] and contains:

* path-delay-mean: indicates the mean path delay between the encapsulation/marking node and the local node.

* path-delay-min: indicates the lowest path delay between the encapsulation/marking node and the local node.

* path-delay-max: indicates the highest path delay between the encapsulation/marking node and the local node.

* path-delay-sum: indicates the sum of the path delay between the encapsulation/marking node and the local node.

The "ioam-incremental-tracing" contains:

* incremental-tracing: indicates the list of incremental tracing data.

The "ioam-preallocated-tracing" contains:

* preallocated-tracing: indicates the list of preallocated tracing data.

The "ioam-direct-export" contains:

* direct-export: indicates the list of direct export data.

The "ioam-proof-of-transit" contains:

* proof-of-transit: indicates the list of proof of transit data.

The "ioam-edge-to-edge" contains:

* edge-to-edge: indicates the list of edge to edge data.

5. On-Path Telemetry YANG Data Model

```
<CODE BEGINS> file "ietf-on-path-telemetry@2025-06-30.yang"
module ietf-on-path-telemetry {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-on-path-telemetry";
  prefix "on-path-telemetry";

     import ietf-access-control-list {
       prefix acl;
       reference
         "RFC 8519: YANG Data Model for Network Access Control
          Lists (ACLs)";
     }

     import ietf-interfaces {
       prefix if;
      reference
        "RFC 8343: A YANG Data Model for Interface Management";
     }

     import ietf-yang-types {
       prefix yang;
       reference
         "Section 3 of RFC 6991";
     }

  organization
    "IETF IPPM (IP Performance Metrics) Working Group";

  contact
    "WG Web: <https://datatracker.ietf.org/wg/ippm>
     WG List: <ippm@ietf.org>
     Author: giuseppe.fioccola@huawei.com
     Author: zhoutianran@huawei.com
     Author: zhuyq8@chinatelecom.cn
     Author: zhangwq@chinatelecom.cn
     Author: zhukeyi@huawei.com";

  description
    "This YANG module specifies a vendor-independent data
     model for Alternate Marking Telemetry.

     The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL
     NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED',
     'MAY', and 'OPTIONAL' in this document are to be interpreted as
     described in BCP 14 (RFC 2119) (RFC 8174) when, and only when,
     they appear in all capitals, as shown here.
```

```
        Copyright (c) 2024 IETF Trust and the persons identified as
        authors of the code.  All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject to
        the license terms contained in, the Revised BSD License set
        forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
        (https://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC XXXX
        (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
        for full legal notices.";

     revision 2025-06-30 {
       description "First revision.";
       reference "RFC XXXX: A YANG Data Model for On-path Telemetry";
     }

    /*
     * FEATURES
     */

     feature altmark
     {
       description
         "This feature indicated that the Alternate-Marking Method is
         supported.";
       reference
         "RFC 9341: Alternate-Marking Method;
          RFC 9342: Clustered Alternate-Marking Method";
     }

     feature pathdelay
     {
       description
         "This feature indicated that the Path Delay is
         supported.";
       reference
         "[I-D.ietf-opsawg-ipfix-on-path-telemetry]";
     }

     feature incremental-trace
     {
       description
         "This feature indicated that the incremental tracing option is
         supported.";
       reference "RFC 9197: Data Fields for In-situ OAM";
```

```
  }

  feature preallocated-trace
  {
    description
      "This feature indicated that the preallocated tracing option is
      supported.";
    reference "RFC 9197: Data Fields for In-situ OAM";
  }

  feature direct-export
  {
    description
      "This feature indicated that the direct export option is
      supported.";
    reference "RFC 9326: In-situ OAM Direct Exporting";
  }

  feature proof-of-transit
  {
    description
      "This feature indicated that the proof of transit option is
      supported";
    reference "RFC 9197: Data Fields for In-situ OAM";
  }

  feature edge-to-edge
  {
    description
      "This feature indicated that the edge-to-edge option is
      supported.";
    reference "RFC 9197: Data Fields for In-situ OAM";
  }

 /*
  * IDENTITIES
  */

  identity filter {
    description
      "Base identity to represent a filter. A filter is used to
      specify the flow to which the On-Path Telemetry method is applied.";
  }

  identity acl-filter {
    base filter;
    description
      "Apply ACL rules to specify the flow.";
```

```
  }

  identity protocol {
    description
      "Base identity to represent the protocol. It's used to
      indicate the protocol for the application of the On-Path Telemetry
      method.";
  }

  identity ipv6 {
    base protocol;
    description
      "The On-Path Telemetry method is applied to IPv6 protocol.";
    reference
      "RFC 9343: IPv6 Application of the Alternate-Marking Method,
       RFC 9486: In-situ OAM IPv6 Options";
  }

  identity srh  {
    base protocol;
    description
      "The On-Path Telemetry method is applied to SRH.";
    reference
      "[I-D.fz-spring-srv6-alt-mark]: Application of the
      Alternate Marking Method to the Segment Routing Header";
  }

  identity mpls  {
    base protocol;
    description
      "The On-Path Telemetry method is applied to MPLS.";
    reference
      "[I-D.ietf-mpls-inband-pm-encapsulation]: Application of the
      Alternate Marking Method to the MPLS Label Stack";
  }

  identity nsh  {
    base protocol;
    description
      "The described IOAM data is embedded in NSH.";
    reference
      "RFC 9452: Network Service Header (NSH)
      Encapsulation for In-situ OAM (IOAM) Data";
   }

  identity node-action {
    description
      "Base identity to represent the node actions. It's used to
```

```
          indicate what action the node will take.";
      }

      identity action-marking {
        base node-action;
        description
          "It indicates that the node must mark the AltMark data field,
          according to the operations described in RFC 9341 and
          RFC 9342";
      }

      identity action-unmarking {
        base node-action;
        description
          "It indicates that the node must unmark the AltMark data field,
          according to the operations described in RFC 9341 and
          RFC 9342";
      }

      identity action-read {
        base node-action;
        description
          "It indicates the node only reads the AltMark data,
          according to the operations described in RFC 9341 and
          RFC 9342";
      }

      identity action-encapsulate {
        base node-action;
        description
          "It indicates the node is to encapsulate the IOAM packet";
      }

      identity action-decapsulate {
        base node-action;
        description
          "It indicates the node is to decapsulate the IOAM packet";
      }

      identity action-transit {
        base node-action;
        description
          "It indicates the node is to transit the IOAM packet";
      }

      identity measurement-period {
        description
          "It indicates the On-Path Telemetry Period.";
```

```
}

identity measurement-period-number {
  description
    "It indicates the Period Number.";
}

identity flow-mon-id {
  description
    "It indicates the FlowMonID.";
}

identity method {
  description
    "Base identity to represent the AltMark method type.";
}

identity trace-data {
  description
    "Base identity to represent trace data.";
}

identity pot-data {
  description
    "Base identity to represent POT data.";
 }

identity e2e-data {
  description
    "Base identity to represent E2E data.";
 }

identity telemetry-param-type {
  description
     "Base identity for telemetry param types";
 }

identity loss-measurement {
  base telemetry-param-type;
  description
    "To specify loss counters according to RFC 9341";
 }

identity delay-measurement {
  base telemetry-param-type;
  description
    "To specify timestamps for delay according to RFC 9341";
 }
```

```
    /*
     * TYPE DEFINITIONS
     */

     typedef telemetry-filter-type {
       type identityref {
         base filter;
       }
       description
         "It specifies a known type of filter.";
     }

     typedef telemetry-node-action {
       type identityref {
         base node-action;
       }
       description
         "It specifies a node action.";
     }

     typedef telemetry-protocol-type {
       type identityref {
         base protocol;
       }
       description
         "It specifies a known type of carrier protocol for the On-path
         Telemetry data.";
     }

     typedef altmark-method-type {
       type identityref {
         base method;
       }
       description
         "It specifies the AltMark method used.";
     }

     typedef ioam-trace-data {
       type identityref {
         base trace-data;
       }
       description
         "It specifies the trace data.";
     }

     typedef ioam-pot-data {
       type identityref {
         base pot-data;
```

```
      }
      description
        "It specifies the pot data.";
    }

    typedef ioam-e2e-data {
      type identityref {
        base e2e-data;
      }
      description
        "It specifies the edge-to-edge data.";
    }

   /*
    * GROUP DEFINITIONS
    */

    grouping telemetry-filter {
      description "A grouping for On-path Telemetry filter definition";

      leaf filter-type {
        type telemetry-filter-type;
        description "filter type";
      }

      leaf ace-name {
        when "derived-from-or-self(../filter-type,
        'on-path-telemetry:acl-filter')";
        type leafref {
          path "/acl:acls/acl:acl/acl:aces/acl:ace/acl:name";
        }
        description "The Access Control Entry name is used to
        refer to an ACL specification.";
      }
    }

    grouping telemetry-setup {
      description
        "A grouping for On-path Telemetry profile.";

      leaf node-action {
        type telemetry-node-action;
        description
          "This object indicates the action that the node needs to
           take, i.e. marking/read/unmarking/encapsulate/transit/decapsulate.";
      }

      leaf measurement-period {
```

```
        type uint64;
        description
        "It specifies the On-path Telemetry period.
        It is the marking period for AltMark.";
      }

      leaf measurement-period-number {
        type uint64;
        description
        "It specifies the On-path Telemetry period number.";
      }

      leaf flow-mon-id {
        type uint32;
        description
        "It specifies the 20-bit FlowMonID.";
      }

      leaf method-type {
        type altmark-method-type;
        description
        "It specifies the AltMark method type.";
      }

     }

    grouping loss-counters {
      description
        "The set of counters for RFC 9341 loss calculation.";

      leaf in-traffic-pkts {
        type yang:counter64;
        description
          "Total inbound packets of the period according to RFC 9341";
      }
      leaf out-traffic-pkts {
        type yang:counter64;
        description
          "Total outbound packets of the period according to RFC 9341";
      }

      leaf in-traffic-bytes {
        type uint64;
        description
          "Total inbound bytes of the period according to RFC 9341";
      }

      leaf out-traffic-bytes {
```

```
          type uint64;
          description
            "Total outbound bytes of the period according to RFC 9341";
        }

       }

      grouping delay-timestamps {
        description
          "It indicates the set of timestamps for RFC 9341 delay calculation.";

        container pkts-timestamps {
          description
            "The list of timestamps of the period according to RFC 9341";

          leaf pkt-timestamp {
            type yang:date-and-time;
            description
              "To specify the timestamp of the delay packet for delay measurements";
          }
          leaf pkt-seq-num {
            type yang:counter32;
            description
              "To specify the sequence number of the delay packet for delay measurements";
          }
         }
        }

      grouping path-delay-metrics {
        description
          "It indicates the path delay measurements.";

        leaf path-delay-mean {
          type uint32;
          description
            "mean path delay as per [I-D.ietf-opsawg-ipfix-on-path-telemetry]";
        }
        leaf path-delay-min {
          type uint32;
          description
            "min path delay as per [I-D.ietf-opsawg-ipfix-on-path-telemetry]";
        }

        leaf path-delay-max {
          type uint32;
          description
            "max path delay as per [I-D.ietf-opsawg-ipfix-on-path-telemetry]";
        }
```

```
        leaf path-delay-sum {
          type uint64;
          description
            "sum of the path delay as per [I-D.ietf-opsawg-ipfix-on-path-telemetry]";
        }
       }

      grouping ioam-incremental-tracing-data-list {
        description
          "A grouping for incremental tracing data.";

        container ioam-incremental-tracing {
          description
            "The list of incremental tracing data";
          leaf-list incremental-tracing {
            type ioam-trace-data;
            description
              "This object indicates the incremental tracing data.";
         }
        }
       }

      grouping ioam-preallocated-tracing-data-list {
        description
          "A grouping for the list of pre-allocated tracing data.";

          leaf-list preallocated-tracing {
            type ioam-trace-data;
            description
              "This object indicates the preallocated tracing data.";
         }
       }

      grouping ioam-direct-export-tracing-data-list {
        description
          "A grouping for the list of direct export data.";

          leaf-list direct-export {
            type ioam-trace-data;
            description
              "This object indicates the direct export data.";
         }
       }

       grouping ioam-proof-of-transit-data-list {
        description
           "A grouping for the list of proof of transit data.";
```

```
         leaf-list proof-of-transit {
           type ioam-pot-data;
           description
             "This object indicates the proof of transit data.";
         }
       }

       grouping ioam-edge-to-edge-data-list {
        description
           "A grouping for the list of edge-to-edge data.";

         leaf-list edge-to-edge {
           type ioam-e2e-data;
           description
             "This object indicates the edge to edge data.";
         }
       }


     /*
      * DATA NODES
      */

       container on-path-telemetry-data {
         config false;
         description "On-path Telemetry top level container";

          list interface {
          key "if-name";
          description
              "It contains the list of the interfaces activated for AltMark and IOAM";
           leaf if-name {
             type if:interface-ref;
             description "This is a reference to the Interface name.";
           }

           leaf profile-name {
             type string{
               length "1..300";
             }
           description
               "Unique identifier for the On-path Telemetry profile.";
           }

           container filter {
             uses telemetry-filter;
             description
               "The filter which is used to indicate the flow where
```

```
            the On-path Telemetry is applied.";
          }

          leaf protocol-type {
            type telemetry-protocol-type;
            description
              "This item is used to indicate the carrier protocol where
              the On-path Telemetry is applied.";
          }

          uses telemetry-setup;

          container altmark-loss-measurement {
             if-feature altmark;
             description
               "It reports the loss measurement data.";

             uses loss-counters;
          }

          container altmark-delay-measurement {
             if-feature altmark;
             description
               "It reports the delay measurement data.";

             uses delay-timestamps;
          }

          container path-delay {
             if-feature pathdelay;
             description
               "It reports the path delay measurements.";

             uses path-delay-metrics;
          }

          container ioam-incremental-tracing {
             if-feature incremental-trace;
             presence "Enables incremental tracing option.";
             description
               "It reports the incremental tracing option data.";

             uses ioam-incremental-tracing-data-list;
          }

          container ioam-preallocated-tracing {
             if-feature preallocated-trace;
             presence "Enables preallocated tracing option.";
```

```
            description
              "It reports the preallocated tracing option data.";

            uses ioam-preallocated-tracing-data-list;
          }

          container ioam-direct-export {
            if-feature direct-export;
            presence "Enables direct-export option.";
            description
              "It reports the direct-export option data";

            uses ioam-direct-export-tracing-data-list;
          }

          container ioam-proof-of-transit {
            if-feature proof-of-transit;
            presence "Enables Proof of Transit option.";
            description
              "It reports the PoT option data.";

            uses ioam-proof-of-transit-data-list;
          }

          container ioam-edge-to-edge {
            if-feature edge-to-edge;
            presence "Enables edge-to-edge option.";
            description
              "It reports the edge-to-edge option data.";

            uses ioam-edge-to-edge-data-list;
          }
        }
      }
    }
    <CODE ENDS>
```

6. Security Considerations

IOAM [RFC9197], Alternate Marking [RFC9341] and Multipoint Alternate Marking [RFC9342] analyze different security concerns and related solutions. These aspects are valid and applicable also to this document. In particular the fundamental security requirement is that Alternate Marking MUST only be applied in a specific limited domain, as also mentioned in [RFC8799].

The YANG module specified in this document defines a schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8446].

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

The top level administrative configurations related to the AltMark and IOAM functionalities are already reported in [I-D.ietf-ippm-alt-mark-yang] and [RFC9617]. Unexpected changes to those items could lead to the AltMark and IOAM function disruption and/ or misbehavior of the AltMark.

There are a number of data nodes defined in this YANG module. These data nodes may be considered sensitive or vulnerable in some network environments. These are the subtrees and data nodes and their sensitivity/vulnerability:

* /on-path-telemetry-data/interface

The entries in the container above include the AltMark and IOAM profile telemetry data which can be considered sensitive or vulnerable in some network environments. It is important to control read access (e.g., via get, get-config, or notification) to the readable data nodes.

7. IANA Considerations

IANA is requested to assign a new URI from the IETF XML Registry [RFC3688]. The following URI is suggested:

```
URI: urn:ietf:params:xml:ns:yang:ietf-on-path-telemetry
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.
```

This document also requests a new YANG module name in the YANG Module Names registry [RFC7950] with the following suggestion:

```
name: ietf-on-path-telemetry
namespace: urn:ietf:params:xml:ns:yang:ietf-on-path-telemetry
prefix: on-path-telemetry
reference: RFC XXXX
```

8. Acknowledgements

The authors would like to thank Martin Bjorklund and Alex Huang Feng for the precious comments and suggestions.

9. Contributors

Xiaoming He
China Telecom
Email: hexm4@chinatelecom.cn

10. References

10.1. Normative References

[I-D.ietf-ippm-alt-mark-yang]
Graf, T., Wang, M., Fioccola, G., Zhou, T., and X. Min, "A YANG Data Model for the Alternate Marking Method", Work in Progress, Internet-Draft, draft-ietf-ippm-alt-mark-yang-00, 8 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-alt-mark-yang-00>.

[I-D.ietf-opsawg-ipfix-on-path-telemetry]
Graf, T., Claise, B., and A. H. Feng, "Export of Delay Performance Metrics in IP Flow Information eXport (IPFIX)", Work in Progress, Internet-Draft, draft-ietf-opsawg-ipfix-on-path-telemetry-17, 5 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-ipfix-on-path-telemetry-17>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <https://www.rfc-editor.org/info/rfc8639>.

[RFC8640] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Dynamic Subscription to YANG Events and Datastores over NETCONF", RFC 8640, DOI 10.17487/RFC8640, September 2019, <https://www.rfc-editor.org/info/rfc8640>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <https://www.rfc-editor.org/info/rfc8641>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/info/rfc9197>.

[RFC9326] Song, H., Gafni, B., Brockners, F., Bhandari, S., and T. Mizrahi, "In Situ Operations, Administration, and Maintenance (IOAM) Direct Exporting", RFC 9326, DOI 10.17487/RFC9326, November 2022, <https://www.rfc-editor.org/info/rfc9326>.

[RFC9341] Fioccola, G., Ed., Cociglio, M., Mirsky, G., Mizrahi, T., and T. Zhou, "Alternate-Marking Method", RFC 9341, DOI 10.17487/RFC9341, December 2022, <https://www.rfc-editor.org/info/rfc9341>.

[RFC9342] Fioccola, G., Ed., Cociglio, M., Sapio, A., Sisto, R., and T. Zhou, "Clustered Alternate-Marking Method", RFC 9342, DOI 10.17487/RFC9342, December 2022, <https://www.rfc-editor.org/info/rfc9342>.

[RFC9617] Zhou, T., Ed., Guichard, J., Brockners, F., and S. Raghavan, "A YANG Data Model for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9617, DOI 10.17487/RFC9617, August 2024, <https://www.rfc-editor.org/info/rfc9617>.

10.2. Informative References

[I-D.ietf-ippm-alt-mark-deployment] Fioccola, G., Zhu, K., Graf, T., Nilo, M., and L. Zhang, "Alternate Marking Deployment Framework", Work in Progress, Internet-Draft, draft-ietf-ippm-alt-mark-deployment-03, 27 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-alt-mark-deployment-03>.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <https://www.rfc-editor.org/info/rfc2863>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

[RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <https://www.rfc-editor.org/info/rfc9232>.

[RFC9343] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate-Marking Method", RFC 9343, DOI 10.17487/RFC9343, December 2022, <https://www.rfc-editor.org/info/rfc9343>.

Appendix A. Example

An example of the way for a client to subscribe to the telemetry information is reported in the following figure. The telemetry parameters that the client is interested are Alternate-Marking, path delay and IOAM.

```
<rpc xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0"
    netconf:message-id="101">
    <establish-subscription xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
      <filter netconf:type="subtree">
        <on-path-telemetry-data xmlns="urn:ietf:params:xml:ns:yang:ietf-on-path-telemetry
">
          <interface>
            <if-name/>
            <profile-name/>
            <protocol-type/>
            <node-action/>
            <measurement-period/>
            <measurement-period-number/>
            <flow-mon-id/>
            <method-type/>
            <altmark-loss-measurement/>
            <altmark-delay-measurement/>
            <path-delay/>
            <ioam-incremental-tracing/>
            <ioam-preallocated-tracing/>
            <ioam-direct-export/>
            <ioam-proof-of-transit/>
            <ioam-edge-to-edge/>
          </interface>
        </on-path-telemetry-data>
      </filter>
      <period>10</period>
      <encoding>encode-xml</encoding>
    </establish-subscription>
 </rpc>
```

Authors' Addresses

Giuseppe Fioccola
Huawei
Viale Martesana, 12
20055 Vimodrone (Milan)
Italy
Email: giuseppe.fioccola@huawei.com

Tianran Zhou
Huawei
156 Beiqing Rd.
Beijing
100095
China
Email: zhoutianran@huawei.com

Yongqing Zhu
China Telecom
Guangzhou
China
Email: zhuyq8@chinatelecom.cn

Wenqiang Zhang
China Telecom
Beijing
China
Email: zhangwq@chinatelecom.cn

Keyi Zhu
Huawei Technologies
Email: zhukeyi@huawei.com