IETF
Internet-Draft
Intended status: Informational
Expires: 2 September 2024

Y. Cui
Tsinghua University
L. Li
Zhongguancun Laboratory
1 March 2024

Extended YANG Data Models for DOTS
draft-cui-dots-extended-yang-01

Commenté [BMI1]: As 3 models are defined.

Abstract

With the development of DDoS defense technologies, the interfaces and parameters defined by DOTS are no longer sufficient to support the collaborative signaling required between DDoS mitigation systems. This document defines three YANG ~~model~~ modules to extend ~~the data models of existing interfaces on the~~both DOTS signal~~ing~~ and data channels, with the aim of supporting the transmission of necessary collaborative information between DDoS mitigation systems via DOTS and enabling efficient collaborative mitigation based on this information.

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 2 September 2024.

Table of Contents

1. Introduction

1.1. Context and motivation

DDoS attacks have been a persistent network security issue plaguing global network operators and software providers. ~~With the growth of global networks,~~ DDoS attacks have increased in scale, frequency, and the emergence of new types, leading to a heightened focus on coordinated attack response and standardization. [RFC8612] defines the DDoS Open Threat Signaling (DOTS) protocol for coordinating responses to DDoS attacks. DOTS can be utilized by any device or software system involved in DDoS mitigation, allowing both parties involved in the coordination to exchange necessary information such as collaborative mitigation requests and monitoring data.

As DDoS mitigation technologies evolve, DDoS protection devices and software systems have expanded their functionalities, yet DOTS has not been adapted to incorporate these updates. In order for collaborative mitigation parties to formulate more effective mitigation strategies and respond more quickly to collaborative mitigation requests, it is necessary to extend the functionality interface and parameter model of DOTS.

This document defines three data models for extending the existing DOTS interfaces, enabling DOTS to support the transmission of crucial information required for collaborative mitigation.

1.2. 2. Terminology

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.

These capitalized words are used to signify the requirements for the DOTS protocols design.

This document adopts the following terms:

DDoS: A distributed denial-of-service attack in which traffic originating from multiple sources is directed at a target on a network. DDoS attacks are intended to cause a negative impact on the

Commenté [BMI2]: Actually, this is defined in RFC9132 (signal channel) and RFC8783 (data channel).

Commenté [BMI3]: You may refer to the use cases RFCs 8903, 9066,

Commenté [BMI4]: You may provide examples.

availability and/or functionality of an attack target. Denial-of-service considerations are discussed in detail in [RFC4732].

Mitigation: A set of countermeasures enforced against traffic destined for the target or targets of a detected or reported DDoS attack, where countermeasure enforcement is managed by an entity in the network path between attack sources and the attack target. Mitigation methodology is out of scope for this document.

Mitigator: An entity, typically a network element, capable of performing mitigation of a detected or reported DDoS attack. The means by which this entity performs these mitigations and how they are requested of it are out of scope for this document. The mitigator and DOTS server receiving a mitigation request are assumed to belong to the same administrative entity.

DOTS client: A DOTS-aware software module responsible for requesting attack response coordination with other DOTS-aware elements.

DOTS server: A DOTS-aware software module handling and responding to messages from DOTS clients.
The DOTS server enables mitigation on behalf of the DOTS client, if requested, by communicating the DOTS client's request to the mitigator and returning selected mitigator feedback to the requesting DOTS client.

2. Problem Sstatement

To illustrate the collaboration for DDoS mitigation systems, the following workflow should be established for efficient collaboration:

* In 'idle' time, ~~The~~ the client sends predetermined configuration information to the server, including but not limited to mitigation strategies and required mitigation resource capacity.

* Upon receiving the predetermined configuration request, the server determines based on its own capabilities whether to accept the installation.

* When collaboration is needed for mitigation, the client initiates a collaborative mitigation request to the server. The mitigation request should include important information such as attack characteristics, mitigation scope, and mitigation strategies.

* The server receives the mitigation request and forwards it to ~~thea~~ mitigat~~ion party~~or, utilizing the information within to confirm the authenticity of the attack and decide on responding to the collaborative mitigation request.

* The mitigation party formulates and executes the mitigation strategy. The server sends a confirmation response to the client.

* Continual exchange of monitoring information can occur between the server and client. The mitigation party can dynamically adjust mitigation strategies based on the monitoring information.

Commenté [BMI5]: I would simply refer to existing RFCs to ensure consistent terms are used.

Commenté [BMI6]: It would be helpful to use an approach similar to the use cases RFCs to explain the problem. See for example RFC 9387 - Use Cases for DDoS Open Threat Signaling (DOTS) Telemetry (ietf.org)

Commenté [BMI7]: I guess you are referring to enriching what is supported in RFC 9244 - Distributed Denial-of-Service Open Threat Signaling (DOTS) Telemetry (ietf.org) ?

Commenté [BMI8]: It would be helpful to explain why this is driven by the client? Clients may not have control on the mitigation plans

Commenté [BMI9]: Why this can't be inferred from the "Telemetry Baseline" (RFC9244)?

Commenté [BMI10]: Do you mean "mitigation hints" in RFC9244:

DOTS clients can send mitigation hints derived from attack details to DOTS servers, with the full understanding that a DOTS server may ignore mitigation hints, as described in [RFC8612] (Gen-004). Mitigation hints will be transmitted across the DOTS signal channel, as the data channel may not be functional during an attack. How a DOTS server handles normal and attack traffic attributes, and mitigation hints, is implementation specific.

Commenté [BMI11]: The interface between the server and mitigator may not be based on DOTS.

Commenté [BMI12]: How this related to the mitigation strategies in request from the client?

* After collaborative mitigation ceases, the server should send a mitigation report to the client.

To improve collaborative mitigation efficiency, it is essential to pre-configure mitigation strategies and mitigation resource capacities. These can assist clients in initiating requests to appropriate mitigation parties and enable mitigation parties to establish mitigation strategies. Currently, DOTS only supports the installation of ACL rules, lacking other widely used mitigation methods such as BGP Flowspec. Additionally, DOTS does not support the installation of mitigation resource capacity information, making it difficult for targets to identify the optimal collaborative mitigation party when facing attacks of different scales.

Within the mitigation request data model defined in DOTS, only descriptions of the mitigation scope are included, such as IP addresses and protocols. In the absence of commercial cooperation, these basic information pieces are insufficient to help mitigation parties identify attacks associated with mitigation requests and develop appropriate mitigation strategies based on the attack situation. Therefore, it is necessary to define an extended attack description model in the signaling channel, allowing mitigation parties to quickly and accurately identify associated attacks. These attack characteristics can also guide mitigation parties in formulating reasonable mitigation strategies.

When requesting mitigation, providing baseline information, mitigation suggestions, or specifying mitigation strategies is also essential. The key role of mitigation is to differentiate between attack packets and non-attack packets. The targeted entities usually have extensive learning experience on their normal business packets or statistical data, enabling them to accurately identify the differences between attacks and legitimate requests, thereby filtering attack traffic more accurately. Sharing baseline information, mitigation suggestions, and mitigation strategies can fully utilize the knowledge of the requesting party to help the mitigation party formulate effective mitigation strategies.

3. YANG Models

3.1. Extended YANG models for signal channel

```
module: ietf-dots-extended-signal-channel
  +-rw dots-signal
     +-rw attack-details
     |  +-rw packet-feature
     |  |  +-rw port-number              inet:port-number
     |  |  +-rw average-packet-length    unit32
     |  |  +-rw duplicate-content        string
     |  +-rw statistical-feature
     |  |  +-ro bps-avg                 unit32
     |  |  +-ro bps-peak                unit32
     |  |  +-ro pps-avg                 unit32
     |  |  +-ro pps-peak                unit32
     |  |  +-ro bkts-avg                unit32
     |  |  +-ro bkts-peak               unit32
     |  +-rw mitigation-strategy  list
     |  |  +-rw name              string
```

Commenté [BMI13]: Between a server and a mitigator?

If so, this is discussed in the telemetry use case draft.

Commenté [BMI14]: Please see rfc9387 for an example of how the filtering can trigger flowspecs action

Commenté [BMI15]: Do you assume that the client is attached to multiple DMSes? Otherwise, it is not clear how this is useful for selecting a DOTS server. You might elaborate.

Commenté [BMI16]: Please refer to 8.2. From DOTS Clients to DOTS Servers of RFC9244

Commenté [BMI17]: Please note that dots-signal uses RFC8791. Augments should use "sx:augment-structure"

Commenté [BMI18]: Should be gauge. Idem for other similar parameters.

```
      +-rw mitigation-advice    list
      |  +-rw description       string
```

Figure 1: DOTS Extended Signal Channel Tree Structure

```
   file "ietf-dots-extended-signal-channel@2024-02-20.yang" module ietf-
   dots-extended-signal-channel {

 yang-version 1.0;
 namespace
   "urn:ietf:params:xml:ns:yang:ietf-dots-extended-signal-channel";

 prefix

   grouping packet-feature {
     description
        "Packet-level characteristics of DDoS attack events.";
      leaf port-number {
        type inet:port-number;
        description
          "Target port number of the attack packet.";
      }
      leaf average-packet-length {
        type inet32unit32;
        units "byte";
        description
          "Average length of attack packets.";
      }
      leaf duplicate-content {
        type string;
        description
          "Duplicate content in the attack packet.";
      }
   }

   grouping statistical-feature {
     description
        "Statistical characteristics of DDoS attack events.";
      leaf bps-avg {
        type inet32;
        description
          "Average bps.";
      }
      leaf bps-peak {
        type inet32;
        description
          "Peak bps.";
      }
      leaf pps-avg {
        type inet32;
        description
          "Average pps.";
      }
      leaf pps-avg {
        type inet32;
        description
```

Commenté [BMI19]: The structure should indicate if the message is sent from a client to a server or the other way around.

Commenté [BMI20]: A prefix is missing, etc.

Please use the template https://datatracker.ietf.org/doc/html/draft-ietf-netmod-rfc8407bis-09#name-template-for-ietf-modules

Commenté [BMI21]: I suspect the telemetry attributes covers most of those. Please double check

a mis en forme : Surlignage

a mis en forme : Surlignage

```
          "Peak pps.";
      }

      leaf kbps-avg {
        type inet32;
        description
          "Average kbps.";
      }
      leaf kbps-avg {
        type inet32;
        description
          "Peak kbps.";
      }
    }

    typedef mitigation-strategy{
      leaf name{
        type: string;
        description
          "Name of the mitigation policy installed on the server.";
      }
    }

    typedef mitigation-advice{
      leaf description{
        type: string;
        description
          "Mitigation recommendations
          or other remarks that the expert can understand.";
      }
    }   }
```

Commenté [BMI22]: Please run pyang or similar tool to help fix the issues with the module.

* The mitigation request should include a description of the attack details, such as the type and characteristics of the attack. This will help the mitigator to identify the attack related to the mitigation request and decide whether to respond to the mitigation request. The attack characteristics can also serve as the basis for formulating mitigation strategies. The mitigator can develop reasonable mitigation strategies based on the specific features of the attack, such as the port, packet-level characteristics, etc. Furthermore, by utilizing statistical features of the attack, such as peak packet rate, the mitigator can allocate appropriate mitigation resources.

* In a mitigation request, it is optional to include the target's daily business baseline information, such as normal business ports and average packet length. This can assist the mitigator in comparing the differences between the normal baseline and attack characteristics, thus allowing them to select appropriate mitigation strategies.

* A request to be cached may selectively carry cache relief information, including specific cache relief strategies and recommendations. Cache relief strategies are policies already installed on the server by the client in advance, while cache relief recommendations can be any potentially effective cache relief strategy or important information proposed by the client.

Cache relief information can assist the cache relief party in devising appropriate cache relief strategies.

3.2. Extended YANG models for data channel

```
module: ietf-dots-extended-data-channel
 +-rw dots-data
    +-rw mitigation-strategy
    |  +-rw name            string
    |  +-rw type            string
    |  +-rw method          string
    |  +-rw content         string
    +-rw mitigation-capacity
    |  +-rw name            string
    |  +-rw type                  int8
    |  +-rw method                int8
    |  +-rw block-range           string
    |  +-ro filtering-capacity    unit32
    |  +-rw description           string
    +-rw baseline-information
    |  +-ro bps-avg               unit32
    |  +-ro bps-peak              unit32
    |  +-ro pps-avg               unit32
    |  +-ro pps-peak              unit32
    |  +-ro bkts-avg              unit32
    |  +-ro bkts-peak             unit32
    |  +-rw port-range            [lower-port]
    |  |  +-rw lower-port         inet:port-number
    |  |  +-rw upper-port?        inet:port-number
    |  +-rw packet-length-range
    |  |  +-rw min-length         unit32
    |  |  +-rw max-length         unit32
    +-rw intelligence
    |  +-rw type                  string
    |  +-rw content               string
    +-rw mitigation-capabilities
    |  +-rw type                  string
    |  +-rw capacity              string
```

Figure 2: DOTS Extended Data Channel Tree Structure

```
file "ietf-dots-extended-data-channel@2024-02-20.yang" module ietf-
dots-extended-data-channel { yang-version 1.0; namespace
"urn:ietf:params:xml:ns:yang:ietf-dots-extended-data-channel";

grouping mitigation-strategy {
  description
     "Mitigation strategy that clients can install on servers.";
    leaf name {
      type string;
      description
        "Name of the mitigation strategy.";
    }
    leaf type {
     tye enumeration {
       enum block {
         value 1;
```

Commenté [BMI23]: Should be defined as identities

Commenté [BMI24]: Already discussed in DOTS and the decision was to avoid redundant info in both sig and data channel.

```
          description
            "Discard all DDoS defense methods from specific sources.";
        }
        enum filter {
          value 2;
          description
            "Network devices such as routers
             are used to identify and filter attack traffic.";
        }
        enum scrubbing {
          value 3;
          description
            "Perform refined attack traffic
            filtering with dedicated DDoS scrubbing products.";
        }
      }
    }
    leaf method {
      type string;
      description
        "The name of the specific mitigation
        method used, such as the speed limit.";
    }
    leaf content {
      type string;
      description
        "Specific mitigation directives,
        such as ACL or BGP Flowspec directives.";
    }
  }

  grouping mitigation-capacity {
    description
      "Mitigation capacity that servers can offer.";
    leaf name {
      type string;
      description
        "Name of the mitigation resource.";
    }
    leaf type {
     tye enumeration {
       enum block {
         value 1;
         description
           "Discard all DDoS defense methods from specific sources.";
       }
       enum filter {
         value 2;
         description
           "Network devices such as routers
           are used to identify and filter attack traffic.";
       }
       enum scrubbing {
         value 3;
         description
           "Perform refined attack traffic filtering
           with dedicated DDoS scrubbing products.";
       }
```

```
      }
    }
    leaf method {
      type string;
      description
        "The name of the specific mitigation
        method used, such as the speed limit.";
    }
    leaf block-range {
      type string;
      description
        "The range that can be blocked when traffic is blocked.";
    }
    leaf filtering-capacity {
      type int32;
      description
        "Filter or clean the maximum acceptable attack traffic rate.";
    }
    leaf description {
      type string;
      description
        "Other supplementary notes.";
    }
  }
```

```
  grouping mitigation-capacity {
    description
      "Describes the mitigation capabilities of
      server-connected Minigators.";
      leaf bps-avg {
      type inet32;
      description
        "Average bps.";
    }
    leaf bps-peak {
      type inet32;
      description
        "Peak bps.";
    }
    leaf pps-avg {
      type inet32;
      description
        "Average pps.";
    }
    leaf pps-avg {
      type inet32;
      description
        "Peak pps.";
    }
    leaf kbps-avg {
      type inet32;
      description
        "Average kbps.";
    }
    leaf kbps-avg {
      type inet32;
      description
        "Peak kbps.";
```

```
      }
      leaf port-range {
        key "lower-port";
        description
          "Port range.  When only 'lower-port' is
           present, it represents a single port number.";
        leaf lower-port {
          type inet:port-number;
          description
            "Lower port number of the port range.";
        }
        leaf upper-port {


          type inet:port-number;
          must '. >= ../lower-port' {
            error-message
              "The upper port number must be greater than
               or equal to the lower port number.";
          }
          description
            "Upper port number of the port range.";
        }
      }
      leaf packet-length-range {
        key "lower-packet-length";
        description
          "Packet length range.  When only 'min-length' is
           present, it represents an avarage length.";
        leaf min-length {
          type int32;
          description
            "Minimum length of the packets.";
        }
        leaf max-length  {
          type int32;
          must '. >= ../min-length' {
            error-message
              "The minium length must be smaller than maximum length.";
          }
          description
            "Maximum length of the packets.";
        }
      }
    }

    grouping intelligence {
       description
         "Threat intelligence, such as IP and URI blacklist,
         botnet activity information, etc.";
       leaf type {
         type string;
         description
             "Types of threat intelligence.";
       }
       leaf type {
         type content;
```

```
        description
            "The specifics of the threat intelligence.";
      }
    }
  }
```

Commenté [BMI25]: Idem as for the previous module.

   * The data channel should support pre-deployed mitigation strategies
      for clients to choose from in case of attacks, as clients have a
      better understanding of the protection target's business model.
      Through the data channel, it is also important to proactively
      share information about mitigation resources, including available
      mitigation strategies and capacities provided by mitigation
      parties.

4. IANA Considerations

This document includes no request to IANA.

Commenté [BMI26]: At least two modules are defined. Please refer to the YANG guidelines

5. Normative References

[RFC8612] Mortensen, A., Reddy, T., and R. Moskowitz, "DDoS Open Threat Signaling (DOTS) Requirements", RFC 8612, DOI 10.17487/RFC8612, May 2019, <https://www.rfc-editor.org/rfc/rfc8612>.

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <https://www.rfc-editor.org/rfc/rfc4732>.

[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/rfc/rfc8174>.

[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/rfc/rfc2119>.

Acknowledgements

Authors' Addresses

Yong Cui
Tsinghua University
Beijing, 100084
China
Email: cuiyong@tsinghua.edu.cn
URI: http://www.cuiyong.net/

Linzhe Li
Zhongguancun Laboratory
Beijing, 100094
China
Email: lilz@zgclab.edu.cn