Workgroup: DOTS
Internet-Draft:
draft-ietf-dots-telemetry-use-cases-16
Published: 27 March 2023
Intended Status: Informational
Expires: 28 September 2023
Authors: Y. Hayashi M. Chen Li. Su
NTT CMCC CMCC

# Use Cases for DDoS Open Threat Signaling (DOTS) Telemetry

## Abstract

DDoS Open Threat Signaling (DOTS) Telemetry enriches the base DOTS protocols to assist the mitigator in using efficient DDoS attack mitigation techniques in a network. This document presents sample use cases for DOTS Telemetry. It discusses what components are deployed in the network, how they cooperate, and what information is exchanged to effectively use these techniques.

## Status of This Memo



## Copyright Notice

Table of Contents



# 1. Introduction

Distributed Denial-of-Service (DDoS) attacks, such as volumetric attacks and resource-consumption attacks, are critical threats to be handled by service providers. When such DDoS attacks occur, service providers have to mitigate them immediately to protect or recover their services.

Therefore, for service providers to immediately protect their network services from DDoS attacks, DDoS mitigation needs to be highly automated. To that aim, multivendor components involved in DDoS attack detection and mitigation should cooperate and support standard interfaces.

DDoS Open Threat Signaling (DOTS) is a set of protocols for real-time signaling, threat-handling requests, and data filtering between the multivendor elements [RFC9132][RFC8783]. DOTS Telemetry enriches the DOTS protocols with various telemetry attributes allowing optimal DDoS attack mitigation [RFC9244]. This document presents sample use cases for DOTS Telemetry which makes concrete overview and purpose described in [RFC9244]. This document also presents what components are deployed in the network, how they cooperate, and what information is exchanged to effectively use attack-mitigation techniques.

## 2. Terminology

The readers should be familiar with the terms defined in [RFC8612], [RFC8903] and [RFC9244].

In addition, this document uses the following terms:

**Top-talker:** A list of attack sources that are involved in an attack and which are generating an important part of the attack traffic.

**Supervised Machine Learning:** A machine-learning technique in which labeled data is used to train the algorithms (the input and output data are known).

**Unsupervised Machine Learning:** A machine learning technique in which unlabeled data is used to train the algorithms (the data has no historical labels).

## 3. Telemetry Use Cases

This section describes DOTS telemetry use cases that use attributes included in the DOTS telemetry specification [RFC9244].

The following subsections assume that once the DOTS signal channel is established, DOTS clients proceed with the telemetry setup configuration as detailed in Section 7 of [RFC9244]. The following telemetry parameters are used:

* 'measurement-interval' to define the period during which percentiles are computed.

* 'measurement-sample' to define the time distribution for measuring values that are used to compute percentiles.

### 3.1. Mitigation Resources Assignment

#### 3.1.1. Mitigating Attack Flow of Top-talker Preferentially

Some transit providers have to mitigate large-scale DDoS attacks by using DDoS Mitigation Systems (DMSes) with limited resources, which are already deployed in their network. For example, recently reported large DDoS attacks exceeded several Tbps. [DOTS_Overview]

This use case enables transit providers to use their DMS efficiently under volume-based DDoS attacks whose volume is more than the available capacity of the DMS. To enable this, the attack traffic of top-talkers is redirected to the DMS preferentially by cooperation among forwarding nodes, flow collectors, and orchestrators.

Figure 1 gives an overview of this use case. Figure 2 provides an example of a DOTS telemetry message body that is used to signal top-talkers (2001:db8:1::/48 and 2001:db8:2::/48).

```
(Internet Transit Provider)

               +-----------+      +--------------+ SNMP or YANG/NETCONF
        IPFIX +-----------+| DOTS |              |<---
          --->| Flow      ||C<-->S| Orchestrator | BGP Flowspec
              | collector |+      |              |--->   (Redirect)
              +-----------+       +--------------+

                         +-------------+
                  IPFIX +-------------+| BGP Flowspec (Redirect)
                    <---| Forwarding  ||<---
                        |    nodes    ||
                        |             ||           DDoS Attack
[ Target(s) ]<==========================================
                        |    ++=========================[top-talker]
                        |    || ++======================[top-talker]
                        +----|| ||---+
                             || ||
                             || ||
                             |/ |/
                        +----x--x----+
                        | DDoS       | SNMP or YANG/NETCONF
                        | mitigation |<---
                        | system     |
                        +------------+

* C is for DOTS client functionality
* S is for DOTS server functionality
```

Figure 1: Mitigating DDoS Attack Flow of Top-talkers Preferentially

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "target": {
          "target-prefix": [
            "2001:db8::1/128"
          ]
        },
        "total-attack-traffic-protocol": [
          {
            "protocol": 17,
            "unit": "megabit-ps",
            "mid-percentile-g": "900"
          }
        ],
        "attack-detail": [
          {
            "vendor-id": 32473,
            "attack-id": 77,
            "start-time": "1645057211",
            "attack-severity": "high",
            "top-talker":{
              "talker": [
                {
                  "source-prefix": "2001:db8:1::/48",
                  "total-attack-traffic": [
                    {
                      "unit": "megabit-ps",
                      "mid-percentile-g": "100"
                    }
                  ]
                },
                {
                  "source-prefix": "2001:db8:2::/48",
                  "total-attack-traffic": [
                    {
                      "unit": "megabit-ps",
                      "mid-percentile-g": "90"
                    }
                  ]
                }
              ]
            }
          }
        ]
      }
    ]
  }
```

```
}
```

Figure 2: An Example of Message Body to Signal Top-Talkers

The forwarding nodes send traffic statistics to the flow collectors, e.g., using IP Flow Information Export (IPFIX) [RFC7011]. When DDoS attacks occur, the flow collectors identify the attack traffic and send information about the top-talkers to the orchestrator using the "target-prefix" and "top-talkers" DOTS telemetry attributes. The orchestrator then checks the available capacity of the DMSes by using a network management protocol, such as Simple Network Management Protocol (SNMP) [RFC3413] or YANG with Network Configuration Protocol (YANG/NETCONF) [RFC7950]. After that, the orchestrator orders the forwarding nodes to redirect as much of the top-talker's traffic to each DMS as that DMS can handle by dissemination of Flow Specifications using tools such as Border Gateway Protocol Dissemination of Flow Specification Rules (BGP Flowspec) [RFC8955].

The flow collector implements a DOTS client while the orchestrator implements a DOTS server.

### 3.1.2. DMS Selection for Mitigation

Transit providers can deploy their DMSes in clusters. Then, they can select the DMS to be used to mitigate a DDoS attack at the time of an attack.

This use case enables transit providers to select a DMS with sufficient capacity for mitigation based on the volume of the attack traffic and the capacity of a DMS. Figure 3 gives an overview of this use case. Figure 4 provides an example of a DOTS telemetry message body that is used to signal various attack traffic percentiles.

```
(Internet Transit Provider)

               +-----------+      +--------------+ SNMP or YANG/NETCONF
        IPFIX +-----------+| DOTS |              |<---
          --->| Flow      ||C<-->S| Orchestrator | BGP (Redirect)
              | collector |+      |              |--->
              +-----------+       +--------------+

                         +------------+
                  IPFIX +------------+| BGP (Redirect)
                    <---| Forwarding ||<---
                        |    nodes   ||
                        |            ||     DDoS Attack
[Target A]              | ++=================== [Destined for Target A]
[Target B]              | ||  ++=============== [Destined for Target B]
                        +-||--||-----+
                          ||  ||
                    ++====++  ||  (congested DMS)
                    ||        ||  +-----------+
                    ||        |/  |      DMS3 |
                    ||  +-----x------+        |<--- SNMP or YANG/NETCONF
                    |/  |       DMS2 |--------+
                 +--x---------+      |<--- SNMP or YANG/NETCONF
                 |       DMS1 |------+
                 |            |<--- SNMP or YANG/NETCONF
                 +------------+
```

* C is for DOTS client functionality
* S is for DOTS server functionality

Figure 3: DMS Selection for Mitigation

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "target": {
          "target-prefix": [
            "192.0.2.3/32"
          ]
        },
        "total-attack-traffic": [
          {
            "unit": "megabit-ps",
            "low-percentile-g": "600",
            "mid-percentile-g": "800",
            "high-percentile-g": "1000",
            "peak-g":"1100",
            "current-g":"700"
          }
        ]
      }
    ]
  }
}
```


Figure 4: Example of Message Body with Total Attack Traffic

The forwarding nodes send traffic statistics to the flow collectors, e.g., using IPFIX. When DDoS attacks occur, the flow collectors identify the attack traffic and send information about the attack traffic volume to the orchestrator by using the "target-prefix" and "total-attack-traffic" DOTS telemetry attributes. The orchestrator then checks the available capacity of the DMSes by using a network management protocol, such as Simple Network Management Protocol (SNMP) [RFC3413] or YANG with Network Configuration Protocol (YANG/ NETCONF) [RFC7950]. After that, the orchestrator selects a DMS with sufficient capacity to which attack traffic should be redirected. For example, a simple DMS selection algorithm is to choose a DMS whose available capacity is greater than the "peak-g" attribute indicated in the DOTS telemetry message. The orchestrator orders the appropriate forwarding nodes to redirect the attack traffic to the DMS relying upon routing policies, such as BGP [RFC4271].

The detailed DMS selection algorithm is out of the scope of this document.

The flow collector implements a DOTS client while the orchestrator implements a DOTS server.

### 3.1.3.  Path Selection for Redirection

A transit provider network has multiple paths to convey attack traffic to a DMS. In such a network, the attack traffic can be conveyed while avoiding congested links by adequately selecting an available path.

This use case enables transit providers to select a path with sufficient bandwidth for redirecting attack traffic to a DMS according to the bandwidth of the attack traffic and total traffic. Figure 5 gives an overview of this use case. Figure 6 provides an example of a DOTS telemetry message body that is used to signal various attack traffic percentiles and total traffic percentiles.

```
(Internet Transit Provider)

          +-----------+      +--------------+ DOTS
         +-----------+|      |              |S<---
   IPFIX | Flow      || DOTS | Orchestrator |
      -->| collector ||C<-->S|              | BGP Flowspec (Redirect)
         |           |+      |              |--->
         +-----------+       +--------------+

               DOTS +------------+  DOTS +------------+ IPFIX
               --->C| Forwarding |  --->C| Forwarding |--->
       BGP Flowspec |   node     |       |   node     |
     (Redirect) --->|            |       |            |  DDoS Attack
[Target]            |       ++===================================
                    +-------||---+       +------------+
                            ||              /
                            ||             / (congested link)
                            ||            /
                    DOTS  +-||----------------+ BGP Flowspec (Redirect)
                     --->C| ||  Forwarding    |<---
                          | ++===  node       |
                          +----||-------------+
                               |/
                            +--x-----------+
                            |     DMS      |
                            +--------------+

* C is for DOTS client functionality
* S is for DOTS server functionality
```

Figure 5: Path Selection for Redirection

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "target": {
          "target-prefix": [
            "2001:db8::1/128"
          ]
        },
        "total-traffic": [
          {
            "unit": "megabit-ps",
            "mid-percentile-g": "1300",
            "peak-g": "800"
           }
        ],
        "total-attack-traffic": [
          {
            "unit": "megabit-ps",
            "low-percentile-g": "600",
            "mid-percentile-g": "800",
            "high-percentile-g": "1000",
            "peak-g": "1100",
            "current-g": "700"
           }
        ]
      }
    ]
  }
}
```

Figure 6: An Example of Message Body with Total Attack Traffic and Total Traffic

The forwarding nodes send traffic statistics to the flow collectors, e.g., using IPFIX. When DDoS attacks occur, the flow collectors identify attack traffic and send information about the attack traffic volume to the orchestrator by using "target-prefix" and "total-attack-traffic" DOTS telemetry attributes. The underlying forwarding nodes send the volume on the total traffic passing the node to the orchestrator by using "total-traffic" telemetry attributes. The orchestrator then selects a path with sufficient bandwidth to which attack-traffic flow should be redirected. For example, the simple algorithm of the selection is to choose a path whose available capacity is greater than the "peak-g" attribute that was indicated in a DOTS telemetry message. After that, the orchestrator orders the appropriate forwarding nodes to redirect the attack traffic to the DMS by dissemination of Flow Specifications using tools such as Border Gateway Protocol Dissemination of Flow Specification Rules (BGP Flowspec) [RFC8955].

The detailed path selection algorithm is out of the scope of this document.

The flow collector and forwarding nodes implement a DOTS client while the orchestrator implements a DOTS server.

#### 3.1.4. Short but Extreme Volumetric Attack Mitigation

Short but extreme volumetric attacks, such as pulse wave DDoS attacks, are threats to Internet transit provider networks. These attacks start from zero and go to maximum values in a very short time span, then go back to zero, and then back to maximum, repeating in continuous cycles at short intervals. It is difficult for the transit providers to mitigate such an attack with their DMSes using a redirecting attack flows because this may cause route flapping in the network. The practical way to mitigate short but extreme volumetric attacks is to offload mitigation actions to a forwarding node.

This use case enables transit providers to mitigate short but extreme volumetric attacks. Furthermore, the aim is to estimate the network-access success rate based on the bandwidth of the attack traffic. Figure 7 gives an overview of this use case. Figure 8 provides an example of a DOTS telemetry message body that is used to signal total pipe capacity. Figure 9 provides an example of a DOTS telemetry message body that is used to signal various attack traffic percentiles and total traffic percentiles.

```
(Internet Transit Provider)

            +------------+      +----------------+
            | Network    |  DOTS | Administrative |
Alert ----->| Management |C<--->S| System         | BGP Flowspec (Rate-L
            | System     |       |                |--->
            +------------+      +----------------+

              +------------+     +------------+ BGP Flowspec (Rate-Limit
              | Forwarding |     | Forwarding |<---
              |   node     |     |   node     |
        Link1 |            |     |            | DDoS & Normal traffic
[Target]<-------------------------------------================
Pipe          +------------+     +------------+  Attack Traffic
Capability                                       Bandwidth
  X bps                                           Y bps

                    Network access success rate
                           X / (X + Y)

* C is for DOTS client functionality
* S is for DOTS server functionality
```

Figure 7: Short but Extreme Volumetric Attack Mitigation


```
  {
    "ietf-dots-telemetry:telemetry-setup": {
      "telemetry": [
        {
          "total-pipe-capacity": [
            {
              "link-id": "link1",
              "capacity": "1000",
              "unit": "megabit-ps"
            }
          ]
        }
      ]
    }
  }
```

Figure 8: Example of Message Body with Total Pipe Capacity

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "target": {
          "target-prefix": [
            "2001:db8::1/128"
          ]
        },
        "total-traffic": [
          {
            "unit": "megabit-ps",
            "mid-percentile-g": "800",
            "peak-g": "1300"
           }
        ],
        "total-attack-traffic": [
          {
            "unit": "megabit-ps",
            "low-percentile-g": "200",
            "mid-percentile-g": "400",
            "high-percentile-g": "500",
            "peak-g": "600",
            "current-g": "400"
          }
        ]
       }
    ]
  }
}
```


Figure 9: Example of Message Body with Total Attack Traffic, and Total Traffic

When DDoS attacks occur, the network management system receives alerts. Then, it sends the target IP address(es) and volume of the DDoS attack traffic to the administrative system by using the "target-prefix" and "total-attack-traffic" DOTS telemetry attributes. After that, the administrative system orders relevant forwarding nodes to carry out rate-limiting of all traffic destined to the target based on the pipe capability by the dissemination of the Flow Specifications using tools such as Border Gateway Protocol Dissemination of Flow Specification Rules (BGP Flowspec) [RFC8955]. In addition, the administrative system estimates the network-access success rate of the target, which is calculated by (total-pipe-capability / (total-pipe-capability + total-attack-traffic)).

Note that total pipe capability information can be gathered by telemetry setup in advance (Section 7.2 of [RFC9244]).

The network management system implements a DOTS client while the administrative system implements a DOTS server.

#### 3.1.5. Selecting Mitigation Technique Based on Attack Type

Some volumetric attacks, such as DNS amplification attacks, can be detected with high accuracy by checking the Layer 3 or Layer 4 information of attack packets. These attacks can be detected and mitigated through cooperation among forwarding nodes and flow collectors by using IPFIX. It may also be necessary to inspect the Layer 7 information of suspicious packets to detect attacks such as DNS Water Torture Attacks [DNS_Water_Torture_Attack]. To carry out the DNS water torture attack, an attacker commands a botnet to make thousands of DNS requests for fake subdomains against an Authoritative Name Server. Such attack traffic should be detected and mitigated at the DMS.

This use case enables transit providers to select a mitigation technique based on the type of attack traffic: amplification attack or not. To use such a technique, the attack traffic is blocked by forwarding nodes or redirected to a DMS based on the attack type through cooperation among forwarding nodes, flow collectors, and an orchestrator.

Figure 10 gives an overview of this use case. Figure 11 provides an example of attack mappings that are shared by using the DOTS data channel in advance. Figure 12 provides an example of a DOTS telemetry message body that is used to signal various attack traffic percentiles, total traffic percentiles, total attack connection, and attack type.

The example in Figure 11 uses the folding defined in [RFC8792] for long lines.

```
  (Internet Transit Provider)

           +-----------+ DOTS +--------------+
          +-----------+|<---->|              | BGP (Redirect)
    IPFIX | Flow      ||C    S| Orchestrator | BGP Flowspec (Drop)
      --->| collector |+      |              |--->
          +-----------+       +--------------+

                      +------------+ BGP (Redirect)
               IPFIX +------------+| BGP Flowspec (Drop)
                 <---| Forwarding ||<---
                     |    nodes   ||              DDoS Attack
                     |     ++=====||================
                     |     ||     ||x<==============[DNS Amp]
                     |     ||     |+x<==============[NTP Amp]
                     +-----||-----+
                           ||
                           |/
                     +-----x------+
                     | DDoS       |
                     | mitigation |
                     | system     |
                     +------------+

  * C is for DOTS client functionality
  * S is for DOTS server functionality
  * DNS Amp: DNS Amplification
  * NTP Amp: NTP Amplification
```

Figure 10: DDoS Mitigation Based on Attack Type

```
=============== NOTE: '\' line wrapping per RFC 8792 ================

{
  "ietf-dots-mapping:vendor-mapping": {
    "vendor": [
      {
        "vendor-id": 32473,
        "vendor-name": "mitigator-c",
        "last-updated": "1629898958",
        "attack-mapping": [
          {
            "attack-id": 77,
            "attack-description": "DNS amplification Attack: \
This attack is a type of reflection attack in which attackers \
spoof a target's IP address. The attackers abuse vulnerabilities \
in DNS servers to turn small queries into larger payloads."
          },
          {
            "attack-id": 92,
            "attack-description":"NTP amplification Attack: \
This attack is a type of reflection attack in which attackers \
spoof a target's IP address. The attackers abuse vulnerabilities \
in NTP servers to turn small queries into larger payloads."
          }
        ]
      }
    ]
  }
}
```

Figure 11: Example of Message Body with Attack Mappings

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "target": {
          "target-prefix": [
            "2001:db8::1/128"
          ]
        },
        "total-attack-traffic": [
          {
            "unit": "megabit-ps",
            "low-percentile-g": "600",
            "mid-percentile-g": "800",
            "high-percentile-g": "1000",
            "peak-g": "1100",
            "current-g": "700"
           }
        ],
        "total-attack-traffic-protocol": [
          {
            "protocol": 17,
            "unit": "megabit-ps",
            "mid-percentile-g": "500"
          },
          {
            "protocol": 15,
            "unit": "megabit-ps",
            "mid-percentile-g": "200"
          }
        ],
        "total-attack-connection": [
        {
           "mid-percentile-l": [
            {
              "protocol": 15,
              "connection": 200
            }
           ],
           "high-percentile-l": [
            {
              "protocol": 17,
              "connection": 300
            }
           ]
        }
        ],
        "attack-detail": [
```

```
          {
            "vendor-id": 32473,
            "attack-id": 77,
            "start-time": "1641169211",
            "attack-severity": "high"
          },
          {
            "vendor-id": 32473,
            "attack-id": 92,
            "start-time": "1641172809",
            "attack-severity": "high"
          }
        ]
      }
    ]
  }
}
```


Figure 12: Example of Message Body with Total Attack Traffic, Total Attack Traffic Protocol, Total Attack Connection and Attack Type

Attack mappings are shared by using the DOTS data channel in advance (Section 8.1.6 of [RFC9244]). The forwarding nodes send traffic statistics to the flow collectors, e.g., using IPFIX. When DDoS attacks occur, the flow collectors identify attack traffic and send attack type information to the orchestrator by using "vendor-id" and "attack-id" telemetry attributes. The orchestrator then resolves abused port numbers and orders relevant forwarding nodes to block the amplification attack traffic flow by dissemination of Flow Specifications using tools such as Border Gateway Protocol Dissemination of Flow Specification Rules (BGP Flowspec) [RFC8955]. Also, the orchestrator orders relevant forwarding nodes to redirect other traffic than the amplification attack traffic by using a routing protocol, such as BGP [RFC4271].

The flow collector implements a DOTS client while the orchestrator implements a DOTS server.

### 3.2. Detailed DDoS Mitigation Report

It is possible for the transit provider to add value to the DDoS mitigation service by reporting ongoing and detailed DDoS countermeasure status to the enterprise network. In addition, it is possible for the transit provider to know whether the DDoS countermeasure is effective or not by receiving reports from the enterprise network.

This use case enables sharing of information about ongoing DDoS countermeasures between the transit provider and the enterprise network mutually. Figure 13 gives an overview of this use case. Figure 14 provides an example of a DOTS telemetry message body that is used to signal total pipe capacity from the enterprise network administrator to the orchestrator in the ISP. Figure 15 provides an example of a DOTS telemetry message body that is used to signal various total traffic percentiles, total attack traffic percentiles, and attack details from the orchestrator to the network.

```
  +------------------+       +------------------------+
  | Enterprise       |       |    Upstream            |
  | Network          |       |    Internet Transit    |
  |  +------------+  |       |    Provider            |
  |  | Network    |C |       |   S+--------------+    |
  |  | admini-    |<-----DOTS---->| Orchestrator |    |
  |  | strator    |  |       |    +--------------+    |
  |  +------------+  |       |         C ^            |
  |                  |       |           | DOTS       |
  |                  |       |         S v            |
  |                  |       |    +---------------+ DDoS Attack
  |                  |       |    |      DMS      |+=======
  |                  |       |    +---------------+   |
  |                  |       |           || Clean     |
  |                  |       |           |/ Traffic   |
  |  +---------+     |       |   +---------------+    |
  |  | DDoS    |     |       |   | Forwarding    | Normal Traffic
  |  | Target  |<================| Node          |========
  |  +---------+     | Link1 |   +---------------+    |
  +------------------+       +------------------------+

* C is for DOTS client functionality
* S is for DOTS server functionality
```

Figure 13: Detailed DDoS Mitigation Report


```
{
  "ietf-dots-telemetry:telemetry-setup": {
    "telemetry": [
      {
        "total-pipe-capacity": [
          {
            "link-id": "link1",
            "capacity": "1000",
            "unit": "megabit-ps"
          }
        ]
      }
    ]
  }
}
```


Figure 14: An Example of Message Body with Total Pipe Capacity

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "tmid": 567,
        "target": {
          "target-prefix": [
            "2001:db8::1/128"
          ]
        },
        "target-protocol": [
          17
        ],
        "total-traffic": [
          {
            "unit": "megabit-ps",
            "mid-percentile-g": "800"
          }
        ],
        "total-attack-traffic": [
          {
            "unit": "megabit-ps",
            "mid-percentile-g": "100"
          }
        ],
        "attack-detail": [
          {
            "vendor-id": 32473,
            "attack-id": 77,
            "start-time": "1644819611",
            "attack-severity": "high"
          }
        ]
      }
    ]
  }
}
```


Figure 15: An Example of Message Body with Total Traffic,
Total Attack Traffic Protocol, and Attack Detail

The network management system in the enterprise network reports limits of incoming traffic volume from the transit provider to the orchestrator in the transit provider in advance. It is reported by using the "total-pipe-capacity" telemetry attribute in the DOTS telemetry setup.

When DDoS attacks occur, DDoS mitigation orchestration [RFC8903] is carried out in the transit provider. Then, the DDoS mitigation systems report the status of DDoS countermeasures to the orchestrator by sending "attack-detail" telemetry attributes. After that, the orchestrator integrates the reports from the DDoS mitigation systems, while removing duplicate contents, and sends the integrated report to a network administrator by using DOTS telemetry periodically.

During the DDoS mitigation, the orchestrator in the transit provider retrieves link congestion status from the network manager in the enterprise network by using "total-traffic" telemetry attributes. Then, the orchestrator checks whether the DDoS countermeasures are effective or not by comparing the "total-traffic" and the "total-pipe-capacity" attributes.

The DMS implements a DOTS server while the orchestrator behaves as a DOTS client and a server in the transit provider. In addition, the network administrator implements a DOTS client.

### 3.3. Tuning Mitigation Resources

#### 3.3.1. Supervised Machine Learning of Flow Collector

DDoS detection based on tools, such as IPFIX, is a lighter weight method of detecting DDoS attacks than DMSes in Internet transit provider networks. DDoS detection based on the DMSes is a more accurate method for detecting attack traffic than flow monitoring.

The aim of this use case is to increase flow collectors' detection accuracy by carrying out supervised machine-learning techniques according to attack detail reported by the DMSes. To use such a technique, forwarding nodes, flow collectors, and a DMS should cooperate. Figure 16 gives an overview of this use case. Figure 17 provides an example of a DOTS telemetry message body that is used to signal various total attack traffic percentiles and attack detail.

```
                                +-----------+
                               +-----------+| DOTS
                         IPFIX | Flow      ||S<---
                           --->| collector ||
                               +-----------++

                                +------------+
                         IPFIX +------------+|
                           <---| Forwarding ||
                               |    nodes   ||           DDoS Attack
 [ Target ]                    |   ++================================
                               |   || ++=============================
                               |   || || ++==========================
                               +---||-|| ||-+
                                   || || ||
                                   |/ |/ |/
                         DOTS  +---X--X--X--+
                          --->C| DDoS       |
                               | mitigation |
                               | system     |
                               +------------+

        * C is for DOTS client functionality
        * S is for DOTS server functionality

Figure 16: Training Supervised Machine Learning of Flow Collectors
```

```
{
  "ietf-dots-telemetry:telemetry": {
    "pre-or-ongoing-mitigation": [
      {
        "target": {
          "target-prefix": [
            "2001:db8::1/128"
          ]
        },
        "attack-detail": [
          {
            "vendor-id": 32473,
            "attack-id": 77,
            "start-time": "1634192411",
            "attack-severity": "high",
            "top-talker": {
              "talker": [
                {
                  "source-prefix": "2001:db8::2/127"
                }
              ]
            }
          }
        ]
      }
    ]
  }
}
```


Figure 17: An Example of Message Body with Attack Type
and top-talkers

The forwarding nodes send traffic statistics to the flow collectors, e.g., using IPFIX. When DDoS attacks occur, DDoS mitigation orchestration is carried out (as per Section 3.3 of [RFC8903]) and the DMS mitigates all attack traffic destined for a target. The DDoS mitigation system reports the "vendor-id", "attack-id", and "top-talker" telemetry attributes to a flow collector.

After mitigating a DDoS attack, the flow collector attaches outputs of the DMS as labels to the statistics of traffic flow of top-talkers. The outputs, for example, are the "attack-id" telemetry attributes. The flow collector then carries out supervised machine learning to increase its detection accuracy, setting the statistics as an explanatory variable and setting the labels as an objective variable.

The DMS implements a DOTS client while the flow collector implements a DOTS server.

### 3.3.2. Unsupervised Machine Learning of Flow Collector

DMSes can detect DDoS attack traffic, which means DMSes can also identify clean traffic. This use case supports unsupervised machine-learning for anomaly detection according to a baseline reported by the DMSes. To use such a technique, forwarding nodes, flow collectors, and a DMS should cooperate. Figure 18 gives an overview of this use case. Figure 19 provides an example of a DOTS telemetry message body that is used to signal baseline.

```
                              +-----------+
                             +-----------+|
                        DOTS | Flow      ||
                        --->S| collector ||
                             +-----------++

                              +------------+
                             +------------+|
                             | Forwarding ||
                             |    nodes   ||             Traffic
[ Destination ] <== =============++==============================
                             |   ||       ||
                             |   ||       |+
                             +---||-------+
                                 ||
                                 |/
                       DOTS  +---X--------+
                        --->C| DDoS       |
                             | mitigation |
                             | system     |
                             +------------+

      * C is for DOTS client functionality
      * S is for DOTS server functionality
```

Figure 18: Training Unsupervised Machine Learning of Flow Collectors

```
{
  "ietf-dots-telemetry:telemetry-setup": {
    "telemetry": [
      {
        "baseline": [
          {
            "id": 1,
            "target-prefix": [
              "2001:db8:6401::1/128"
            ],
            "target-port-range": [
              {
                "lower-port": "53"
              }
            ],
            "target-protocol": [
              17
            ],
            "total-traffic-normal": [
              {
                "unit": "megabit-ps",
                "low-percentile-g": "30",
                "mid-percentile-g": "50",
                "high-percentile-g": "60",
                "peak-g": "70"
              }
            ]
          }
        ]
      }
    ]
  }
}
```

Figure 19: An Example of Message Body with Traffic Baseline

The forwarding nodes carry out traffic mirroring to copy the traffic destined an IP address and to monitor the traffic by a DMS. The DMS then identifies "clean" traffic and reports the baseline attributes to the flow collector by using DOTS telemetry.

The flow collector then carries out unsupervised machine learning to be able to carry out anomaly detection.

The DMS implements a DOTS client while the flow collector implements a DOTS server.

## 4. Security Considerations

DOTS telemetry security considerations are discussed in Section 14 of [RFC9244]. These considerations apply for the communication interfaces where DOTS is used.

Some use cases involve controllers, orchestrators, and programmable interfaces. These interfaces can be misused by misbehaving nodes to further exacerbate DDoS attacks. The considerations are for end-to-end systems for DoS mitigation, so the mechanics are outside the scope of DOTS protocols. Section 5 of [RFC7149] discusses some generic security considerations to take into account in such contexts (e.g., reliable access control). Specific security measures depend on the actual mechanism used to control underlying forwarding nodes and other controlled elements. For example, Section 13 of [RFC8955] discusses security considerations that are relevant to BGP Flowspec. IPFIX-specific considerations are discussed in Section 11 of [RFC7011].

## 5. IANA Considerations

This document does not require any action from IANA.

## 6. Acknowledgement

The authors would like to thank Mohamed Boucadair and Valery Smyslov for their valuable feedback.

Thanks to Paul Wouters for the detailed AD review.

Many thanks to Donald Eastlake, Phillip Hallam-Baker, Sean Turner, and Peter Yee for their review.

Thanks to Lars Eggert, Murray Kucherawy, Roman Danyliw, Robert Wiltonm, and Eric Vyncke for the IESG review.

## 7. References

### 7.1. Normative References

**[RFC9244]** Boucadair, M., Ed., Reddy.K, T., Ed., Doron, E., Chen, M., and J. Shallow, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Telemetry", RFC 9244, DOI 10.17487/RFC9244, June 2022, <https://www.rfc-editor.org/info/rfc9244>.

### 7.2. Informative References

**[DNS_Water_Torture_Attack]** Xi, L., "A Large Scale Analysis of DNS Water Torture Attack", DOI 10.1145/3297156.3297272, December 2018, <https://dl.acm.org/doi/10.1145/3297156.3297272>.

**[DOTS_Overview]** Reddy, T. and M. Boucadair, "DOTS Overview (RFCs 8782, 8783)", July 2020, <https://datatracker.ietf.org/meeting/108/materials/slides-108-saag-dots-overview-00>.

**[RFC3413]** Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, DOI 10.17487/RFC3413, December 2002, <https://www.rfc-editor.org/info/rfc3413>.

**[RFC4271]** Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

**[RFC7011]** Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

**[RFC7149]** Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <https://www.rfc-editor.org/info/rfc7149>.

**[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>.

**[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/info/rfc8612>.

**[RFC8783]** Boucadair, M., Ed. and T. Reddy.K, Ed., "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", RFC 8783, DOI 10.17487/RFC8783, May 2020, <https://www.rfc-editor.org/info/rfc8783>.

**[RFC8792]** Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/info/rfc8792>.

**[RFC8903]** Dobbins, R., Migault, D., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use Cases for DDoS Open Threat

Signaling", RFC 8903, DOI 10.17487/RFC8903, May 2021, <https://www.rfc-editor.org/info/rfc8903>.

**[RFC8955]** Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/info/rfc8955>.

**[RFC9132]** Boucadair, M., Ed., Shallow, J., and T. Reddy.K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", RFC 9132, DOI 10.17487/RFC9132, September 2021, <https://www.rfc-editor.org/info/rfc9132>.

## Authors' Addresses

Yuhei Hayashi
NTT
3-9-11, Midori-cho, Tokyo
180-8585
Japan

Email: yuuhei.hayashi@gmail.com

Meiling Chen
CMCC
32, Xuanwumen West
BeiJing
BeiJing, 100053
China

Email: chenmeiling@chinamobile.com

Li Su
CMCC
32, Xuanwumen West
BeiJing, BeiJing
100053
China

Email: suli@chinamobile.com