Workgroup: DOTS
Internet-Draft:
draft-ietf-dots-telemetry-use-cases-06
Published: 13 February 2022
Intended Status: Informational
Expires: 17 August 2022
Authors: Y. Hayashi   M. Chen   Li. Su
NTT   CMCC   CMCC

Use Cases for DDoS Open Threat Signaling (DOTS) Telemetry

Abstract

Denial-of-service 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: 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

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, multi-vendor 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 multi-vendor elements [RFC9132][RFC8783]. DOTS Telemetry enriches the DOTS protocols with various telemetry attributes allowing optimal DDoS attack mitigation [I-D.ietf-dots-telemetry]. This document presents sample use cases for DOTS Telemetry, which makes concrete overview and purpose described in [I-D.ietf-dots-telemetry]: 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] and [I-D.ietf-dots-telemetry].

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 DOTS telemetry specifications [I-D.ietf-dots-telemetry].

3.1. Mitigation Resources Assignment

3.1.1. Mitigating Attack Flow of Top-talker Preferentially

Recent reported large DDoS attacks which exceeded 1 Tps. Some transit providers have to mitigate such large-scale DDoS attacks using DMSes (DDoS Mitigation System) with limited resources, which is already deployed in their network.

The aim of this use case is to enable 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.

```
(Internet Transit Provider)

               +-----------+      +--------------+ e.g., SNMP
  e.g., IPFIX +-----------+| DOTS |              |<---
        --->| Flow      ||C<-->S| Orchestrator | e.g., BGP Flowspec
              | collector |+      |              |--->   (Redirect)
              +-----------+       +--------------+

                         +--------------+
            e.g., IPFIX +-------------+| e.g., BGP Flowspec
                    <---| Forwarding  ||<---   (Redirect)
                        |    nodes    ||
                        |             ||           DDoS Attack
[ Target  ]<============|================================
[   or    ]             |    ++=========================[top talker]
[ Targets ]             |    || ++======================[top talker]
                        +----|| ||---+
                             || ||
                             || ||
                             |/ |/
                        +----x--x----+
                        | DDoS       | e.g., SNMP
                        | mitigation |<---
                        | system     |
                        +------------+

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

Figure 1: Mitigating DDoS Attack Flow of Top-talker 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": "1644539068",
            "attack-severity": "high",
            "top-talker":{
              "talker": [
                {
                  "source-prefix": "2001:db8::2/128",
                  "total-attack-traffic": [
                    {
                      "unit": "megabit-ps",
                      "mid-percentile-g": "100"
                    }
                  ]
                },
                {
                  "source-prefix": "2001:db8::3/128",
                  "total-attack-traffic": [
                    {
                      "unit": "megabit-ps",
                      "mid-percentile-g": "90"
                    }
                  ]
                }
              ]
            }
          }
        ]
      }
    ]
  }
```

}

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

In this use case, the forwarding nodes send statics of traffic flow to the flow collectors using, e.g., IPFIX [RFC7011]. When DDoS attacks occur, the flow collectors identifies the attack traffic and send information of the top-talkers to the orchestrator using the "target-prefix" and "top-talkers" telemetry attributes. The orchestrator, then, checks the available capacity of the DMSes by using a network management protocol, such as SNMP [RFC3413]. After that, the orchestrator orders forwarding nodes to redirect as much of the top taker's traffic to the DMS as possible by dissemination of flow-specification-rules relying upon tools, such as BGP Flowspec [RFC8955].

In this use case, the flow collector implements a DOTS client while the orchestrator implements a DOTS server.

3.1.2. Optimal 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 under attack time.

The aim of this use case is to enable transit providers to select an optimal DMS 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)

```
               +-----------+      +--------------+ e.g., SNMP
  e.g., IPFIX +-----------+| DOTS |              |<---
          --->| Flow      ||C<-->S| Orchestrator | e.g., BGP
              | collector |+      |              |--->   (Redirect)
              +-----------+       +--------------+

                         +------------+
            e.g., IPFIX +------------+| e.g., BGP
                    <---| Forwarding ||<---   (Redirect)
                        |    nodes   ||
                        |            ||            DDoS Attack
[Target]                | ++============================
[Target]                | ||  ++========================
                        +-||--||-----+
                          ||  ||
                    ++====++  ||  (congested DMS)
                    ||        ||  +-----------+
                    ||        |/  |      DMS3 |
                    ||  +-----x------+        |<--- e.g., SNMP
                    |/  |       DMS2 |--------+
                 +--x---------+      |<--- e.g., SNMP
                 |       DMS1 |------+
                 |            |<--- e.g., SNMP
                 +------------+
```

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

Figure 3: Optimal DMS Selection for Mitigation

```
{
  "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"
          }
        ]
      }
    ]
  }
}
```

Figure 4: Example of Message Body with Total Attack Traffic

In this use case, the forwarding nodes send statics of traffic flow to the flow collectors using, e.g., IPFIX [RFC7011]. When DDoS attacks occur, the flow collectors identify attack traffic and send information of the attack traffic volume to the orchestrator using the "target-prefix" and "total-attack-traffic" telemetry attributes. The orchestrator, then, checks the available capacity of the DMSes using a network management protocol, such as SNMP [RFC3413]. After that, the orchestrator chooses an optimal DMS to which each attack traffic should be redirected. [Note: An example how the information used in the telemetry message is used to trigger the selection will be written]. The orchestrator then orders the appropriate forwarding nodes to redirect the attack traffic to the optimal DMS by a routing protocol such as BGP [RFC4271]. The DMS selection algorithm is out of the scope of this document.

In this use case, the flow collector implements a DOTS client while the orchestrator implements a DOTS server.

3.1.3. Best-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 selecting an available path.

The aim of this use case is to enable transit providers to select an optimal path 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
  e.g.,  +-----------+|      |              |S<---
   IPFIX | Flow      || DOTS | Orchestrator |
      -->| collector ||C<-->S|              | e.g., BGP Flow spec
         |           |+      |              |--->   (Redirect)
         +-----------+       +--------------+

               DOTS +------------+  DOTS +------------+ e.g., IPFIX
               --->C| Forwarding |  --->C| Forwarding |--->
e.g., BGP Flow spec |   node     |       |   node     |
     (Redirect) --->|            |       |            |  DDoS Attack
[Target]            |       ++====================================
                    +-------||---+       +------------+
                            ||              /
                            ||             / (congested link)
                            ||            /
                    DOTS  +-||----------------+ e.g., BGP Flow spec
                     --->C| ||  Forwarding    |<---   (Redirect)
                          | ++===  node       |
                          +----||-------------+
                               |/
                            +--x-----------+
                            |     DMS      |
                            +--------------+

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

Figure 5: Best-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: Example of Message Body with Total Attack Traffic and Total Tr

In this use case, the forwarding nodes send statics of traffic flow to the flow collectors using, e.g., IPFIX [RFC7011]. When DDoS attacks occur, the flow collectors identify attack traffic and send information of the attack traffic volume to the orchestrator using a "target-prefix" and "total-attack-traffic" telemetry attributes. On the other hands, forwarding nodes send volume of the total traffic passing the node to the orchestrator using "total-traffic" telemetry attributes. [Note: Should forwarding nodes send the volume of the total traffic passing the node using telemetry? IPFIX or SNMP is enough to send ths information.] The orchestrator then selects an optimal path to which each attack-traffic flow should be redirected. [Note: An example how this information is used to selection a non-congested path will be written] After that, the orchestrator orders the appropriate forwarding nodes to redirect the attack traffic to the optimal DMS by dissemination of flow-specification-rules relying upon tools, such as BGP Flowspec [RFC8955]. Path selection algorithm is out of the scope of this document.

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. [Note: Pointer of pulse wave DDoS attacks will be written] It is difficult for them to mitigate an attack by DMS by redirecting attack flows because it 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.

The aim of this use case is to enable 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 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 various attack traffic percentiles and total traffic percentiles.

```
(Internet Transit Provider)

          +------------+       +----------------+
e.g.,     | Network    |  DOTS | Administrative |
Alert --->| Management |C<--->S| System         | e.g., BGP Flow spec
          | System     |       |                |--->   (Rate-Limit)
          +------------+       +----------------+

            +------------+     +------------+ e.g., BGP Flow spec
            | Forwarding |     | Forwarding |<---  (Rate-Limit X bps)
            |   node     |     |   node     |
            |            |     |            | DDoS & Normal traffic
[Target]<------------------------------------================
Pipe        +------------+     +------------+  Attack Traffic
Capability                                     Bandwidth
e.g., X bps                                    e.g., Y bps

                    Network access success rate
                        e.g., X / (X + Y)

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

Figure 7: Short but Extreme Volumetric Attack Mitigation

```
{
  "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 8: Example of Message Body with Total Attack Traffic and Total Tr

In this use case, when DDoS attacks occur, the network management system receives alerts. Then, it sends the target IP address and volume of the DDoS attack traffic to the administrative system using the "target-prefix" and "total-attack-traffic" telemetry attributes. After that, the administrative system orders upper forwarding nodes to carry out rate-limit all traffic destined to the target based on the pipe capability by the dissemination of the flow-specification-rules relying upon tools, such as 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 gatherd by telemetry setup in advance. [Note: An example of telemetry pipe setup message will be written]

3.1.5. Selecting Mitigation Technique Based on Attack Type

Some volumetric attacks, such as 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 using IPFIX[RFC7011]. On the other hand, it is necessary to inspect the Layer 7 information of attack packets to detect attacks such as DNS Water Torture Attacks. Such attack traffic should be detected and mitigated at a DMS.

The aim of this use case is to enable transit providers to select a mitigation technique based on the type of attack traffic: amplification attack or not. To use such a technique, attack traffic is blocked at forwarding nodes or redirected to a DMS based on attack type through cooperation among forwarding nodes, flow collectors, and an orchestrator. Figure 9 gives an overview of this use case. Figure 10 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.

```
  (Internet Transit Provider)

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

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

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

Figure 9: DDoS Mitigation Based on Attack Type

```
{
  "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": "1644539068",
            "attack-severity": "high"
          },
          {
            "vendor-id": 32473,
            "attack-id": 92,
            "start-time": "1644539080",
            "attack-severity": "high"
          }
        ]
      }
    ]
  }
}
```

In this example, attack mappings as below are shared using data-channel

```
{
  "ietf-dots-mapping:vendor-mapping": {
    "vendor": [
      {
        "vendor-id": 32473,
        "vendor-name": "mitigator-c",
        "last-updated": "1629898958",
        "attack-mapping": [
          {
            "attack-id": 77,
            "attack-description":
               "attack-description": "DNS amplification Attack: This att
          },
          {
            "attack-id": 92,
            "attack-description":
               "attack-description":"NTP amplification Attack: This atta
          }
        ]
      }
    ]
  }
}
```

Figure 10: Example of Message Body with Total Attack Traffic, Total Atta

In this use case, the forwarding nodes send statics of traffic flow to the flow collectors using, e.g., IPFIX [RFC7011]. When DDoS attacks occur, the flow collectors identify attack traffic and send attack type information to the orchestrator the using "vendor-id" and "attack-id" telemetry attributes. The orchestrator then resolves abused port and orders forwarding nodes to block the amp attack traffic flow by dissemination of flow-specification-rules relying upon tools, such as BGP Flowspec [RFC8955]. On the other hand, the orchestrator orders forwarding nodes to redirect other traffic than the amp attack traffic by a routing protocol such as BGP [RFC4271].

In this use case, 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 on-going and detailed DDoS countermeasure status to the enterprise network. In addition, it is possible for the transit provider to know whether the DDoS counter measure is effective or not by receiving reports from the enterprise network.

The aim of this use case is to share the information about on-going DDoS counter measure between the transit provider and the enterprise network mutually. Figure 11 gives an overview of this use case. Figure 12 provides an example of a DOTS telemetry message body that is used to signal various total traffic percentiles, total attack traffic percentiles and attack detail.

```
  +------------------+      +------------------------+
  | 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          |========
  |  +---------+     | Link |   +---------------+    |
  +------------------+      +------------------------+
```

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

Figure 11: Detailed DDoS Mitigation Report

```
{
  "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": "1644539068",
            "attack-severity": "high"
          }
        ]
      }
    ]
  }
}
```

Figure 12: Example of Message Body with Total Traffic, Total Attack Traf

In this use case, 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 "total-pipe-capacity" in DOTS telemetry setup. [Note: An example of total-pipe-capacity message will be written]

When DDoS attacks occur, DDoS Orchestration [RFC8903] is carried out in the transit provider. Then, the DDoS mitigation systems reports status of DDoS counter measure to the orchestrator sending "attack-detail" telemetry attributes. After that, the orchestrator integrates the reports from the DDoS mitigation system, while removing duplicate contents, and send it to network administrator using DOTS telemetry periodically.

During the DDoS mitigation, the orchestrator in the transit provider retrieves link congestion status from the network administrator in the enterprise network using "total-traffic" telemetry attributes. [Note: An example of total-traffic message will be written] Then, the orchestrator checks whether DDoS countermeasure is effective or not by comparing the "total-traffic" and the "total-pipe-capacity".

In this use case, the DMS implements a DOTS server while the orchestrator implements a DOTS client and 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 [RFC7011], is a lighter weight method of detecting DDoS attacks than DMSes in internet transit provider networks. On the other hand, DDoS detection based on the DMSes is a more accurate method of detecting attack traffic or DDoS attacks better than flow monitoring.

The aim of this use case is to increases flow collector's 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 collector, and a DMS should cooperate. 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 various total attack traffic percentiles and attack detail.

```
                                   +-----------+
                                  +-----------+| DOTS
                      e.g., IPFIX | Flow      ||S<---
                              --->| collector ||
                                  +-----------++

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

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

Figure 13: Training Supervised Machine Learning of Flow Collector

```
{
  "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": "1644539068",
            "attack-severity": "high",
            "top-talker": {
              "talker": [
                {
                  "source-prefix": "2001:db8::2/128"
                },
                {
                  "source-prefix": "2001:db8::3/128"
                }
              ]
            }
          }
        ]
      }
    ]
  }
}
```


Figure 14: Example of Message Body with Attack Type and Top Talkers

In this use case, the forwarding nodes send statics of traffic flow to the flow collectors using, e.g., IPFIX [RFC7011]. When DDoS attacks occur, DDoS orchestration use case [RFC8903] is carried out 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 the flow collector.

After mitigating a DDoS attack, the flow collector attaches teacher labels, which shows normal traffic or attack type, to the statistics of traffic flow of top-talkers based on the reports. 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.

In this use case, 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. The aim of this use case is to carry out unsupervised machine-learning for anomaly detection according to baseline reported by DMSes. To use such a technique, forwarding nodes, flow collector, and a DMS should cooperate. Figure 15 gives an overview of this use case. Figure 16 provides an example of a DOTS telemetry message body that is used to signal baseline.

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

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

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

Figure 15: Training Unsupervised Machine Learning of Flow Collector

```
{
  "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",
                "mid-percentile-g": "30",
                "mid-percentile-g": "50",
                "high-percentile-g": "60",
                "peak-g": "70"
              }
            ]
          }
        ]
      }
    ]
  }
}
```


Figure 16: Example of Message Body with Baseline

In this use case, the forwarding nodes carry out mirroring traffic destined "dst-ip" address. The DMS then identifies "clean" traffic and reports the baseline attributes to the flow collector using DOTS telemetry.

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

In this use case, 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 [I-D.ietf-dots-telemetry]. This document does not add new considerations.

5. IANA Considerations

This document does not require any action from IANA.

6. Acknowledgement

The authors would like to thank among others Mohamed Boucadair for their valuable feedback.

7. References

7.1. Normative References

[I-D.ietf-dots-telemetry] Boucadair, M., Reddy.K, T., Doron, E., Chen, M., and J. Shallow, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Telemetry", Work in Progress, Internet-Draft, draft-ietf-dots-telemetry-23, 4 February 2022, <https://www.ietf.org/archive/id/draft-ietf-dots-telemetry-23.txt>.

7.2. Informative References

[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>.

[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>.

[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