DOTS   Y. Hayashi
Internet-Draft   NTT
Intended status: Informational   M. Chen
Expires: December 4, 2021   Li. Su
                                                                    CMCC
                                                          June 02, 2021

          Use Cases for DDoS Open Threat Signaling (DOTS) Telemetry
                  draft-ietf-dots-telemetry-use-cases-02

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

   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 December 4, 2021.

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 automated.
   To automate DDoS-attack mitigation, multi-vendor components involved
   in DDoS-attack detection and mitigation should cooperate and support
   standard interfaces to communicate.

   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 [RFC8782][RFC8783]. Furthermore, 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]

In addition, this document uses the following terms:

Top-talker: A top N list of attackers who attack the same target or
   targets. The list is ordered in terms of a two-tuple bandwidth
   such as bps or pps.

Supervised Machine Learning: A machine-learning technique that maps
   an input to an output based on example input-output pairs.

Unsupervised Machine Learning: Unsupervised Learning is a machine
   learning technique in which the users do not need to supervise the
   model.

3. Use Cases

This section describes DOTS-Telemetry use cases that use attributes
included in DOTS Telemetry specifications.

4. Mitigation Resources Assignment

4.1. Mitigating Attack Flow of Top-talker Preferentially

Large-scale DDoS attacks, such as amplification attacks, often occur.
Some transit providers have to mitigate large-scale DDoS attacks
using DMS 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 bandwidth is
more than the available capacity of the DMS. To enable this, 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.

(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     |
                 +-----------+
```
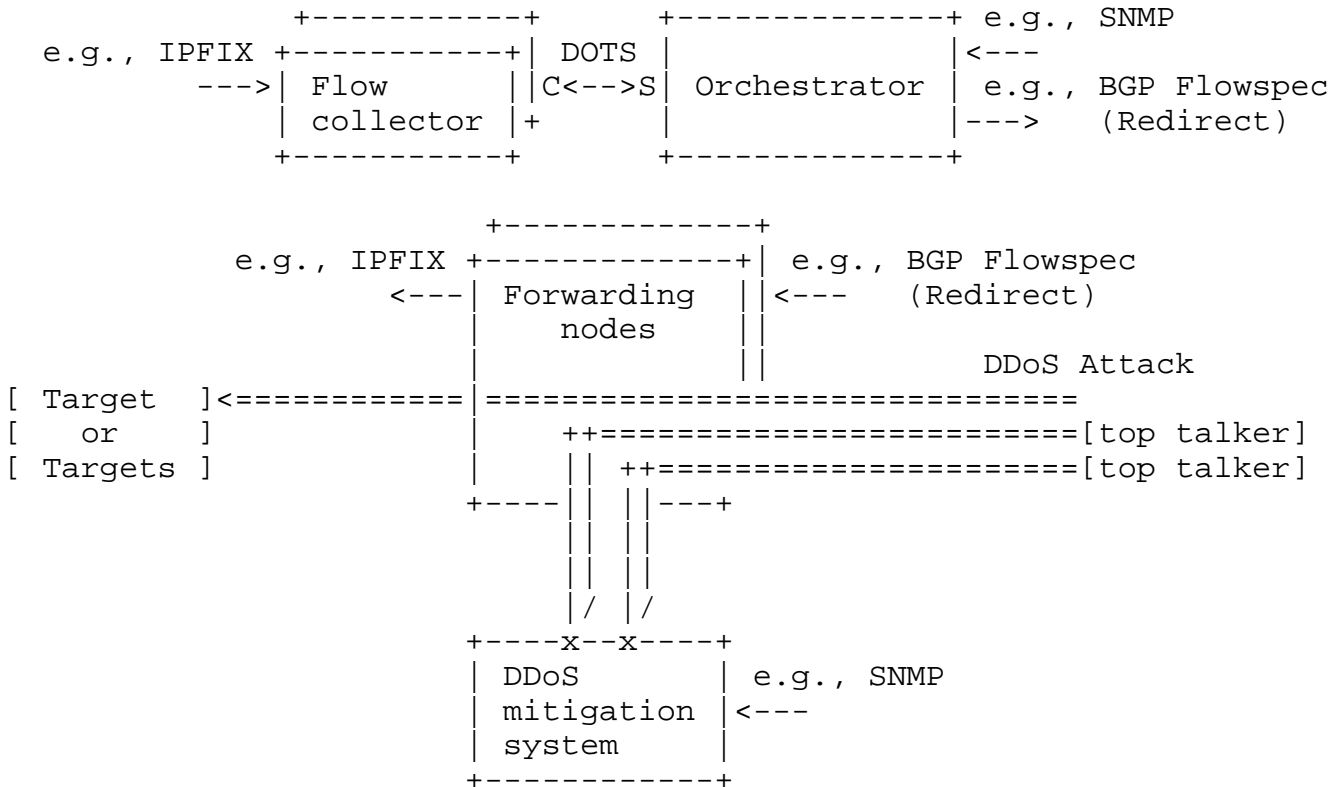
* C is for DOTS client functionality
* S is for DOTS client functionality

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

In this use case, the forwarding nodes always send statistics of
traffic flow to the flow collectors by using monitoring functions
such as IPFIX[RFC7011]. When DDoS attacks occur, the flow collectors
detect attack traffic and send (src_ip, dst_ip, bandwidth)-tuple
information of the top talker to the orchestrator using the target-
prefix and top-talkers attribute of DOTS Telemetry. The orchestrator
then checks the available capacity of DMS 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-
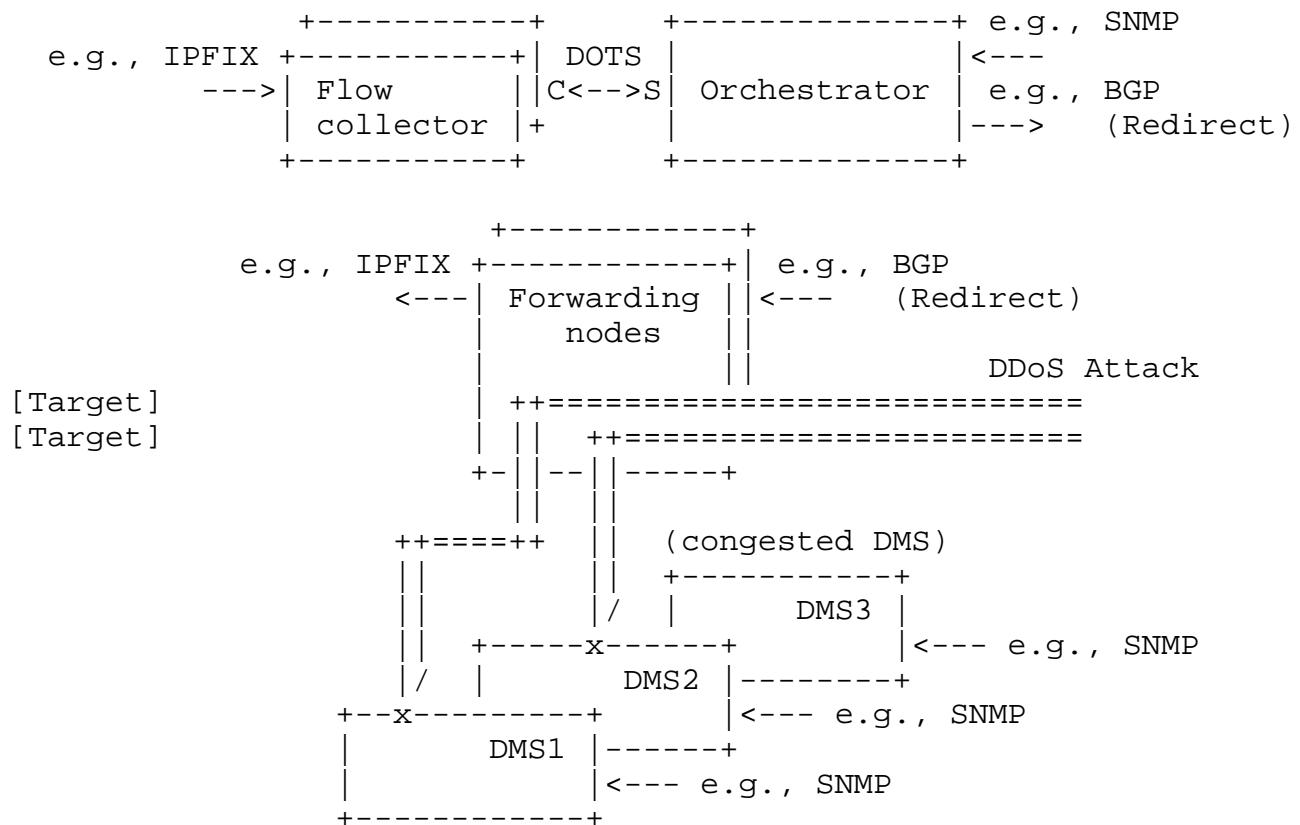specification-rule protocols such as BGP Flowspec[RFC5575].

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

4.2. Optimal DMS Selection for Mitigation

   Transit providers, which have a number of DMSs, can deploy the DMSs
   in clustered form. In the form, they can select DMS to be used to
   mitigate 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 bandwidth of attack traffic,
   capacity of a DMS. Figure 2 gives an overview of this use case.

   (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 |--------+
      |/ |            |<--- e.g., SNMP
   +--x---------+           |
   |    DMS1 |------+
   |         |<--- e.g., SNMP
   +-----------+
```

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

   Figure 2: Optimal DMS selection for Mitigation

   In this use case, the forwarding nodes always send statistics of
   traffic flow to the flow collectors by using monitoring functions
   such as IPFIX[RFC7011]. When DDoS attacks occur, the flow collectors
   detect attack traffic and send (dst_ip, bandwidth)-tuple information
   to the orchestrator using the target-prefix and total-attack-traffic
   attribute of DOTS Telemetry. The orchestrator then checks the

available capacity of the DMSs by using a network management protocol
such as SNMP[RFC3413]. After that, the orchestrator chooses optimal
DMS which each attack traffic should be redirected. The orchestrator
then orders forwarding nodes to redirect the attack traffic to the
optimal DMS by a routing protocol such as BGP[RFC4271]. The
algorithm of selecting a DMS is out of the scope of this draft.

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

4.3. Best-path Selection for Redirection

A transit-provider network, which adopts a mesh network, has multiple
paths to convey attack traffic to a DMS. In this network, 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, total traffic, and total pipe
capability. Figure 3 gives an overview of this use case.

(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       |
            +-------------+
```
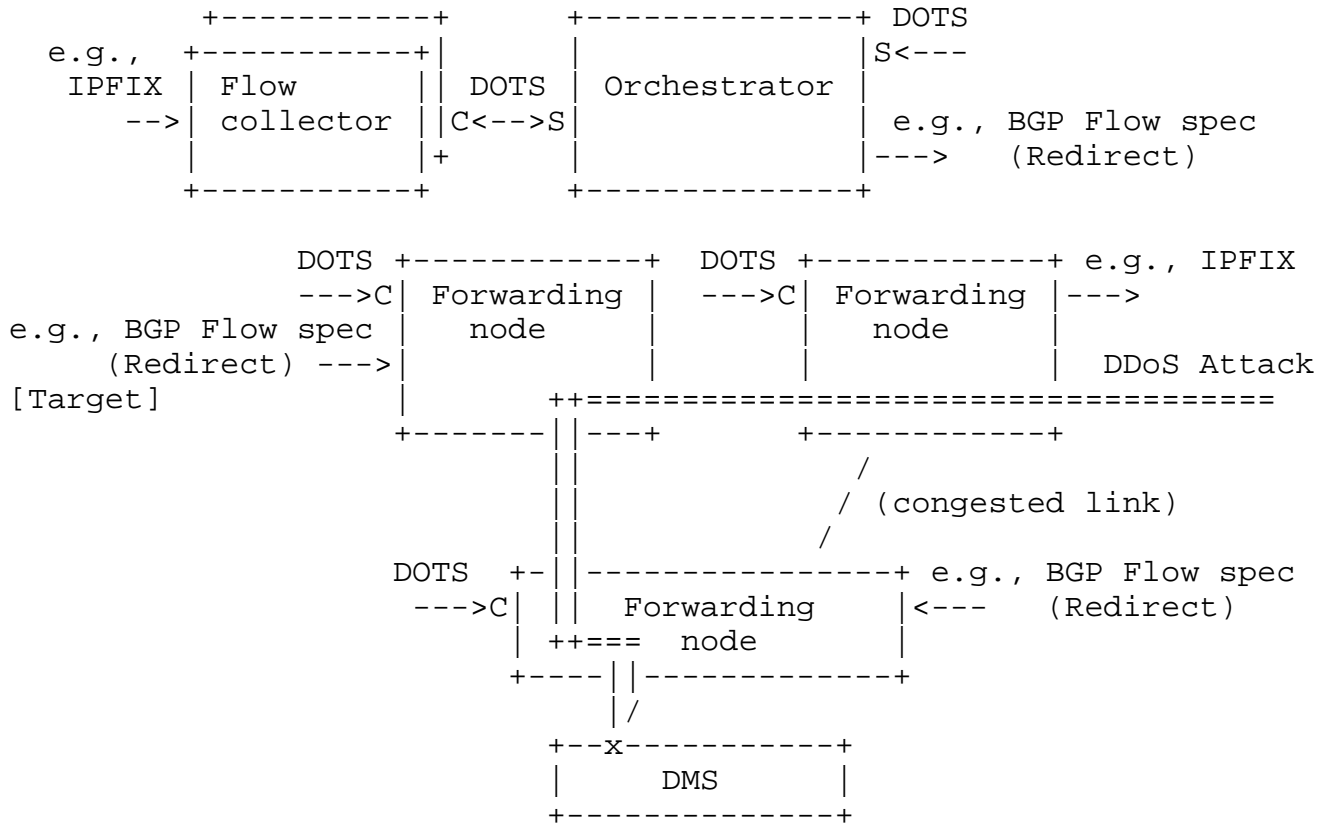
* C is for DOTS client functionality
* S is for DOTS client functionality

Figure 3: Best-path Selection for Redirection

In this use case, the forwarding nodes always send statistics of
traffic flow to the flow collectors by using monitoring functions
such as IPFIX[RFC7011]. When DDoS attacks occur, the flow collectors
detect attack traffic and send (dst_ip, bandwidth)-tuple information
to the orchestrator using a target-prefix and total-attack-traffic
attribute of DOTS Telemetry. On the other hands, forwarding nodes
send bandwidth of total traffic passing the node and total pipe
capability to the orchestrator using total-traffic and total-pipe-
capability attributes of DOTS Telemetry. The orchestrator then
selects an optimal path to which each attack-traffic flow should be
redirected. After that, the orchestrator orders forwarding nodes to
redirect the attack traffic to the optimal DMS by dissemination of
flow-specification-rules protocols such as BGP Flowspec[RFC5575].
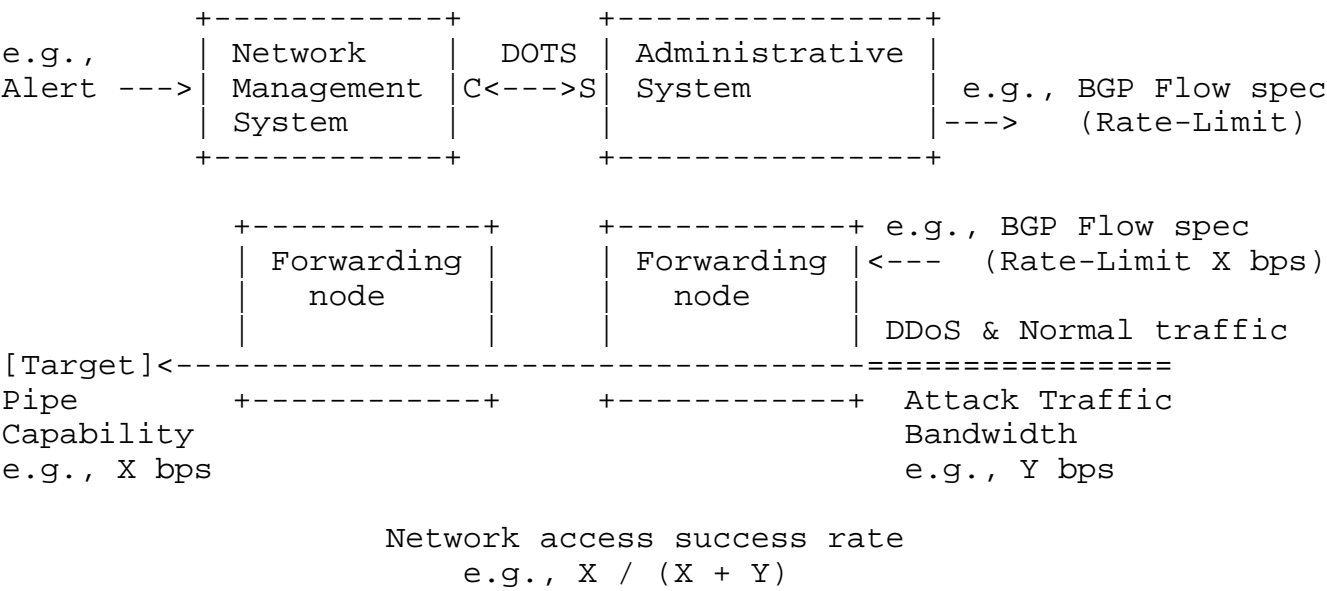The algorithm of selecting a path is out of the scope of this draft.

4.4. Short but Extreme Volumetric Attack Mitigation

   Short but extreme volumetric attacks, such as pulse wave DDoS
   attacks, are threats to internet transit provider networks. 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 a 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 and total pipe capability. Figure 4 gives an overview
   of this use case.

   (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 4: Short but Extreme Volumetric Attack Mitigation

   In this use case, when DDoS attacks occur, the network management
   system receives alerts. It then sends the target ip address, pipe
   capability of the target's link, and bandwidth of the DDoS attack
   traffic to the administrative system using the target-prefix, total-
   pipe-capability and total-attack-traffic attributes of DOTS
   Telemetry. 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 protocols such as BGP Flowspec[RFC5575]. 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).

5. 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 5 gives an overview of this use case.

```
   +------------------+       +-----------------------+
   | 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 |  +--------------+   |
   +------------------+       +-----------------------+
```
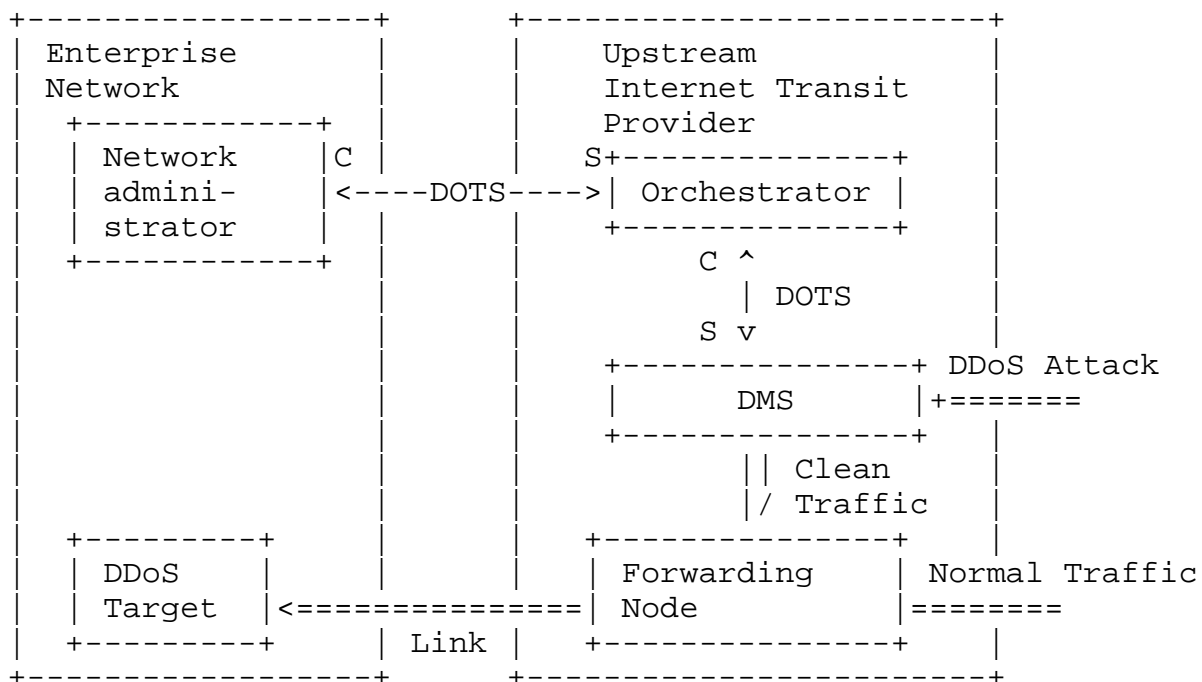
   * C is for DOTS client functionality
   * S is for DOTS server functionality

   Figure 5: Detailed DDoS Mitigation Report

   In this use case, the network managements system in the enterprise
   network reports limits of incoming traffic volume from transit

provider to the orchestrator in the transit provider in advance. It
is reported by using total-pipe-capacity in DOTS telemetry.

When DDoS attacks occurs, DDoS Orchestration [RFC8903] is carried out
in the transit provider. Then, the DDoS mitigation systems reports
status of DDoS counter measure to the orchestrator by using DOTS
telemetry such as attack-detail. After that, the orchestrator
integrates the reports from the DDoS mitigation system, while
removing duplicate contents, and send it to network administrator by
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 by using total-traffic in DOTS telemetry.
Then, the orchestrator checks whether DDoS countermeasure is
effective or not by comparing the total-traffic and the total-pipe-
capacity.

In this 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.

6. Tuning Mitigation Resources

6.1. Supervised Machine Learning of Flow Collector

DDoS detection based on monitoring functions, such as IPFIX[RFC7011],
is a lighter weight method of detecting DDoS attacks than DMSs in
internet transit provider networks. On the other hand, DDoS
detection based on the DMSs 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 DMSs. To use such a
technique, forwarding nodes, flow collector, and a DMS should
cooperate. Figure 6 gives an overview of this use case.

```
                          +-----------+
                          +-----------+| 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
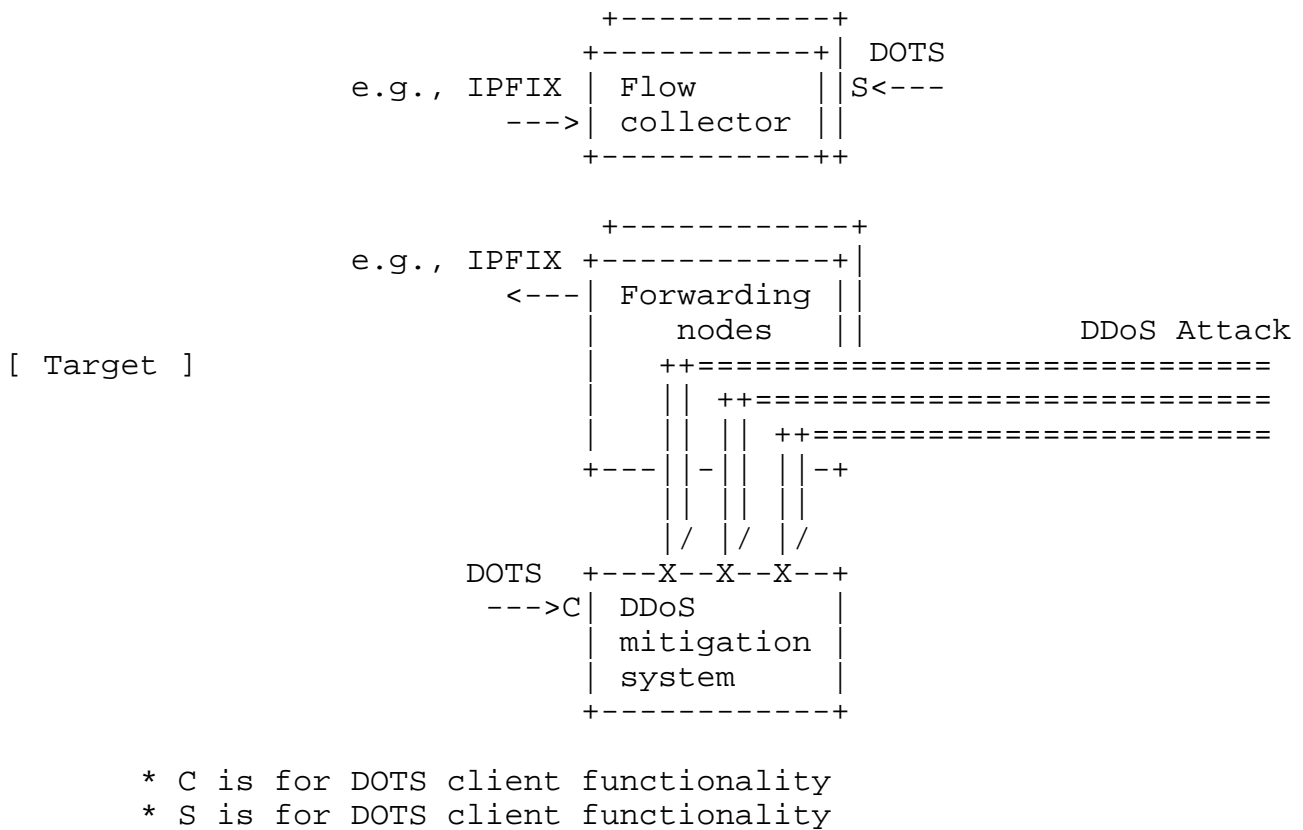   * S is for DOTS client functionality

Figure 6: Training Supervised Machine Learning of Flow Collector

In this use case, the forwarding nodes always send statistics of
traffic flow to the flow collectors by using monitoring functions
such as 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 to the flow collector using
DOTS telemetry.

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-talker 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 case, the DMS implements a DOTS client while the flow
collector implements a DOTS server.

6.2. Unsupervised Machine Learning of Flow Collector

   DMSs can detect DDoS attack traffic, which means DMSs 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 DMSs. To use such a technique, forwarding
   nodes, flow collector, and a DMS should cooperate. Figure 7 gives an
   overview of this use case.

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


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

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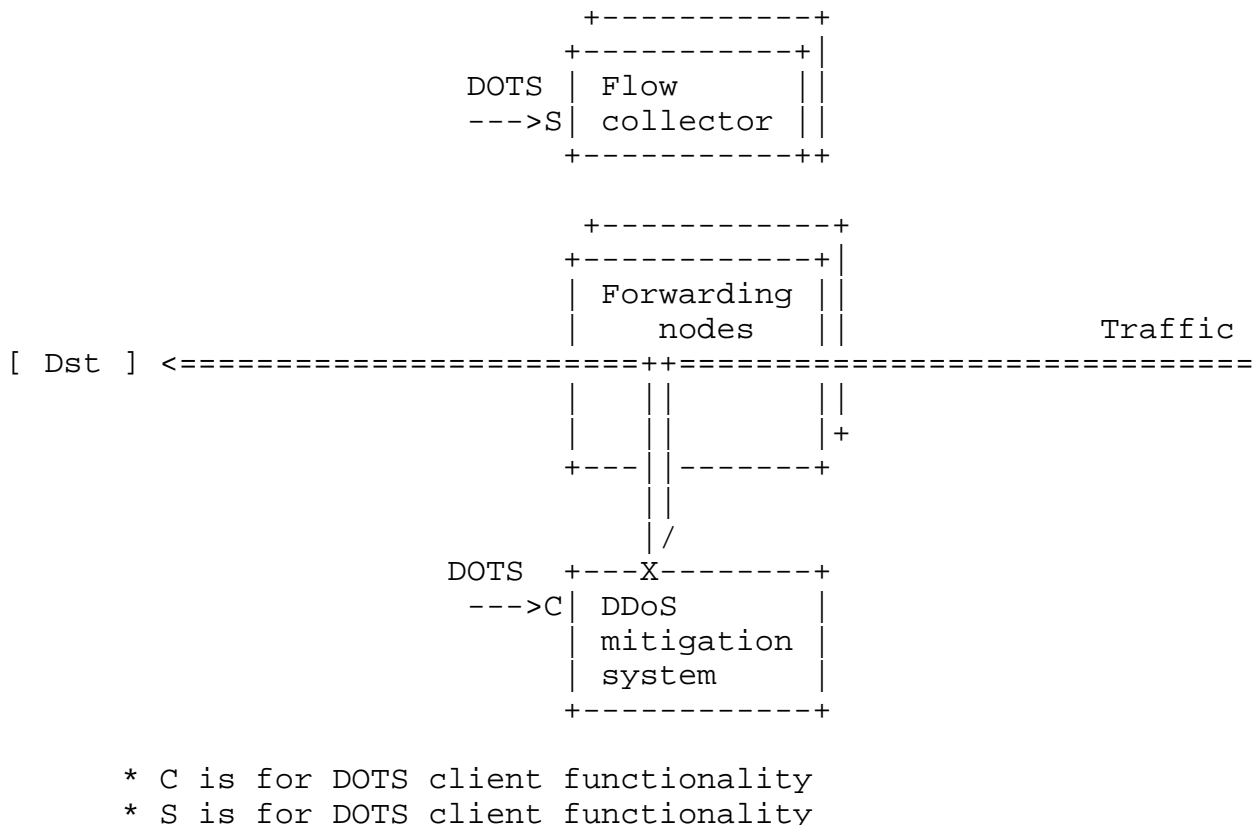   * S is for DOTS client functionality

   Figure 7: Training Unsupervised Machine Learning of Flow Collector

   In this use case, the forwarding nodes carry out mirroring traffic
   destined a 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 case, the DMS implements a DOTS client while the flow
   collector implements a DOTS server.

7. Security Considerations

    TBD

8. IANA Considerations

    This document does not require any action from IANA.

9. Acknowledgement

    TBD

10. References

10.1. Normative References

    [I-D.ietf-dots-telemetry]
               Boucadair, M., Reddy, T., Doron, E., Chen, M., and J.
               Shallow, "Distributed Denial-of-Service Open Threat
               Signaling (DOTS) Telemetry", draft-ietf-dots-telemetry-15
               (work in progress), December 2020.

    [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>.

    [RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J.,
               and D. McPherson, "Dissemination of Flow Specification
               Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009,
               <https://www.rfc-editor.org/info/rfc5575>.

    [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>.

   [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>.

10.2. Informative References

   [RFC8782] Reddy.K, T., Ed., Boucadair, M., Ed., Patil, P.,
              Mortensen, A., and N. Teague, "Distributed Denial-of-
              Service Open Threat Signaling (DOTS) Signal Channel
              Specification", RFC 8782, DOI 10.17487/RFC8782, May 2020,
              <https://www.rfc-editor.org/info/rfc8782>.

   [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>.

Authors' Addresses

   Yuhei Hayashi
   NTT
   3-9-11, Midori-cho
   Musashino-shi, 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   100053
   China

   Email: suli@chinamobile.com