DOTS
Internet-Draft
Intended status: Informational
Expires: June 4, 2020

Y. Hayashi
NTT
M. Chen
CMCC

December 2, 2019

Use Cases for DDoS Open Threat Signaling (DOTS) Telemetry
draft-hayashi-dots-telemetry-use-cases-00

Abstract

DOTS Telemetry enriches base DOTS protocol to assist the mitigator to perform efficient DDoS attack mitigation techniques in the network. This document presents sample use cases for DOTS telemetry: what components are deployed in the network, how they collaborate, and what information is exchanged to perform the 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 June 4, 2020.

Copyright Notice

Table of Contents

1. Introduction

Denial-of-Service (DDoS) attacks such as volumetric attacks or 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 the service providers to immediately protect their network services from DDoS attacks, DDoS mitigation needs to be automated. To automate DDoS attack mitigation, it is desirable that multi-vendor elements involved in DDoS attack detection and mitigation collaborate 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 [I-D.ietf-dots-signal-channel][I-D.ietf-dots-data-channel]. Furthermore, DOTS Telemetry enriches the DOTS protocol with various telemetry attributes allowing optimal DDoS attack mitigation [I-D.ietf-dots-telemetry]. This document presents sample use cases for DOTS telemetry: what components are deployed in the network, how

they collaborate, and what information is exchanged to perform the attack mitigation techniques.

2. Terminology

The readers should be familiar with the terms defined in [RFC8612]

In addition, this document makes use of 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

3. Use Cases

This section describes DOTS Telemetry use cases which uses attributes included in DOTS telemetry spec.

3.1. DDoS Mitigation Based on Attack Traffic Bandwidth

3.1.1. Mitigating Attack Flow of Top-talker Preferentially

Large-scale DDoS attack such as amplification attack often occurs in the world these days. On the other hand, many transit providers have to mitigate the large-scale DDoS attack using DMS with limited resources, which is already deployed in their network.

The aim of this use case is to enable the transit providers to use their DMS efficiently under volume-based DDoS attacks whose bandwidth is more than the available capacity of the DMS. To perform it, attack traffics of top talkers are redirected to their DMS preferentially by collaborating forwarding nodes, flow collectors and orchestrators. Figure 1 shows the abstract of the use case.

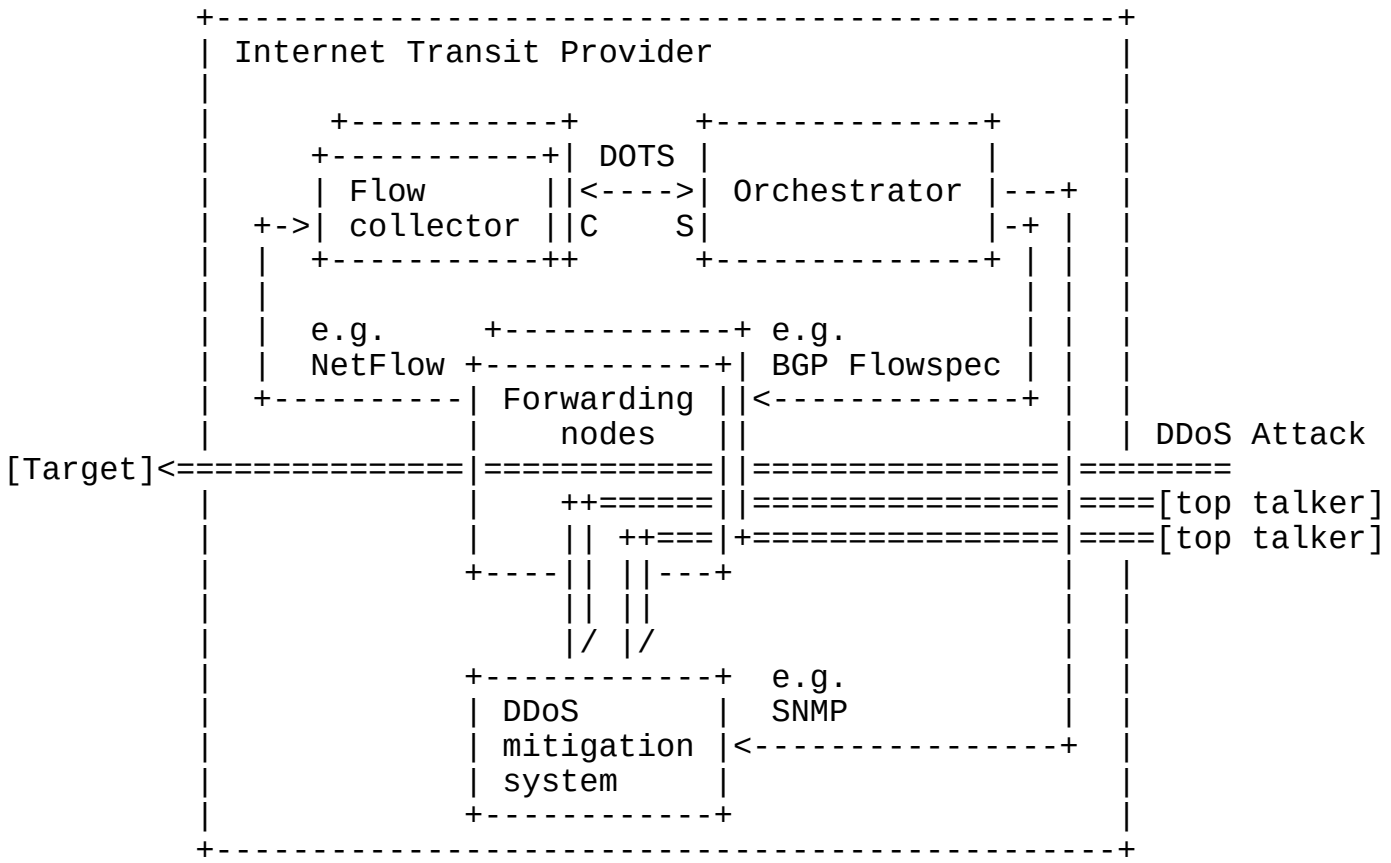


Figure 1: Mitigating DDoS Attack Flow of Top-talker Preferentially

In the use case, the forwarding nodes always send statistics of traffic flow to the flow collectors by using monitoring functions such as NetFlow. 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 top-talkers attribute of DOTS Telemetry. Then, the orchestrator checks the available capacity of DMS. After that, the orchestrator orders forwarding nodes to redirect the top taker’s traffic to the DMS as much as possible by dissemination of flow specification rules protocols such as BGP Flowspec [RFC5575].

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

3.1.2. Selecting Available DMS

Usually, DDoS attack mitigation providers have a number of ddos clean devices which up to the capability of service, ddos clean device can exists in both individual and clustered forms that based on the network requirements, we can all identify it as a DMS, each DMS has three attributes: total capacity, surplus capacity, the last hop bandwidth(how to get the bandwidth of last hop can refer to segment routing technology). When ddos attack occurs, DOTS telemetry carries the value of total attack traffic, orchestrator based on the total attack traffic, and each DMS's triad parameters to select the optimal DMS for mitigation. How to make the decision of DMS will be based on the first principle that operate fast and efficiently, and the detail algorithm is out of scope, this scenario is suitable for scenarios that are sensitive to the processing capabilities of the DMS.

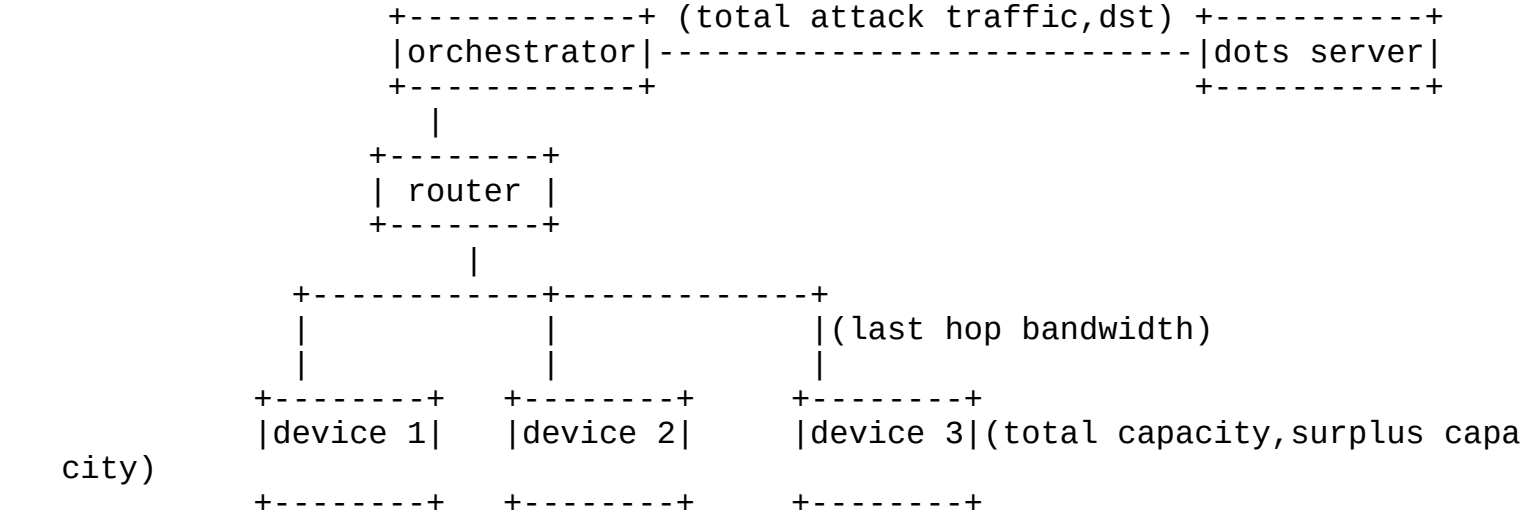


Figure 2: Optimal DMS selection for mitigation

3.1.3. Selecting Best Path for Redirection

Choosing the appropriate path for traffic redirection can also based on the total attack traffic and total pipe capability, but only internet service providers have the ability to know the overall load capacity of each physical paths and load limitation. ISP has many DMS and they are deployed according to the administrative division. After the ddos attack traffic are redirected to the DMS, DMS can perform cleaning operation and inject the normal service flow back. From the perspective of network load management, how to select the bast way to redirect requires the calculation on total attack traffic(TAT),total traffic(TT) and total pipe capability(TPC).

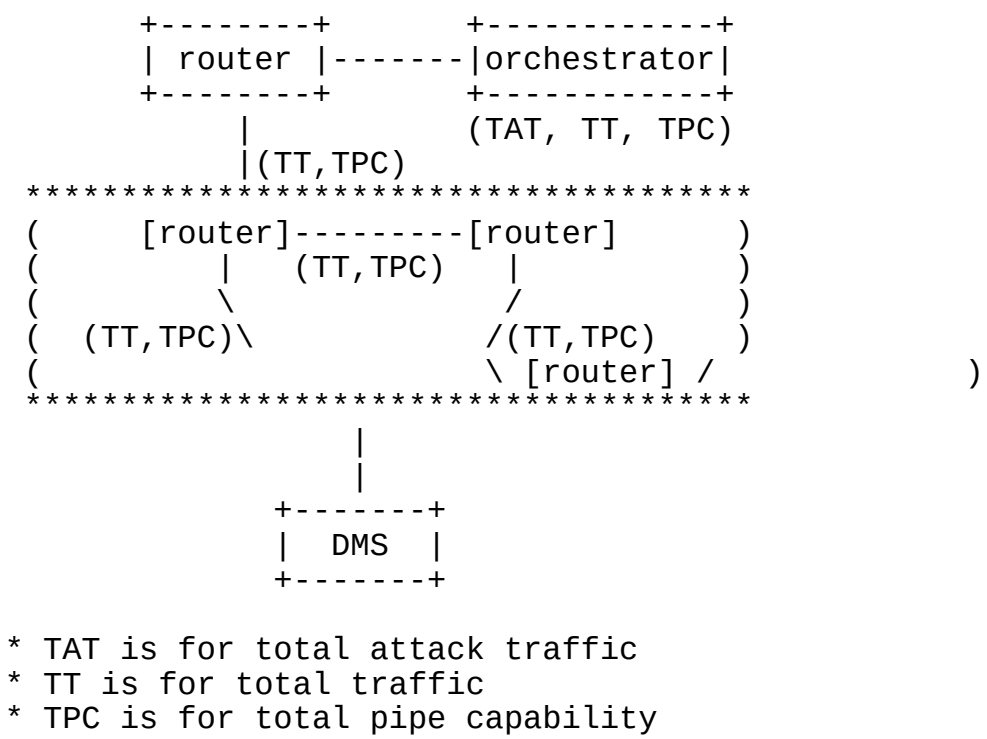


Figure 3: Optimal redirection path for mitigation

3.1.4. Offloading Extream Volumetric Attack Flow

Typically, the bandwidth between the attack target and the previous hop route is fixed because the bandwidth is charged based on the size of the bandwidth. If there is a large amount of attack traffic, the whole link is already full, and the attack traffic cannot be mitigated through redirection and cleaning operation. In this case, direct discarding is usually adopted to ensure part of the normal service flow, and the patency of pipeline is given priority. How to identify a super large traffic attack, for example, the attack traffic is not only larger than the bandwidth of last hop, but also larger than the higher path hop, that means the excess traffic of bandwidth A will be discarded, and in this case no need to distinguish between attack traffic and normal traffic.

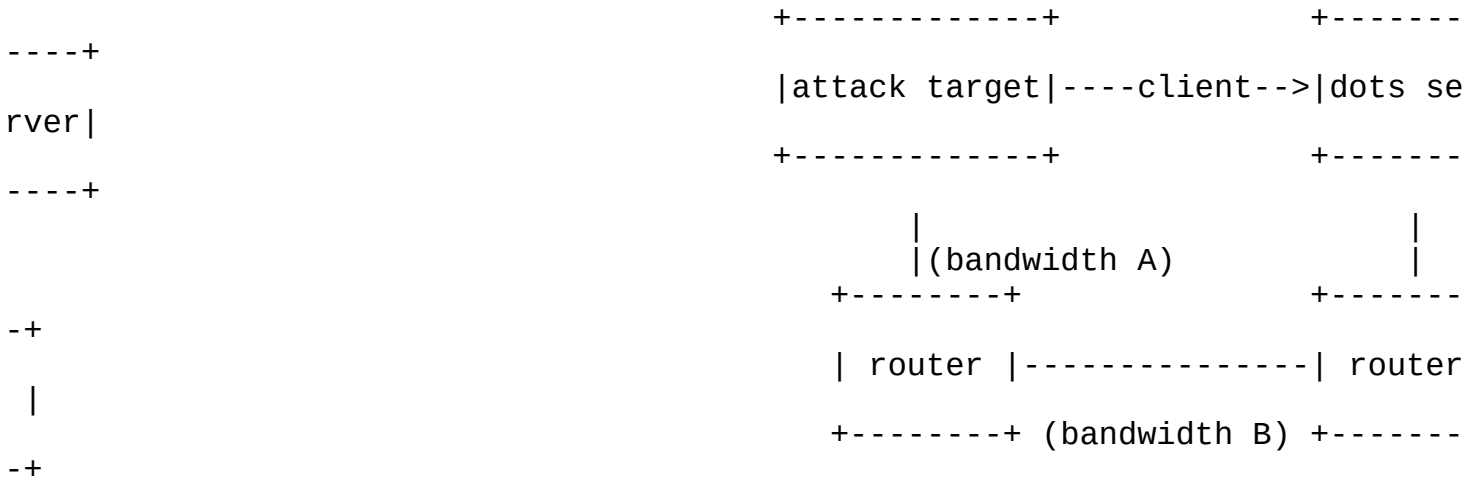


Figure 4: Offloading Extream Volumetric Attack Flow

3.2. DDoS Mitigation Based on Attack Type

3.2.1. Selecting Mitigation Technique

Some volumetric attacks such as amplification attack can be detected with high accuracy by checking layer 3 or layer 4 information of attack packets. These attacks can be detected and mitigated by collaborating forwarding nodes and flow collectors using NetFlow. On the other hand, it is necessary to inspect layer 7 information of attack packets to detect some attacks such as DNS Water Torture Attack. These attacks traffic should be detected and mitigated at DMS.

Aim of this use case is to enable the transit providers to select mitigation technique based on the type of attack traffic: amplification attack or not. To perform it, attack traffic is blocked at forwarding nodes or redirected to DMS base on attack type by collaborating forwarding nodes, flow collectors and an orchestrator. Figure 3 shows the abstract of the use case.

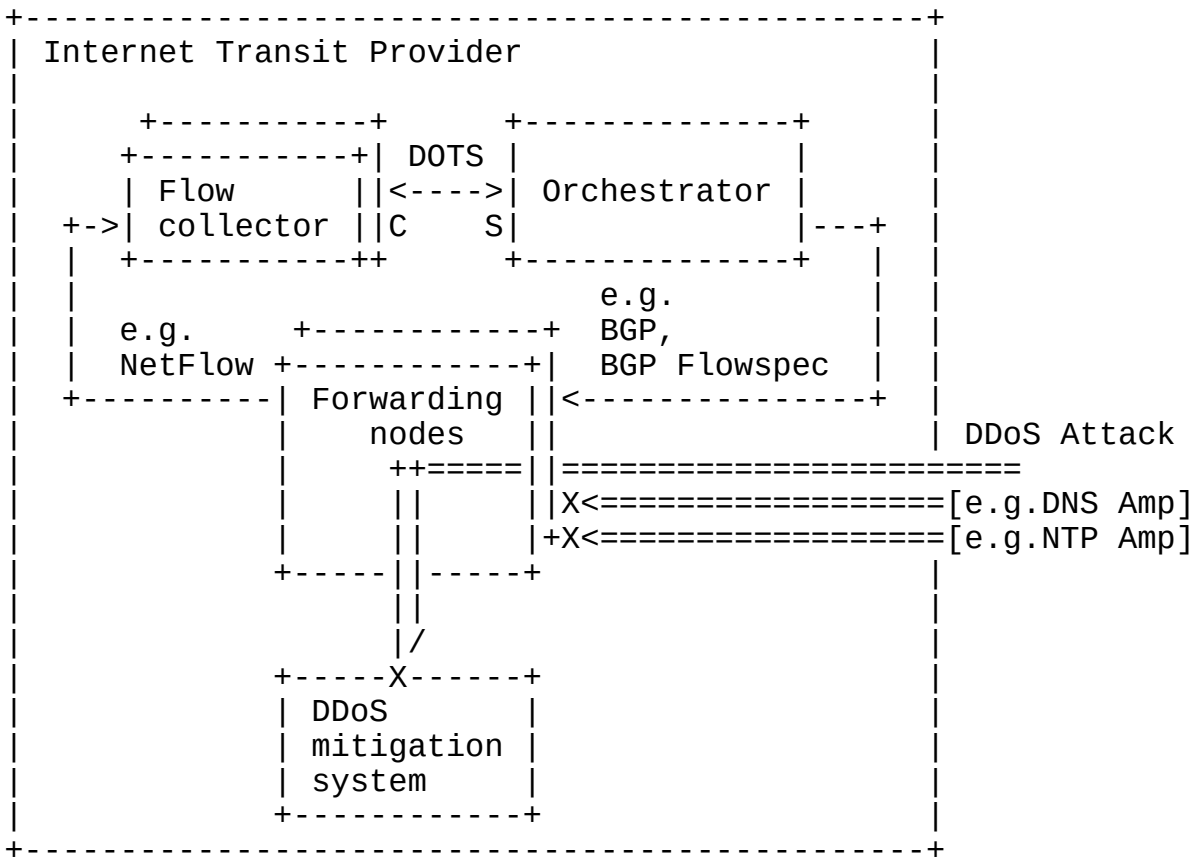


Figure 3: DDoS Mitigation Based on Attack Type

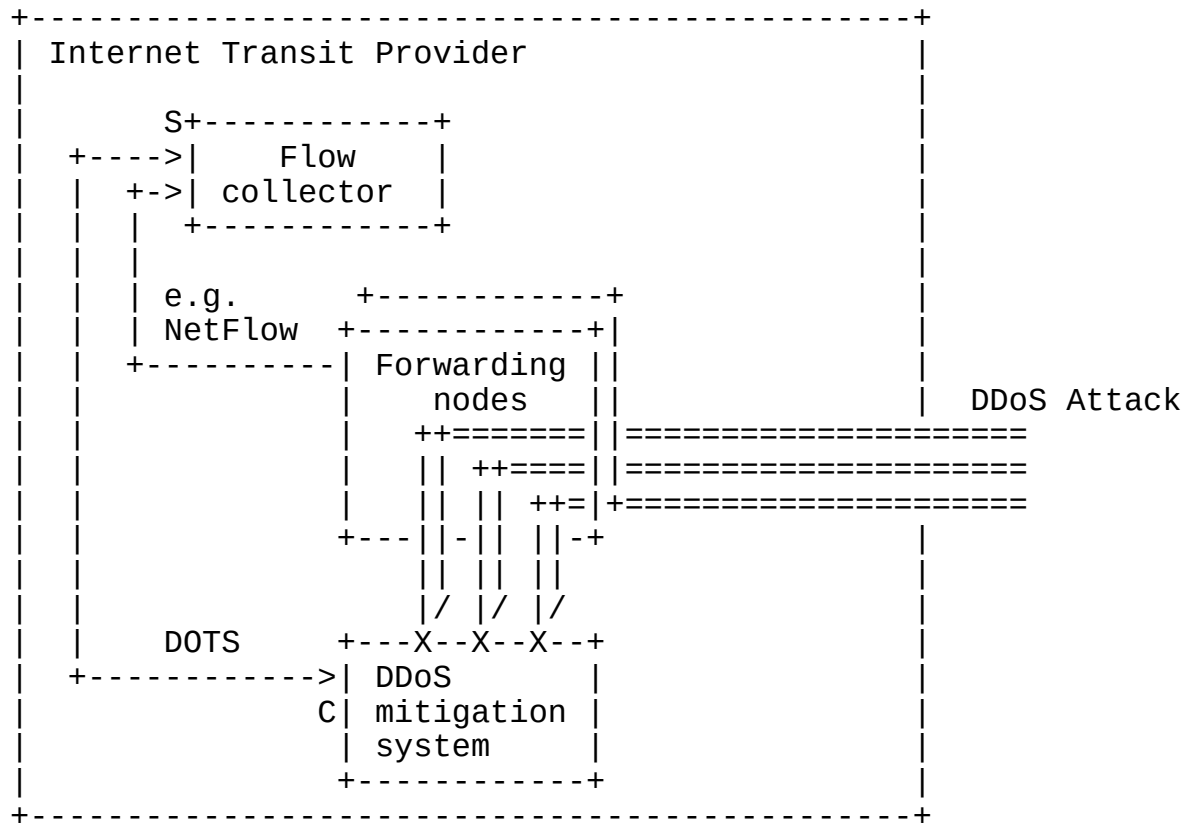
In the use case, the forwarding nodes send statistics of traffic flow to the flow collectors by using monitoring function such as NetFlow. When DDoS attacks occur, the flow collectors detect attack traffic and send (dst_ip, src_port, attack_type)-tuple information to the orchestrator, using attack-name attribute of DOTS Telemetry. Then, the orchestrator orders forwarding nodes to block (dst_ip, src_port)-tuple flow of amp attack traffic by dissemination of flow specification rules protocols such as BGP Flowspec[RFC5575]. On the other hand, the orchestrator orders forwarding nodes to redirect other than the amp attack traffic by routing protocol such as BGP[RFC4271].

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

3.3. Training Flow Collector Using Supervised Machine Learning

DDoS detection based on flow monitoring such as NetFlow is a lighter weight way to detect DDoS attacks than DMS in the internet transit provider network. On the other hand, DDoS detection based on DMS is a more accurate way to detect DDoS attacks than DDoS detection based on flow monitoring.

Aim of this use case is that the flow collector raises their detection accuracy performance carrying out supervised machine learning techniques based on the detection result of DMS. To perform it, forwarding nodes, flow collector and a DMS collaborate. Figure 5 shows the abstract of the use case.



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

Figure 5: Training Flow Collector Using Supervised Machine Learning

In the use case, the forwarding nodes always send statistics of traffic flow to the flow collectors by using monitoring functions such as NetFlow. When DDoS attacks occur, DDoS orchestration use case[I-D.ietf-dots-use-cases] is carried out and DMS mitigates all

attack traffic destined a target. Then, DDoS Mitigation system reports (src_ip, dst_ip)-tuple information of the top talker to the orchestrator, using top-talkers attribute of DOTS Telemetry.

After mitigating DDoS attack, the flow collector attaches labels, which shows normal traffic or attack traffic, to the stastistics of traffic flow based on the reports. Then, the flow collector carry out supervised machine learning to raise their detection accuracy, setting the statistics as explanatory variable and setting the labels as objective variable.

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

4. Security Considerations

TBD

5. IANA Considerations

This document does not require any action from IANA.

6. Acknowledgement

The authors would like to thank among others brabra...

7. References

7.1. Normative References

[I-D.ietf-dots-telemetry]
Boucadair, M., Reddy.K, T., Doron, E., and c. chenmeiling, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Telemetry", draft-ietf-dots-telemetry-02 (work in progress), February 2020.

[I-D.ietf-dots-use-cases]
Dobbins, R., Migault, D., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", draft-ietf-dots-use-cases-20 (work in progress), September 2019.

[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>.

[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>.

7.2. Informative References

[I-D.ietf-dots-data-channel] Boucadair, M. and T. Reddy.K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", draft-ietf-dots-data-channel-31 (work in progress), July 2019.

[I-D.ietf-dots-signal-channel] Reddy.K, T., Boucadair, M., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", draft-ietf-dots-signal-channel-41 (work in progress), January 2020.

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