DOTS
Internet-Draft
Intended status: Informational
Expires: January 6, 2020

Y. Hayashi
NTT
K. Nishizuka
NTT Communications
M. Boucadair
Orange

July 5, 2019

DDoS Mitigation Offload Use Case and DOTS Deployment Considerations
draft-hayashi-dots-dms-offload-usecase-01

Abstract

This document describes a DDoS mitigation offload use case and DOTS deployment consideration of the use case. This use case assumes that a DMS (DDoS Mitigation System) whose utilization rate is high sends its blocked traffic information to an orchestrator using DOTS protocols, then the orchestrator requests forwarding nodes such as routers to filter the traffic. Doing so enables service providers to mitigate DDoS attack traffic automatically while ensuring interoperability and distributed filter enforcement.

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 January 6, 2020.

Table of Contents

1. Introduction

Volume-based distributed denial-of-service (DDoS) attacks such as DNS amplification attacks are critical threats to be handled by service providers. When such 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 between the multi-vendor elements [I-D.ietf-dots-signal-channel] [I-D.ietf-dots-signal-call-home] [I-D.ietf-dots-signal-filter-control] [I-D.ietf-dots-data-channel]. This document describes an automated DDoS Mitigation offload use case

inherited from the DDoS orchestration use case [I-D.ietf-dots-use-cases], which ambitions to enable cost-effective DDoS Mitigation. Furthermore, this document describes deployment consideration for network operators who carry out this use-case using DOTS protocols in their network.

2. Terminology

The readers should be familiar with the terms defined in [I-D.ietf-dots-requirements] [I-D.ietf-dots-use-cases]

In addition, this document uses the terms defined below:

Mitigation offload: Getting rid of a DMS's mitigation action and assigning the action to another entity when the utilization rate of the DMS reaches a given threshold. How such threshold is set is deployment-specific.

Utilization rate: A scale to measure load of an entity such as link utilization rate or CPU utilization rate.

3. The Problem

In general, DDoS countermeasures are divided into detection and filtering, and detection is technically difficult. DDoS Mitigation System (DMS) can detect attack traffic based on the technology of their vendors, so service providers can increase DDoS countermeasure level by deploying the DMS in their network.

However, the number/capacity of DMS instances that can be deployed in a service providers network is limited due to equipment cost and dimensioning matters. Thus, DMS's utilization rate can reach its maximum capacity faster when the volume of DDoS attacks is enormous. When the rate reaches maximum capacity, the mitigation strategy needs to offload mitigation actions from the DMS to cost-effective forwarding nodes such as routers.

4. DDoS Mitigation Offload Use Case

This section describes offloading mitigation action from DMS whose utilization rate is high to cost-effective forwarding node using DOTS protocols. This section does not consider deployments where the network orchestrator and DMS are co-located.

Figures 1 and 2 show a component diagram and a sequence diagram of the use case, respectively.

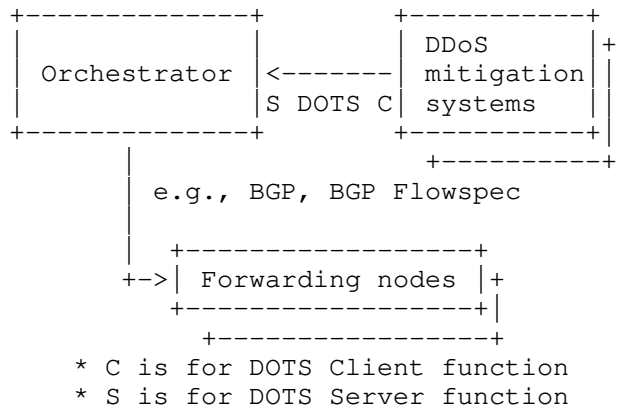

Figure 1: Component Diagram of DDoS Mitigation Offload Use Case

The component diagram shown in Figure 1 differs from that of DDoS Orchestration use case in [I-D.ietf-dots-use-cases] in some respects. First, the DMS embeds a DOTS client to send DOTS requests to the orchestrator. Second, the orchestrator sends a request to underlying forwarding nodes to filter the attack traffic.

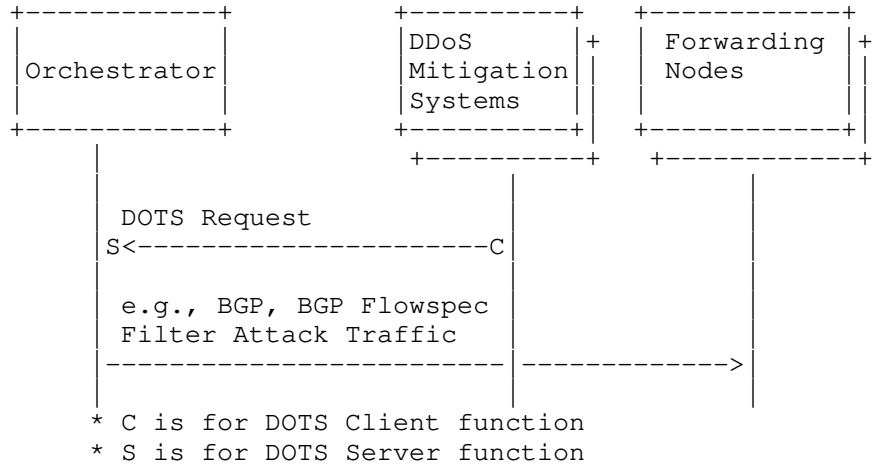

Figure 2: Sequence Diagram of DDoS Mitigation Offload Use Case

In this use case, it is assumed that volume based attack already hits a network and attack traffic is detected and blocked by a DMS in the network. When the volume-based attack becomes intense, DMS's utilization rate can reach a certain threshold (e.g., maximum capacity). Then, the DMS sends a DOTS request as offload request to the orchestrator with the actions to enforce on the traffic. After

that, the orchestrator requests the forwarding nodes to filter attack traffic by dissemination of flow specification rules protocols such as BGP Flowspec [RFC5575] on the basis of the blocked traffic information.

This use case is divided into two cases based on type of link between the DMS and the orchestrator: "out-of-band case" and "in-band case".

"Out-of-band case" is that the DMS sends a DOTS request to the orchestrator with blocked traffic information by the DMS via out-of-band link. The link is not congested when it is under volume attack-time, so the link can convey a lot of information.

On the other hand, "in-band case" is that the DMS sends a mitigation request to the orchestrator with blocked traffic information by the DMS via in-band channel. The link can be congested when it is under volume attack-time, so the link can convey limited information.

5. DOTS Deployment Considerations

This section describes deployment considerations: what type of DOTS protocol can be used and what type of information can be conveyed by DOTS protocol in this use case. Figure 3 shows overview of the DOTS signaling method and conveyed information for the out-of-band case and in-band case.

The volume of information should be considered carefully when DOTS protocol is used in in-band-case. What type of information can be conveyed by DMS relys on attack type detected by the DMS: reflection attack or non-reflection attack. When it is under non-reflection attack, src_ip and src_port information cannot be conveyed because attackers usually randomize the parameters so number of its become enormous. On the other hand, when it is under reflection attack, dst_port information cannot be conveyed because attackers usually randomize src_port so the number of dst_port of attack packets reached to victim become enormous. Furthermore, when it is under reflection attack, src_ip information cannot be conveyed when number of reflector is enormous.

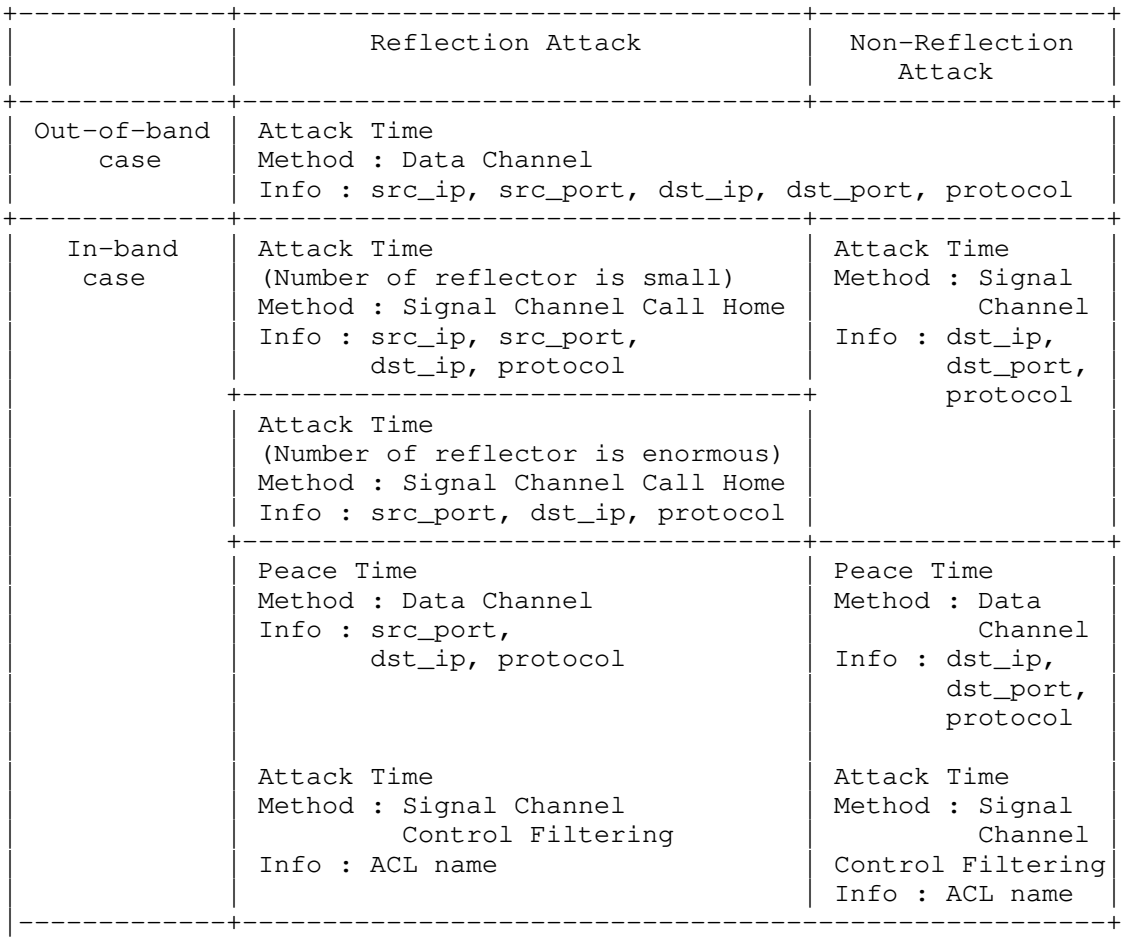

Figure 3: Signaling Method and Conveyed Information

About offloading DMS against reflection attack, the current signal channel [I-D.ietf-dots-signal-channel] is insufficient in terms of conveying src information. On the other hand, both call home expansion [I-D.ietf-dots-signal-call-home] and Filtering control expansion [I-D.ietf-dots-signal-filter-control] can convey src information.

Signal channel expansion of call home defines source-* clauses so it can convey src_ip information and src_port information in attack time. On the other hand, filtering control expansion can activate filtering rule configured in peacetime. Filtering rule for well-known port numbers abused for reflection attack can be configured to

DOTS server in peacetime. However, filtering rule for reflector's ip address in attack time can't be known in peace time. So filtering control expansion can convey src_port information but can't send src_ip information against reflection attack. About sending src information in the DMS offload use case, the capability of the call home extension encompasses the capabilities of the filtering control extension.

Hereafter, this document describes example of use DOTS protocol in each case.

5.1. DOTS Signaling via Out-of-band Link

In this case, the link is not congested when it is under volume attack-time, so DOTS data channel [I-D.ietf-dots-data-channel] is suitable because DOTS data channel has capability of conveying the drop-listed filtering rules including (src_ip, src_port, dst_ip, dst_port, protocol) information (and other actions such as 'rate-limit').

5.1.1. Example of using Data Channel

The procedure to use DOTS Data Channel in such case is as follows:

- The DMS generates a list of flow (src_ip, src_port, dst_ip, dst_port, protocol) information which the DMS is blocking/rate-limiting and wants to offload.
- The DMS creates data-channel ACL such as shown figure 4.
- The DMS sends the data-channel ACL to the orchestrator.

```
{
  "ietf-dots-data-channel:acls": {
    "acl": [
      {
        "name": "DMS_Offload_use_case_ACL",
        "type": "ipv4-acl-type",
        "activation-type": "immediate",
        "aces": {
          "ace": [
            {
              "name": "DMS_Offload_use_case_ACE_00",
              "matches": {
                "ipv4": {
                  "destination-ipv4-network": "192.0.2.2/32",
                  "source-ipv4-network": "203.0.113.2/32",
                  "protocol":17
```

```
                    },
                    "udp": {
                      "source-port": {
                        "operator": "eq",
                        "port": 53
                      }
                    }
                  },
                  "actions": {
                    "forwarding": "drop"
                  }
                },
                {
                  "name": "DMS_Offload_use_case_ACE_01",
                  "matches": {
                    "ipv4": {
                      "destination-ipv4-network": "192.0.2.2/32",
                      "source-ipv4-network": "203.0.113.3/32",
                      "protocol":17
                    },
                    "udp": {
                      "source-port": {
                        "operator": "eq",
                        "port": 53
                      }
                    }
                  },
                  "actions": {
                    "forwarding": "drop"
                  }
                }
              ]
            }
          }
        ]
      }
    }
```

Figure 4: JSON Example of ACL including (src_ip, src_port, dst_ip, dst_port, protocol) information conveyed by DOTS data channel

5.2. DOTS Signaling via In-band Link

In this case, the link can be congested when it is under volume attack-time, so DOTS data channel can't be used to convey the drop-listed filtering rules as blocked traffic information [Interop]. On the other hand, DOTS signal channel [I-D.ietf-dots-signal-channel], the source-* clauses defined in [I-D.ietf-dots-signal-call-home] and

flitering control [I-D.ietf-dots-signal-filter-control] can be used to communicate the policies to the orchestrator.

5.2.1. Example of using Signal Channel

DOTS signal channel has capability to send (dst_ip, dst_port, protocol) information. The procedure to use DOTS Signal Channel in this case is as follows:

- The DMS generates a list of (dst_ip, dst_port, protocol) information which the DMS is blocking/rate-limiting and wants to offload.
- The DMS creates mitigation request such as shown figure 5.
- The DMS sends the mitigation requests to the orchestrator.

```
{
  "ietf-dots-signal-channel:mitigation-scope": {
    "scope": [
      {
        "target-prefix": [
        "192.0.2.2/32"
        ],
        "target-port-range": [
          {
           "lower-port": 80
          },
          {
           "lower-port": 443
          }
        ],
        "target-protocol": [
          6
        ],
        "lifetime": 3600
      },
      {
        "target-prefix": [
        "192.0.2.2/32"
        ],
        "target-port-range": [
          {
           "lower-port": 53
          },
          {
           "lower-port": 123
          }
        ],
        "target-protocol": [
          17
        ],
        "lifetime": 3600
      }
    ]
  }
}
```


Figure 5: JSON Example of offload request including (dst_ip, dst_port, protocol) information conveyed by DOTS signal channel

5.2.2. Example of using Signal Channel Call Home

DOTS signal channel call home [I-D.ietf-dots-signal-call-home] has capability to send (dst_ip, dst_port, src_ip, src_port, protocol) information. The channel can convey src_ip information when number of reflector detected by DMS is small. The procedure to use DOTS call home in the situation is as follows:

- The DMS generates a list of (dst_ip, src_ip, src_port, protocol) information which the DMS is blocking/rate-limiting and wants to offload.
- The DMS creates mitigation request such as shown figure 6.
- The DMS sends the mitigation requests to the orchestrator.

```
{
  "ietf-dots-signal-channel:mitigation-scope": {
    "scope": [
      {
        "target-prefix": [
        "192.0.2.2/32"
        ],
        "target-protocol": [
          6
        ],
         "source-prefix": [
         "203.0.113.2/32"
         ],
         "source-port-range" : [
         {
          "lower-port": 53
         },
         {
          "lower-port": 123
         }
         ],
        "lifetime": 3600
      },
      {
        "target-prefix": [
        "192.0.2.2/32"
        ],
        "target-protocol": [
          6
        ],
         "source-prefix": [
         "203.0.113.3/32"
```

```
            ],
            "source-port-range" : [
            {
             "lower-port": 19
            },
            {
             "lower-port": 11211
            }
            ],
           "lifetime": 3600
        }
      ]
    }
  }
```

Figure 6: JSON Example of offload request including (dst_ip, src_ip, src_port, protocol) information conveyed by DOTS signal channel

On the other hand, signal channel call home cannot convey src_ip information when number of reflector detected by DMS is enormous. The procedure to use DOTS call home in the situation is as follows:

- The DMS generates a list of (dst_ip, src_port, protocol) information which the DMS is blocking/rate-limiting and wants to offload.

- The DMS creates mitigation request such as shown figure 7.

- The DMS sends the mitigation requests to the orchestrator.

```
{
  "ietf-dots-signal-channel:mitigation-scope": {
    "scope": [
      {
        "target-prefix": [
        "192.0.2.2/32"
        ],
        "target-protocol": [
          6
        ],
         "source-port-range" : [
         {
          "lower-port": 53
         },
         {
          "lower-port": 123
         },
         {
          "lower-port": 19
         },
         {
          "lower-port": 11211
         }
         ],
        "lifetime": 3600
      }
    ]
  }
}
```

Figure 7: JSON Example of offload request including (dst_ip, src_port, protocol) information conveyed by DOTS signal channel

5.2.3. Data Channel and Signal Channel Controlling Filtering

DOTS signal channel controlling filtering [I-D.ietf-dots-signal-filter-control] has capability to activate or deactivate ACL configured by Data Channel. Against reflection attack, DOTS client configures ACL including (dst_ip, src_port, protocol) information in peace time by Data Channel, and DOTS client activate the ACL in attack time by Signal Channel controlling filtering. Note that the src_port is well known port abused to carry out reclection attack by attacker. The procedure to use DOTS data channel and signal channel controlling filtering is as follows:

- In peace time, the DMS sends the ACL including (dst_ip, src_port, protocol) information such as figure 8.

o In attack time, the DMS generates a list of (dst_ip, src_port, protocol) which the DMS is blocking/rate-limiting and wants to offload. After that, the DMS sends the mitigation requests to activate corresponding ACL configured to the orchestrator such as figure 9.

```
{
  "ietf-dots-data-channel:acls": {
    "acl": [
      {
        "name": "DMS_Offload_use_case_ACL",
        "type": "ipv4-acl-type",
        "activation-type": "activate-when-mitigating",
        "aces": {
          "ace": [
            {
              "name": "DMS_Offload_use_case_ACL_DNS_amp",
              "matches": {
                "ipv4": {
                  "destination-ipv4-network": "192.0.2.2/32",
                  "protocol":17
                },
                "udp": {
                  "source-port": {
                    "operator": "eq",
                    "port": 53
                  }
                }
              },
              "actions": {
                "forwarding": "drop"
              }
            },
            {
              "name": "DMS_Offload_use_case_ACL_NTP_amp",
              "matches": {
                "ipv4": {
                  "destination-ipv4-network": "192.0.2.2/32",
                  "protocol":17
                },
                "udp": {
                  "source-port": {
                    "operator": "eq",
                    "port": 123
                  }
                }
              },
              "actions": {
```

```
                  "forwarding": "drop"
                }
              }
            ]
          }
        }
      ]
    }
  }
```

Figure 8: JSON Example of ACL including (dst_ip, src_port, protocol) information conveyed by DOTS data channel

```
{
  "ietf-dots-signal-channel:mitigation-scope": {
    "scope": [
      {
        "target-prefix": [
           "192.0.2.2/32"
         ],
         "target-protocol": [
           17
         ],
         "acl-list": [
           {
             "acl-name": "DMS_Offload_use_case_ACL_DNS_amp",
             "activation-type": "immediate"
           }
        "lifetime": 3600
      }
    ]
  }
}
```

Figure 9: JSON Example of including acl name conveyed by DOTS signal channel

Against non-reflection attack, DOTS client configures ACL including (dst_ip, dst_port, protocol) information in peace time by Data Channel, and DOTS client activate the acl in attack time by Signal Channel. Note that the dst_port is well known port abused to carry out non-reclection attack by attacker. The procedure to use DOTS data channel and signal channel controlling filtering is as follows:

- In peace time, the DMS sends the ACL including (dst_ip, dst_port, protocol) information such as figure 10.

o In attack time, the DMS generates a list of (dst_ip, dst_port, protocol) which the DMS is blocking/rate-limiting and wants to offload. After that, the DMS sends the mitigation requests to activate corresponding ACL configured to the orchestrator such as figure 11.

```
{
  "ietf-dots-data-channel:acls": {
    "acl": [
      {
        "name": "DMS_Offload_use_case_ACL",
        "type": "ipv4-acl-type",
        "activation-type": "activate-when-mitigating",
        "aces": {
          "ace": [
            {
              "name": "DMS_Offload_use_case_HTTP_GET_Flooding",
              "matches": {
                "ipv4": {
                  "destination-ipv4-network": "192.0.2.2/32",
                  "protocol":6
                },
                "tcp": {
                  "destination-port": {
                    "operator": "eq",
                    "port": 80
                  }
                }
              },
              "actions": {
                "forwarding": "drop"
              }
            },
            {
              "name": "DMS_Offload_use_case_SYN_Flooding_FTP",
              "matches": {
                "ipv4": {
                  "destination-ipv4-network": "192.0.2.2/32",
                  "protocol":6
                },
                "tcp": {
                  "destination-port": {
                    "operator": "eq",
                    "port": 20
                  }
                }
              },
              "actions": {
```

```
                  "forwarding": "drop"
                }
              }
            ]
          }
        }
      ]
    }
  }
```

Figure 10: JSON Example of ACL including (dst_ip, dst_port, protocol) information conveyed by DOTS data channel

```
{
  "ietf-dots-signal-channel:mitigation-scope": {
    "scope": [
      {
        "target-prefix": [
           "192.0.2.2/32"
         ],
         "target-protocol": [
           6
         ],
         "acl-list": [
           {
             "acl-name": "DMS_Offload_use_case_HTTP_GET_Flooding",
             "activation-type": "immediate"
           }
        "lifetime": 3600
      }
    ]
  }
}
```

Figure 11: JSON Example of including ACL name conveyed by DOTS signal channel

6. Security Considerations

Security considerations discussed in [I-D.ietf-dots-data-channel] and [I-D.ietf-dots-signal-channel] are to be taken into account.

7. IANA Considerations

This document does not require any action from IANA.

8. Acknowledgement

Thanks to Tirumaleswar Reddy, Shunsuke Homma for the comments.
Thanks to Koichi Sakurada for demonstrating proof of concepts of this .

9. References

9.1. Normative References

[I-D.ietf-dots-data-channel]
Boucadair, M. and R. K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", draft-ietf-dots-data-channel-29 (work in progress), May 2019.

[I-D.ietf-dots-requirements]
Mortensen, A., K, R., and R. Moskowitz, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-22 (work in progress), March 2019.

[I-D.ietf-dots-signal-call-home]
K, R., Boucadair, M., and J. Shallow, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home", draft-ietf-dots-signal-call-home-02 (work in progress), May 2019.

[I-D.ietf-dots-signal-channel]
K, R., 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-34 (work in progress), May 2019.

[I-D.ietf-dots-signal-filter-control]
Nishizuka, K., Boucadair, M., K, R., and T. Nagata, "Controlling Filtering Rules Using Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel", draft-ietf-dots-signal-filter-control-01 (work in progress), May 2019.

[I-D.ietf-dots-use-cases]
Dobbins, R., Migault, D., Fouant, S., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", draft-ietf-dots-use-cases-17 (work in progress), January 2019.

9.2. Informative References

[Interop] Nishizuka, K., Shallow, J., and L. Xia , "DOTS Interop test report, IETF 103 Hackathon", November 2018, <https://datatracker.ietf.org/meeting/103/materials/slides-103-dots-interop-report-from-ietf-103-hackathon-00>.

[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>.

Authors' Addresses

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

Email: yuuhei.hayashi@gmail.com

Kaname Nishizuka
NTT Communications
GranPark 16F 3-4-1 Shibaura, Minato-ku
Tokyo 108-8118
Japan

Email: kaname@nttv6.jp

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com