DOTS
Internet-Draft
Intended status: Experimental
Expires: April 18, 2019

Y. Hayashi
NTT
K. Nishizuka
NTT Communications
October 15, 2018

DDoS ~~mitigation~~ Mitigation ~~offload~~ Offload ~~usecase~~ Use Case and Companion ~~YANG module expansion in signal~~Signal ~~channel~~Channel YANG Module Extension

draft-h-dots-mitigation-offload-expansion-00

Abstract

This document describes a DDoS ~~Mitigation~~ mitigation offload use case and an ~~expansion~~ extension to ~~of the YANG module in~~ the DOTS signal channel YANG module for mitigating DDoS attack traffic correctly ~~with general routers or switches~~by forwarding nodes. The proposed use case and YANG module enhance DOTS capability to send attacker information and enable service providers to mitigate DDoS attack traffic by using general routers or switches in their intra-domain NW.

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 April 18, 2019.

Copyright Notice

Mis en forme : Surlignage

Commentaire [Med1]: What does that mean?

Commentaire [Med2]: What is an intra-domain network?

Do you mean: single administrative domain?

Commentaire [Med3]: I would delete this sentence.

Table of Contents

1. Introduction 2
2. Terminology 3
3. DDoS Mitigation Offload Usecase 3
4. Expansion of DOTS Signal Channel 6
4.1. Expansion of YANG Module of DOTS Signal Channel 6
4.2. Expansion of Mapping Parameters to CBOR 8
5. Security Considerations 8
6. IANA Considerations 8
7. Acknowledgement 8
8. References 8
8.1. Normative References 8
8.2. Informative References 9
Authors' Addresses 9

1. Introduction

~~Volume-~~Volume-based distributed denial-of-service (DDoS) attacks such as DNS amplification attacks are critical threats to be handled by ~~for internet~~ Internet service providers ~~because of their impact on network services~~. When such attacks occur, service providers have to mitigate them immediately to protect or recover their service(s). 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 ~~concerned~~ involved ~~with~~in DDoS attack detection and~~,~~ mitigation ~~and so on~~ collaborate.

On the other hand, the number of DDoS Mitigation Systems (DMS) that can be deployed in a service providers network is limited due to equipment cost. Thus, DMS's utilization rate can reach maximum capacity soon when the volume of DDoS attacks is enormous. When the rate reaches its maximum capacity, the network needs to offload mitigation action from the DMS to cost-effective network devices such as switches and routers.

DDoS Open Threat Signaling (DOTS) is a set of protocols ~~to standardize~~for real-time signaling, threat-handling requests, and data between the multi-vendor elements [I-D.ietf-~~dots-use-cases~~dots-signal-channel][I-D.ietf-dots-data-channel]. This document describes an automated DDoS Mitigation offload use case inherited from a DOTS usecase [I-D.ietf-dots-use-cases], which enables cost-effective DDoS Mitigation within ~~an~~ a single administrative domain~~intra-domain network~~. Furthermore, this document

Commentaire [Med4]: Please a reference to the section describing the use case you are referring to.

describes an ~~expansion~~ extension to ~~of~~ the signal channel YANG module ~~in the DOTS signal channel~~

[I-D.ietf-dots-signal-channel], which enables a service provider's network to mitigate attack traffic correctly in the use_case.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Commentaire [Med5]: Not used in the document

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

The terminology related to YANG data modules is defined in [RFC7950].

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~~n inacceptable level~~. How such threshold is set is deployment-specific.

DDoS attackers: Source ~~Devices~~ devices that ~~carry out~~originate DDoS attacks.

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

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

3. DDoS Mitigation Offload Use_~~case~~Case

The purpose of this use_case is to protect ~~intra-domain~~a network from volume-based DDoS attacks automatically, cost-effectively, and vendor-independently. The use_case is inherited from the DDoS Orchestration usecase in [I-D.ietf-dots-use-cases] and works on an intra-domain network.

Commentaire [Med6]: already mentioned above.

Figures 1 and ~~Figure~~ 2 show a component diagram and ~~C-plane~~a sequence diagram of the use_case, respectively.

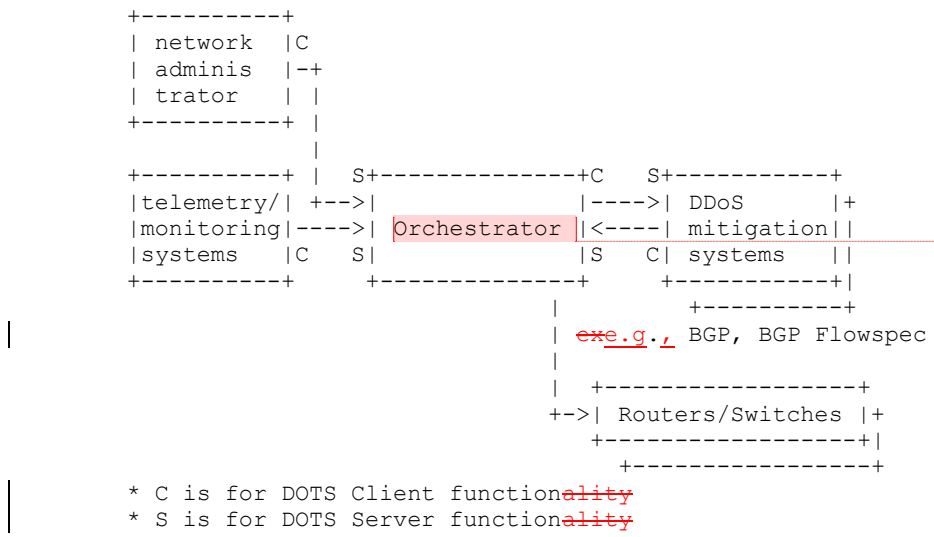
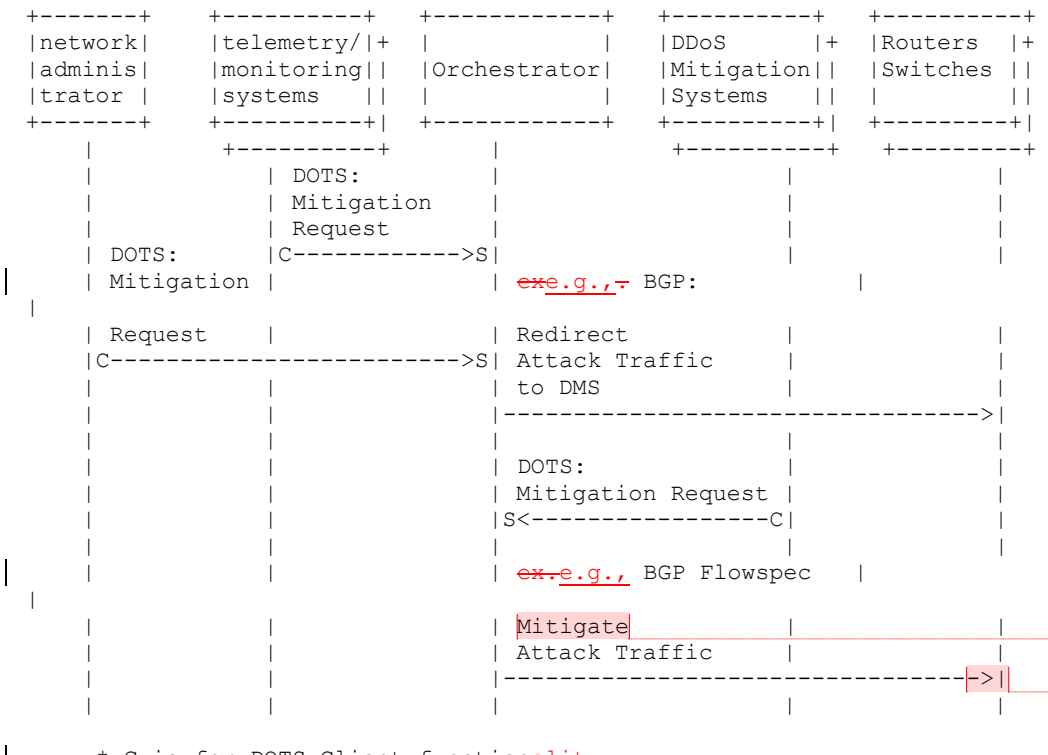


Figure 1: Component ~~diagram~~ Diagram of DDoS Mitigation ~~offload~~ Offload ~~usecase~~Use Case

~~This~~ 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 DDoS mitigation systems ~~have~~ embeds a DOTS client ~~function~~ to send mitigation requests to the orchestrator. Second, the orchestrator sends a request to ~~routers or switches~~underlying forwarding nodes to ~~block~~ filter attack traffic.

Commentaire [Med7]: Is there any specific configuration at the orchestration to allow for the top-talker clause to be supplied only by the DMS?



Commentaire [Med8]: Filter (block/rate-limit/…)?

Commentaire [Med9]: Add that only portion of the suspect traffic not matching the new filtering rule, is still redirected to a DMS.

Figure 2: ~~C-plane~~ Sequence D~~d~~iagram of DDoS Mitigation ~~offload~~ Offload ~~usecase~~Use Case

In this use case, when the telemetry/monitoring system detects a volume-based DDoS attack in the network, it sends a DOTS mitigation request to the orchestrator with target information such as 'target-prefix'. Then, the network administrator confirms the request and sends a DOTS mitigation request to the orchestrator with the target information.

After that, the orchestrator requests the ~~routers or switches~~forwarding nodes to redirect attack traffic to the DMS ~~by~~ using, for example, ~~a configuration protocol such as a routing protocol like~~ BGP [RFC4271] on the basis of the target information. Then, the DMS analyzes ~~attack~~ suspect traffic in detail and detects not only target but also attacker's information, such as top-talker, and mitigates the attack ~~traffic~~ on the basis of the detected information.

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 mitigation request to the orchestrator as an offload request with the detection information. After that, the orchestrator requests the ~~routers or switches~~forwarding nodes to ~~block~~ filter attack traffic to the DMS by dissemination of flow specification rules protocols such as BGP flowspec [RFC5575] on the basis of the detected information.

4. ~~Expansion~~ Extension to the~~of~~ DOTS Signal Channel

It is desirable that the ~~routers or switches~~forwarding nodes ~~mitigate~~ filter the attack traffic correctly after the DMS sends a DOTS ~~Mitigation~~ mitigation ~~Request~~ request as an offload request in the use case described in Section 3. For mitigating attack traffic correctly, this document proposes ~~expanding~~ extending DOTS signal channel [I-D.ietf-dots-signal-channel] so that it can send not only target information, but also representative attacker information such as top talker (sources). Note that it is difficult to send all attackers' information because there is an enormous number of attackers when a volume-based DDoS attack occurs and also because this list is dynamic.

This section describes ~~expansion~~ an extension ~~of~~ to the DOTS signal channel ~~the~~ YANG module ~~[RFC7950]~~ and required mapping parameters to CBOR [RFC7049] of the DOTS Signal Channel.

4.1. ~~Expansion of~~Updates to the ~~YANG Module of~~ DOTS Signal Channel YANG Module

Figure 3 shows an ~~expanded~~ extended YANG ~~Module of the~~ DOTS Signal Channel module.

~~Note that the "augment" statement allows a module to insert additional nodes into existing data models.~~ The module defines a new grouping "attacker" and adds the grouping to an existing Signal Channel module by using an "augment" statement.

xxx

```
{
module ietf-dots-signal-channel-mitigation-offload~~-expansion~~ {
     yang-version 1.1;

     namespace "urn:ietf:params:xml:ns:yang:
                ietf-dots-signal-channel:mitigation-offload~~-expansion~~";

     import ietf-dots-signal-channel {
       prefix signal;
     }
```

Commentaire [Med10]: Please validate the module using pyang.

Commentaire [Med11]: need to add

« <CODE BEGINS> file ietf-xx-xxx@2018-10-15.yang » line

```
import ietf-inet-types {
  prefix inet;
}

organization
  "IETF DDoS Open Threat Signaling (DOTS) Working Group";
```

```
     contact
       "WG Web:   <https://datatracker.ietf.org/wg/dots/>
        WG List:  <mailto:dots@ietf.org>
        Editor:  Yuhei Hayashi
                 <mailto:hayashi.yuhei@lab.ntt.co.jp>
     description
       "This module contains the YANG definition for expanding signaling
        messages exchanged between a DOTS client and a DOTS server.

        Copyright (c) 2018 IETF Trust and the persons identified as
        authors of the code.  All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject
        to the license terms contained in, the Simplified BSD License
        set forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
        (http://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC XXXX; see
        the RFC itself for full legal notices.";

     revision 2018-07-30 {
       description
         "Initial revision.";
       reference
         "RFC XXXX: ietf-dots-signal-channel";
     }

    /*
     * Groupings
     */
     grouping attacker {
       description
         "Specifies the attackers of the mitigation request.";
       leaf-list attacker-top-talker-prefix {
         type inet:ip-prefix;
         description
           "IPv4/IPv6 prefix identifying the a top-talker in attackers.";
       }
     }

    /*
     * Main Container for DOTS Signal Channel Expansion
     */
     augment "/signal:dots-signal/signal:scope/"{
       uses attacker;
     }
```

Commentaire [Med12]: update the date (same as the one used in the file name)

Commentaire [Med13]: the reference should point to `draft-h-dots-mitigation-offload-expansion`

Commentaire [Med14]: I would define offload as a feature.

Commentaire [Med15]: Add if-feature offload and a description clauses.

```
}
}
<CODE ENDS>
```

Figure 3: ~~Expansion~~ Extension ~~of~~ of YANG Module of DOTS Signal Channel

4.2. ~~Expansion~~ Update to ~~o~~f Mapping Parameters to CBOR

Figure 4 shows ~~expansion~~ an update to ~~of~~ Mapping Parameters to CBOR ~~[RFC7049]~~ related to Figure 3.

Parameter Name	YANG Type	CBOR Key	CBOR Major Type & Information	JSON Type
...	...	...	...	...
attacker-top-talker -prefix	leaf-list inet: ip-prefix	XX	4 array 3 text string	Array String

Figure 4: Expansion of Mapping Parameters to CBOR

5. Security Considerations

TBD

6. IANA Considerations

TBD

7. Acknowledgement

TBD

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

Mis en forme : Anglais (États Unis)

Commentaire [Med16]: should be listed in the IANA section

Commentaire [Med17]: to be completed with the yang required actions

[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>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[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-25 (work in progress), September 2018.

Commentaire [Med18]: Those are not normative. Should be moved to 8.2.

Commentaire [Med19]: Idem as above ?

Commentaire [Med20]: should be listed as a normative reference

8.2. Informative References

[I-D.ietf-dots-requirements] Mortensen, A., Moskowitz, R., and R. K, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-15 (work in progress), August 2018.

~~[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-25 (work in progress), September 2018.~~

[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-16 (work in progress), July 2018.

Authors' Addresses

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

Email: hayashi.yuhei@lab.ntt.co.jp, yuuhei.hayashi@gmail.com

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

Email: kaname@nttv6.jp