DOTS
Internet-Draft
Intended status: Informational
Expires: April 21, 2016

K. Nishizuka
NTT Communications

October 19, 2015

Inter-Domain DOTS Use Cases
draft-nishizuka-dots-inter-domain-usecases-00

Abstract

This document describes inter-domain use cases of the DDoS Open Threat Signaling(DOTS).

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 http://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 22, 2016.

Table of Contents

1. Introduction

Maximum size of DDoS attack is increasing. According to a report from Cloudflare[Cloudflare], in 2013, over 300 Gbps DDoS attack against Spamhaus was observed which exploited DNS reflection mechanism to create massive attack with intention to overwhelm the capacity of the targeted system.

If this trend continued, the volume of DDoS attack will exceed preparable anti-DDoS capability by one organization mostly in the aspect of cost. Moreover, possibility of DDoS attack is unpredictable, so it is not realistic that every organization prepare sufficient anti-DDoS system.

This problem could be solved by sharing anti-DDoS system over multi-organizations. We can share the burden of protection against DDoS attack by inter-domain cooperation. To accomplish this, we need a framework which use common interface to call for protection.

To describe the mechanism of such a framework, we classified inter-domain use cases into three models.

1. Multi-home Model (one supplicant and multi mitigators)

2. Cloud Model (multi supplicants and one mitigator)

3. Delegation Model (both sides of supplicant and mitigator)

By blocking DDoS attack with inter-domain cooperation, average usage of DDoS mitigation equipment will increase. This will leverage total capacity of anti-DDoS system in all over the internet. With this mechanism, we can manage DDoS attacks which exceed the capacity of its own platform.

At the same time, it might be needed to convey information of amount of processed threat traffic which would be used to charge other organization each other. However this kind of information is out of scope of DOTS.

2. Terminology

supplicant: call for an anti-DDoS action to a mitigator. It could be a service under attack itself. Also, it could be a monitoring system which inspect the traffic towards the service by netflow/sflow or DPI, from which it can detect DDoS attack in the traffic. The minimum requirement to supplicant is that it must know which IP address is under attack and convey it to a mitigator by DOTS protocol.

mitigator: protect a service from DDoS attack. It can use blackholing, ACLs, flowspec, rate-limit, dedicated DDoS mitigation devices and other methods depending on its capabilities. It must be preprovisioned to determine a DDoS protection entity. It starts DDoS protection based on information provided by a supplicant. The minimum information is IP address of the service which it must protect from the DDoS attack. Other information like source IP address, port, type of DDoS, etc. provided by the supplicant are optional. The optional information may be used, but it might be overridden by the mitigator according to the on-going attack.

Other terminology and acronyms are inherited from [I-D.draft-mglt-dots-use-cases]

3. DDoS Protection Scenario

DDoS protection can be divided into two stages.

o Provisioning stage

Before getting attacked by malicious traffic, a supplicant needs capacity building with a mitigator in advance. In this provisioning stage, following information should be provided to the mitigator side to prepare for DDoS attack:

1. Protection capability

2. Restriction on the range of IP addresses and ports

3. Return path information of the mitigated traffic

4. Authorization information to restrict the supplicant

These informations can be conveyed off the wire, thus this is out of scope of DOTS. However, provisioning stage is very important to protect the service, therefore we describes how DDoS protection works comprehensively.

o Signaling stage

After getting attacked, we need to signal SOS information immediately if the service has not implemented any other anti-DDoS system except preprovisioned DDoS mitigation. In this signaling stage, the supplicant signals targeted IP address to the mitigator with authorization information. The mitigator decides to protect the system based on the preprovisioned information. This signaling should have characteristics as follows:

1. Common transport and schema

2. Secure signaling

Even in the signaling stage, preprovisioned information can be changed according to the DDoS attack vector. However, provisioning and signaling must be separated to keep DOTS requirements simple.

3.1. Provisioning Stage

In this section, we describe how preprovisioned information is used to protect a service. In the provisioning stage, before getting attacked, the operator of the service register following informations to a mitigator to protect the service correctly and effectively.

3.1.1. Protection Capability

Protection capability is consist of three informations: protection method, protection threshold and traffic capacity.

o protection method

Available protection methods of mitigator may be selectable, which include blackholing, ACLs, flowspec, dedicated DDoS appliances, etc. These methods have their own max capacity. Therefore, protection threshold should be determined in advance according to the traffic capacity of the method.

In the case of blackholing, it stops the traffic destined to the service totally. In a way, the "denial" of service is successful except in the case of selective blackhole. However, the capacity of the blackholing is rather higher than other methods because it just divert traffic to null0 interface of routers.

On the other hand, in the case of DDoS mitigation appliances, only the malicious traffic will be discarded on the box and the scrubbed normal traffic will be returned to the original service thus service continuity will be kept, though there is possibility of false positives and false negatives. However, the total volume of processable traffic is limited to the capacity of the hardware. To reduce the possibility of the mis-classification, which type of DDoS attack will be processed and which countermeasures will be applied to should be determined in the provisioning stage.

o protection threshold

Protection threshold defines when the appropriate method should be invoked to start protection. Typical threshold is traffic volume(bps/pps) of the attack. Depending on the type of the service, the appropriate threshold differs. If the threshold is not appropriate, possibility of false positives and false negatives increases. For example, if the service is widely used content server, low threshold of SYN attack protection(rate-limit) could cause failure of normal transaction.

o traffic capacity

Traffic capacity is protectable total volume[bps/pps] of DDoS traffic which include both malicious traffic and normal traffic. This capacity should be negotiated carefully because it could affect the service directly. From the point of view of the mitigator, maximum duration and number of protection could be limited to protect the DDoS mitigation system from exclusive occupancy.

If the protection capability of one mitigator is insufficient to a service, DOTS can provide capacity leverage to both the service and the mitigator.

3.1.2. Restriction on the Range of IP Addresses and Ports

In the provisioning stage, the service should register the range of IP addresses which they need to protect to the mitigator. Without this restriction, they can use anti-DDoS system to protect any other organization. Especially, in case of blackholing, they can abuse the system by blocking all of the traffic to the other organization.

In addition, they can register range of source IP address/port and destination IP address/port as a whitelist. If they know some range of 5 tuples which never include DDoS traffic, they can exclude it from the target of anti-DDoS protection, which reduce the possibility of false positive.

3.1.3. Return Path Information of the Mitigated Traffic

In many cases, DDoS mitigator controls traffic to divert DDoS attack traffic to its own domain to deal with it. It classifies the traffic into malicious traffic and normal traffic. Normal traffic should be returned to the original server, however simply returning traffic to the internet can cause routing loop because the returning traffic could re-enter the diversion path again. To avoid this routing loop, the returning path should be provisioned in advance. If there is no dedicated line between the mitigator and the service, tunnel technology such as GRE[RFC2784] can be used. In that case, tunnel information should be preprovisioned. In general, next-hop and prefix information should be provided to the mitigator to determine the returning path of the mitigated traffic.

3.1.4. Authorization Information to Restrict the Supplicant

After the provisioning, the mitigator should limit the usage of the provisioned DDoS protection entity to the legitimate supplicant. Only authorized supplicant can trigger the anti-DDoS action. If the supplicant was not restricted, a spoofed signal could abuse the mitigator. Also, the system should be protected from replay attack.

3.2. Signaling Stage

After the provisioning stage, the authorization information of the DDoS protection entity will be supplied to a supplicant. Then, the supplicant can call for help to the DDoS mitigator by signaling mandatory information.

3.2.1. Signaling Information

The mandatory information which should be included in the signaling is as follows:

- IP address of defence target
- Instruction (Start/Stop)
- Authorization information

Suppose a supplicant, which is the service itself or monitoring system, can know that the service is under a severe DDoS attack. After the detecting the DDoS attack, the supplicant records attacked IP address(es). Adding the authorization information provided in advance, it signals protection-start-instruction packet to the mitigator including IP address of defence target.

The mitigator which recieved the signal reacts to start mitigation. First, it checks the authorization information to decide the signaling is legitimate or not. If failed, it never react. If succeeded, it checks IP address with according DDoS protection entity. Second, If the IP address was included in the range which was declaired in advance, it starts mitigation. The protection method will be selected appropoately according to the provisioned protection capability. Finally, it classifies malicious traffic and normal traffic, then return the normal traffic to the service in specified returning path.

The supplicant can stop the mitigation by sending protection-stop-instruction packet. However, in some case, it is difficult to know whether the DDoS attack has ended or not from the monitoring point of the supplicant.

The following informations are useful for mitigators in many cases but they are optional.

- Attack ID
- (Average/Maximum/Currrent)Traffic volume[bps/pps]
- Severity
- Type of attack
- Protection method
- Src IP/Port

- Dst Port

- Attack start time

We describe the reason why these informations are not mandatory.

- Attack ID

Attack ID could be assigned by a supplicant. By recieving the attack ID, a mitigator can tell the attack vector is the same or not from the observation of the supplicant. However, regardless of the provided attack ID, the behavior of DDoS protection will not change. Therefore this is optional information.

- (Average/Maximum/Currrent)Traffic volume[bps/pps]

Traffic volume information can be used to determine protection method. However, in the case of massive DDoS attack, the circuit connected to the internet from the service could be saturated by the traffic, so there is no way to know how much traffic is incoming on the saturated link. Thus, traffic volume information provided by the supplicant is unreliable. That is why this is optional information.

- Severity

Severity information can be used to determine protection method. However, in many cases, DDoS attack vectors change time to time, so there is no constant index of severity. Moreover, the monitoring system on the service side can look through the important attack vector which is very severe to the service, so the severity must be overwritten by the mitigator if it can inspect the traffic more deeply. Therefore this is optional information.

- Type of attack

Similar to severity information, type of attack declared by the monitoring system on the service side is unreliable. Decision of the type of attack must be overwritten by the mitigator if it can inspect the traffic more deeply. Therefore this is optional information.

- Protection method

The supplicant can convey preferable protection method information, which could be used to change the behavior of the mitigator. However, depending on the usage situation, the mitigator could override the protection method. Therefore this is optional information.

- Src IP/Port

In some cases, source IP/Port of the DDoS attack are spoofed. They widely vary and continue changing. Thus, the mitigator can not depend on the Src IP/Port information from the supplicant. Therefore this is optional information.

- Dst Port

Destination port of the DDoS attack can be changed by the attacker if they observed the attack on the port is not effective. Similar to Src IP/Port information, this is optional information.

- Attack start time

Attack start time information can indicate the severity of the attack. The mitigator can find the attack effectively by that inforamtion if it has a constant monitoring system. However, this is optional information.

3.2.2. Common Transport and Schema

To convey the information listed in the previous section, DOTS WG will define a common transport and schema. These are under discussion on Mailing List based on the draft [I-D.draft-reddy-dots-transport]. Defining these common transport and schema is out of scope of this draft. We note that, with a common transport and schema, we can share the burden of protection against DDoS attack in inter-domain model, which is described in Section.4.

3.2.3. Secure Signaling

Secure signaling is fundamental requirement to the DOTS signaling protocol. Only the legitimate supplicants can use the mitigator. Restriction can be accomplished by existing authentication and authorization methodologies. Signaling must be encrypted to avoid man-in-the-middle attack. To deal with the unreliable transport on the link under attack, signaling should have idempotency. Also authorization information must be securely exchanged in the provisioning stage. Though these characteristics are important, defining the signaling method is out of scope of this draft.

3.3. After DDoS Protection

After the DDoS protection was kicked by signaling, some information derived from the mitigator is useful to the operators of the service.

- Status of ongoing protection

Status of the protection(The attack is ongoing or not) will be used to determine that the system is already safe without the protection. The mitigator should have interface from which the supplicant or the operator of the service can get the status of the protection.

o Attack information

The operator of the service will eager to know what kind of attack was pointed to the service. Then, they can study how to try to find the best plan to cope with the situation.

o Number of the dropped packets

Number of the dropped packets can be used to create the billing data. Some DDoS mitigator may have data quantity charging system to account the supplicant based on the usage of their resources.

How to convey these information is indispensable issue of inter-domain DDoS protection. However, we note that these are out of scope of DOTS.

4. Inter-Domain Dots Use Cases

We classified inter-domain use cases into three models. In these models, the signaling packets traverse over multi domains. They utilize the common interface to the DDoS protection entities which are located in the multiple domains. We assume that the provisioning stage has finished in all mitigators, so by sending signaling packets, the mitigators start the according protections and return scrubbed traffic to the service in specified return path.

4.1. Usecase 1: Multi-home Model

In the multi-home model, there are one supplicant and multi mitigators. The supplicant can use both mitigators.

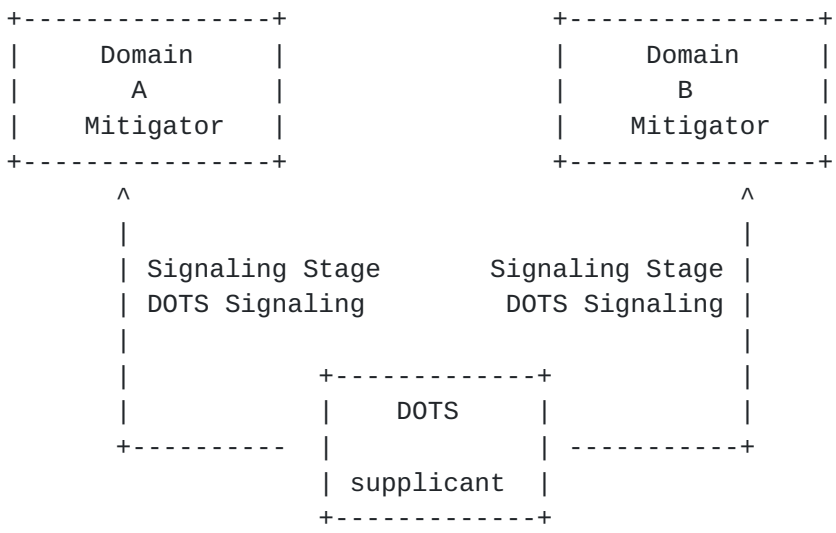

Figure 1: Usecase 1: Multi-home Model

An example of this situation is that a content provider is connected to two transit providers. When the content provider get attacked, the DDoS traffic will come from transit A and B. Signaling to the mitigator in transit A can stop only the DDoS traffic from transit A, and vice verse. Though the provision method will be different, the signaling interfaces are common if the both mitigators are using dots framework. After detecting the DDoS attack, the supplicant will send the signaling packet to the both mitigators at the same time. Common interface of DOTS signaling will shorten the lead time of the DDoS protection on both transits.

4.2. Usecase 2: Cloud Model

In the cloud model, there are multi supplicants and one mitigator. The mitigator accepts signals from multi supplicants in multiple domains.

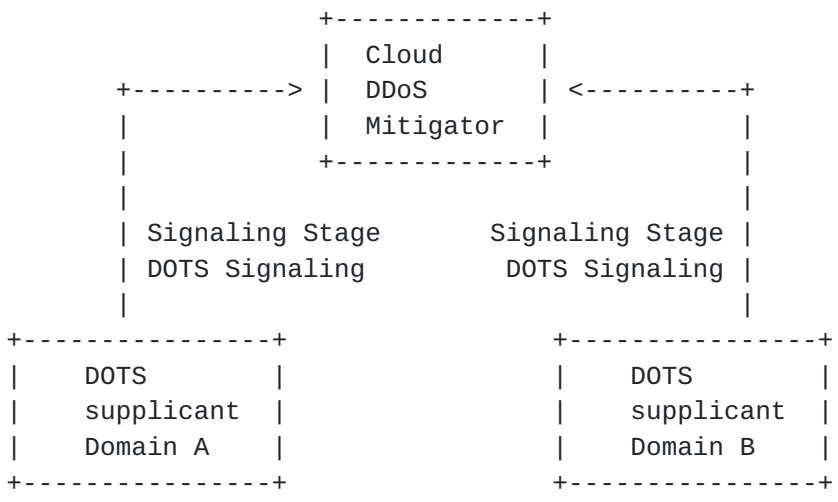

Figure 2:Usecase 2: Cloud Model"

An example of this situation is cloud type of DDoS mitigation service provider. Cloud type of DDoS mitigation service providers divert traffic to its own domain using routing protocols, that is BGP route injection. Though they need to provision the returning path mostly on the tunnel interface because they are not directly connected to the domains of the supplicants, they can accomodate multiple domains remotely.

4.3. Usecase 3: Delegation Model

In the delegation model, a mitigator has both sides of supplicant and mitigator.

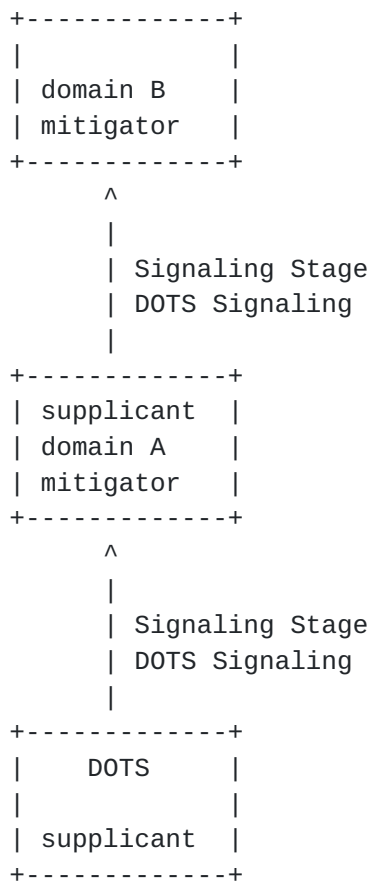

Figure 3: Usecase 3: Delegation Model

If the capacity of the mitigator is insufficient in comparison with ongoing DDoS attack, the mitigator can be a supplicant which call for protection in other domain. The provisioning of the mitigator in domain B can be done by the mitigator in domain A as a supplicant in advance. By just relaying the DOTS signaling information to the mitigator in domain B, the mitigator in domain A can utilize DDoS protection of doamin B. The original supplicant might not notice that the mitigation was delegated to other domain. Even if the capacity is sufficient, in some cases, it is effective to delegate the protection to upstream domain. Stopping DDoS traffic at an ingress border will reduce unnecessary forwarding. The mitigator can delegate the burden of the mitigation, therefore they can accomodate more services which exceed the capacity of its own platform.

A mitigator can be a broker which select appropriate DDoS mitigators according to the capacities and the field of expertise of the mitigators. In this case, billing data could be more important to adjust the cost distribution fairly.

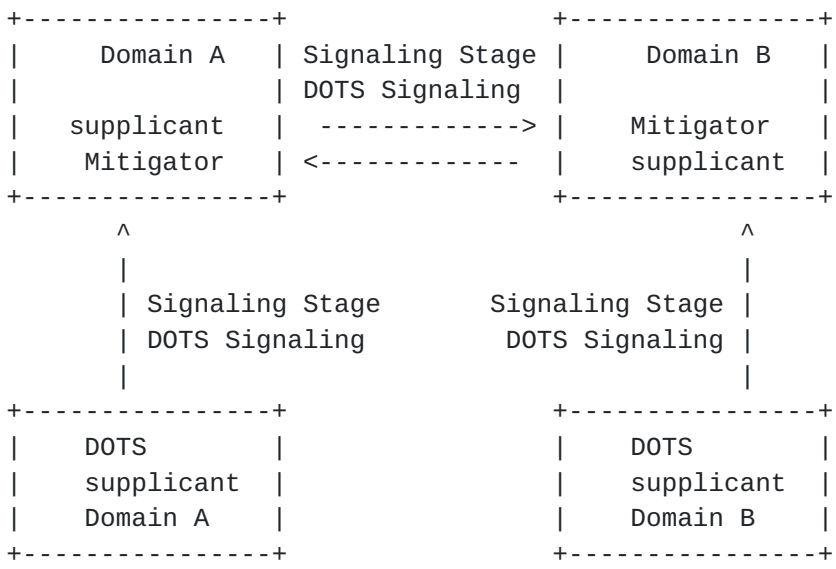

Figure 4: Cooperative DDoS Mitigation with DOTS Signaling

The figure.4 describes a minor changed version of the delegation model. The supplicants and mitigators can signal each other with DOTS signaling. They can ask for help each other. In this model, we can leverage total capacity of anti-DDoS system in all over the internet.

5. Security Considerations

As described in Section.3.2.3, secure signaling is fundamental requirement to the DOTS signaling protocol. Only the legitimate supplicants can use the mitigator. Authorization information must be securely exchanged in the provisioning stage.

6. IANA Considerations

No need to describe any request regarding number assignment.

7. References

7.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2784] D. Farinacci., T. Li., S. Hanks., D. Meyer., and P. Traina., "Generic Routing Encapsulation (GRE), March 2000".

[I-D.draft-mglt-dots-use-cases] D. Migault, Ed., "DDoS Open Threat Signaling use cases, draft-mglt-dots-use-cases-00 (work in progress), April 2015".

[I-D.draft-reddy-dots-transport] T. Reddy., D. Wing., P. Patil., M. Geller., M. Boucadair., and R. Moskowitz., "Co-operative DDoS Mitigation, October 2015".

7.2. URL References

[Cloudflare] Cloudflare, "https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/".

Author's Address

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

EMail: kaname@nttv6.jp