SE Dots: A Sensitive and Extensible Framework for Cross-Region DDoS Processing

Li Su(✉), Meiling Chen, Jin Peng, and Peng Ran

China Mobile Research Institute, Beijing 100053, China
{suli, chenmeiling, pengjin, ranpeng}@chinamobile.com

Abstract. This paper proposed a SE Dots architecture and system with type awareness and high scalability to improve the ability to handle DDoS attacks across networks. Firstly, we designed a Dots protocol that includes attack type extensions, which enables accurate sensing of attack types. Then, the shunt capability module and adaptive matching module are extended in Dots framework to realize the adaptive selection of various disposal mechanisms, thus effectively extend the docking of different types of Mitigator to achieve a finer-grained cleaning effect. Technical verification shows that, under the same DDoS attack, the use of SE Dots scheme and architecture can improve the disposal efficiency by 17% and increase the user access success rate by 31.5% without increasing the cost of equipment. and it has strong advancement and practicability.

Keywords: Dots · DDoS attack · Attack linkage disposal · Flow cleaning

1 Background

Distributed Denial of Service (DDoS) is a type of resource-consuming attack, which exploits a large number of attack resources and uses standard protocols for attacking. DDoS attacks consume a large amount of target object network resources or server resources, so that the target object cannot provide network services normally. At present, DDoS attack is one of the most powerful and indefensible attacks on the Internet, and due to the extensive use of mobile devices and IoT devices in recent years, it is easier for DDoS attackers to attack with real attack sources (broilers). In 2018, the threat of DDoS attacks is still increasing. the traffic of DDoS reflection attack using memcached server vulnerabilities reached a peak of 1.7 Tbps. The opening ceremony of pyeongchang winter Olympics was subjected to DDoS attacks for up to 12 h. The industries affected by DDoS attack include banks, governments and games.

The current anti-DDoS modes mainly include three modes: one is single-point operation, such as self-built anti-DDoS equipment in the machine room [1]; the Second is cloud protection which achieve unified protection through flow lead; The third is joint prevention within an organization (called a domain) [2], such as anti-DDoS linkage processing and cloud cleaning centers. However, the current attack presents a distributed and large traffic trend, and the attack sources are spread all over the world. As far as the current situation is concerned, a certain range of defenses can no longer meet the anti-DDoS attack requirements, and comprehensive cross-network collaboration is required [3]. In order to shield operator differences from defending DDoS

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 509–517, 2019.
https://doi.org/10.1007/978-3-030-21373-2_41

attacks across the entire network (global), the IETF working group proposed the DOTS framework [4], which is used to automate and standardize DDoS countermeasures and to shield differences in various anti-ddos solutions.

The existing DOTS implementation mechanisms have two problems: the first is that the mitigation request only defines the IP address, port range, protocol type, FQDN (fully qualified domain name), URI of the attacked target, but does not contain the attack type or bandwidth. As a result, the amount of information that is being attacked by the attacking target is insufficient. The second problem is that DOTS framework only uses BGP to process attack traffic. The near-source black hole operation will discard all traffic, which directly leads to the normal traffic loss of the attacked object. On the basis of DOTS, this paper proposes a flexible extended DOTS architecture that can perceive the attack types. Firstly, by extending the mitigation request method of signal channel and clarifying the attack type, the Mitigator can specifically handle the attack in the mitigation request; The second is to add request methods of the DDoS http mitigation and shunt policy module, which can adaptively select attack defense method according to the attack site, and improve the DDoS defense under the DOTS framework.

2 Existing Technologies and Shortcomings

At present, the main technologies of DDOS attack protection include: single point device protection, reverse proxy (cloud protection) and linkage defense.

Single point protection relies on the independent deployment of DDOS devices for protection. This method is simple to deploy, but due to the limited processing ability of a single device for attacks, it has insufficient capacity to deal with large traffic attacks that cause network congestion. Moreover, it is difficult to conduct uniform detection and disposal when different devices are deployed upstream and downstream in one network [5].

Reverse proxy, also known as cloud protection, is a dedicated cloud platform that implements DDOS attack detection and filtering. When the system detects abnormal traffic, it actively redirects traffic to the cloud acceleration server, and the cloud protection equipment will perform cleaning operation and then re-injected to the router of the business system [6]. The cloud protection method adopts centralized deployment, which is suitable for the cleaning needs of small and medium-sized enterprises or services; However, in the case of large-scale traffic attack, the cost of flow lead is huge and may cause new network congestion. Therefore, the cloud cleaning method is not suitable for large-scale traffic cleaning.

The linkage disposal technology is to construct a linkage system separately, analyze the data such as attack alarms issued by different anti-DDOS devices, coordinate and dispose of them. The advantage of adopting this mode is that it can deal with attacks in complex networks, especially in the case of attacks against large traffic, which can mobilize the processing capabilities of existing networks to achieve near-source distributed cleaning Under the premise of not adding new equipment, more effective cleaning of larger attack traffic can be realized, especially suitable for scenarios such as Metropolitan area network, IDC, customer business collaborative protection and so on [7].

DOTS is a cross-domain (cross-organization) processing framework for DDoS attacks defined by the IETF, and also is an implementation method of linkage processing technology. The DOTS establishes a general architecture, method and processing mechanism without considering specific attack disposal devices and means [8], which is very suitable for use in the scenarios of network operation and business operation separation. DOTS framework includes the following four parts: Attack Target, DOTS Client, DOTS Server and Mitigator.

The attack mitigation process of the DOTS framework is shown in Fig. 1.

The process is as follows:

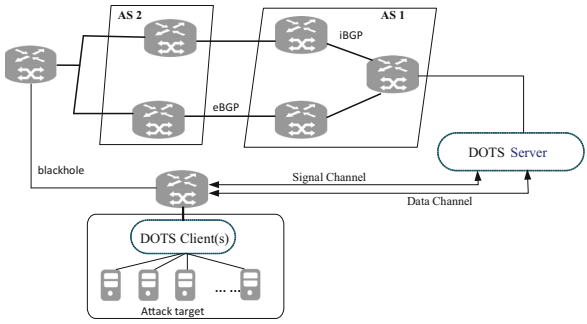

Fig. 1. DOTS framework diagram based on BGP mitigation mode

(1) Attack target is attacked by DDoS, then DOTS Client sent mitigation request to DOTS Server;
(2) Receiving requests, DOTS Server parses request packets to obtain attack details, such as IP address information, etc.;
(3) Using BGP to generate an optimal path through BGP neighbor relationships;
(4) Mitigator chooses one or more of the nearest routers for black holes based on BGP results.

There are two interfaces between DOTS client and DOTS server: Signal Channel [9] and Data Channel. Signal Channel [10] is used for client to seek attack mitigation from server and server to inform client of the state of the mitigation process. The Data Channel is used for related configuration and policy information exchange (between client and server).

There are two implementation shortcomings in the existing DOTS framework: first, only the message communication mechanism is defined, and the attack type transmitted is not defined, which will reduce the Mitigator's processing capability and efficiency. Second, the existing mechanism only supports mitigation notification through BGP, and the mitigation notification based on BGP can only reach the routing device for traffic lead, but cannot convey the attack type and mitigation mechanism, which is not conducive to timely attack disposal, making it difficult to meet the demand by using BGP traffic lead and disposal.

3 SE DOTS Technical Principle

SE DOTS is to add the definition of attack type in the existing DOTS framework, which can effectively improve the processing efficiency and accuracy of DOTS linkage. At the same time, extend the message communication mechanism based on HTTP to form the processing capability of classification and extension.

3.1 Attack Type Awareness

In the current mechanism, when the DOTS client detects a DDoS attack, it sends a mitigation request through the signal channel, which contains the following fields: target-prefix: address prefix of the target being attacked; target-port-range: the port range of the target address under attack; Target-protocol: the protocol involved in this attack; Target-fqdn: full address of the target under attack; Target-uri: URL of the attacked address; Alias-name: alias-name of the target; lifetime: lifetime of mitigation requests. Although the Mitigation request contains target-protocol, which refers to the protocol involved in the attack, the same protocol contains a variety of DDoS attack types. For example, DNS Reply Flood and DNS Query Flood are distinguished below the DNS protocol, and there are differences in the disposal means of different attack types. Adding an "Attack method" field in Dots mitigation request solves the problem that it is difficult to carry out fine protection against the attacked features of the attack target. The specific implementation process includes:

(1) When Attack Target creates an identifier, add the "Target-attack-Type" field;
(2) DOTS Client responds to requests and sends messages to DOTS Server according to existing processes;
(3) DOTS Server parses the request and generates mitigation request messages according to the type requirements of Mitigator;

SE DOTS adds "target-attack-type" and "target-bandwidth" fields to the mitigation request, which belongs to the Signal message generated by the attack target and sent to DOTS Client.

For the target-DDoS-type field, we define it as a string Type, and define the two fields according to the attack method and extension name. Similar to other existing linkage disposal technologies, there may be problems in the actual network environment, that attack target and mitigator (such as cleaning equipment) belong to different models of different vendors, because different vendors have different definitions of Attack in understanding and implementation. When an attack occurs, some devices may not be considered as an attack, and the effect of linkage cleaning may not be achieved. It is also possible that the detection device considere it as A type attack, while the cleaning device consider it as B type attack. When performing the cleaning schedule, it will cause the problem of incorrect cleaning or over-cleaning. Both of these errors will cause the normal business to fail to link. Therefore, it is necessary to unify the attack definition, form a standard attack definition, and solve the problem of

cleaning errors from the source. we give out a complete format for DDoS attacks as [protocol level] [protocol name] [message name/operation name/port] [attack methods feature description field 1] [attack methods feature description field 2] [attack methods describe the standard field], interval between each field operators use “,” symbol or any other symbol agreed.

For example: HTTP Get Flood(CC) definition,we defined the target-Attack-Type field as:

```
{
"Attack-Name":" Application _Layer, HTTP, Get,,, Flood"
"Attack-Alias":"HTTP CC Flood"
}
```

Based on the perceptual extension, the DOTS Server can accurately inform Mitigator of the objects and attack types that need to be disposed when the mitigation instructions are delivered to the Mitigation, so that the Mitigator can be accurately disposed.

3.2 Disposal Capacity Expansion (Extensible)

DOTS framework currently implements DDoS attack mitigation notification using BGP. Under the existing mechanism, BGP mode mitigation includes two types of measures: First, the traffic is drained through the BGP mechanism, and the dedicated cleaning equipment/cleaning center handle the traffic. Second, black hole routing (discarding) is performed on the traffic through the BGP mechanism. However, there are some deficiencies in how to choose these two kinds of measures [11]: in the case of super-large traffic attack (occupying full bandwidth), it is difficult to schedule the traffic on a large scale in the BGP shunt mode; However, when the attack intensity is lower than the limit, the BGP black hole operation drops all the traffic, which directly leads to the loss of normal traffic of the attacked object.

In SE DOTS, the HTTP request handling module of DOTS framework is extended, and a traffic shunt policy module is added between the DOTS Server and the Mitigator to determine which mitigation method is adopted by the DOTS server. The DOTS system architecture diagram that extends the HTTP mitigation communication approach is shown in Fig. 2.

Cleaning equipment refers to the equipment specially used for DDoS attack traffic cleaning, including hardware and software. Cleaning center refers to a centralized cleaning equipments cluster.

The new process is as follows:

(1) Mitigation request issued by DOTS client;
(2) DOTS server receives the mitigation request, parses the request, transfers the mitigation parameters to the shunt policy module, and starts the shunt strategy to select the BGP or HTTP mitigation mode;
   (a) When BGP mode is selected, the processing flow is the same as Fig. 1;

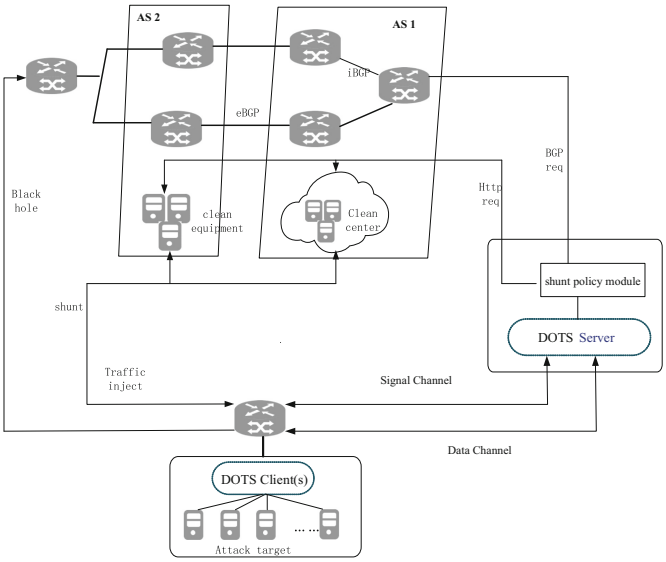

Fig. 2. The DOTS system architecture diagram extending the HTTP method

(b) When select HTTP mode, send the mitigation request to the corresponding cleaning equipment (or cleaning center). The cleaning equipment (or cleaning center) will trigger the flow lead. After processing, the normal business flow will be injected back into the attack target link.

The flow of the shunt policy module is shown in Fig. 3 below.

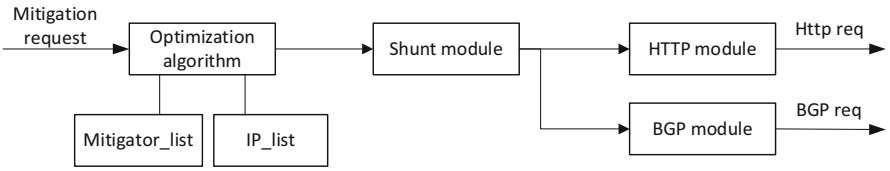

Fig. 3. Processing flow of shunt policy module

Among them, Mitigator_list is the list library of protection devices, and IP_list is the corresponding protection IP of the protection device. The main functions of the shunt strategy module are as follows:

(1) DOTS server parsers parameters, including: target-prefix, target-port-range, target-protocol, target-fqdn, lifetime, target-bandwidth, and target-attack-type;

(2) Take the parsed parameters as the input of the preferred algorithm:
   (a) Compare the target-prefix with the IP_list of the protection device to find the corresponding mitigation provider;
   (b) Select a cleaning device according to the target-protocol;
   (c) Match the bandwidth to the cleaning device capability, and the cleaning device is completely processed within the cleaning capability range. When the capacity is insufficient, the shunt part performs BGP processing. If the cleaning device is selected, select different cleaning devices according to the target-attack-type.

(3) According to the results of the preferred algorithm to select disposal method: when the cleaning device is used for protection, the HTTP module is used to construct an HTTP request, such as POST http://ip:port/traffic/…; when using BGP disposal, BGP request is sent using the BGP module construct.

4 SE DOTS Technical Advantages Analysis and Experiments

In SE DOTS, the Attack Target can report all the attacked situations to the DOTS Server through one message sending, while the DOTS Server can release different types of Attack disposal methods through the shunt module, reducing the communication overhead and improving the efficiency and accuracy of disposal.

Carry out simulation experiments to simulate the existing network in the following experimental network:

- The bandwidth of link A where the protection object resides: 10G;
- traffic model of protection objects: normal service traffic 500M, which are HTTP requests [12] (TCP SYN traffic is generated at the same time); The total limited bandwidth is 1G, and cleaning is performed when the bandwidth exceeds 1G;
- Total attack traffic: 0–10G, using hybrid attack traffic model; There are four types of attacks: UDP Flood (20%), MemCached Flood (25%), SYN Flood (30%) and HTTP Flood [13] (25%). MemCached is not included in UDP and the SYN generated by HTTP is not counted repeatedly.
- The total bandwidth of BGP traction link B: 20G, the use rate of the flow in this link accounts is 60% (simulates existing network), the maximum limitation is 90%, that means that the maximum drainage capacity is 6G;
- Cluster cleaning ability: about 90% of the shunted attack.

Attack Target pre-configured the threshold of SYN, UDP, MemCached, HTTP Attack [14], (assuming that attacks use these four types), perform joint cleaning experiment using environment parameters above [15]. The experimental results of black hole routing (dots-bgp-bhr), bgp-based shunted mode (dots-bgp-fc) and SE DOTS are shown in Figs. 4 and 5 below.

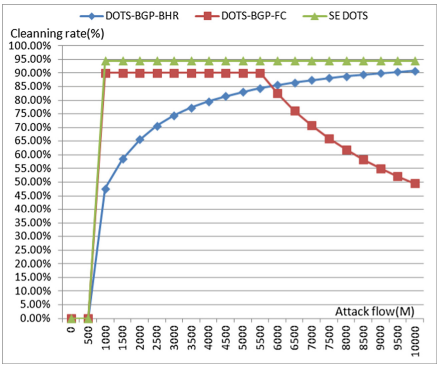

Fig. 4. Cleaning rate comparison during attack

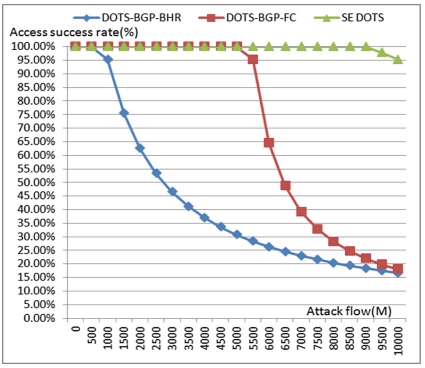

Fig. 5. Comparison of access success rate

In the above scenario, DOTS-BGP-BHR mode can only be discarded according to the sett type. After the attack of the same type exceeds the normal threshold, it can only be discarded according to a certain proportion, so that the access success rate of normal users becomes lower. In the BGP-based DPS-BGP-PC mode, drainable traffic can be disposed. However, because the type of attack cannot be detected, all traffic need to be cleaned, resulting in a waste of network resources and cleaning capacity. Compare the main indicators of DOTS-BGP-BHR, DOTS-BGP-PC, and SE DOTS during the 0–10G attack and calculate the average value. The list is shown in Table 1.

Table 1. SE DOTS attack processing comparative analysis table.

	Cleaning rate	Normal flow rate of false cleaning	User access success rate
DOTS-BGP-BHR	80.0%	63.6%	36.4%
DOTS-BGP-FC	77.5%	31.9%	68.1%
SE DOTS	94.5%	0.4%	99.6%

The experimental results show that, under the same disposal mechanism, SE DOTS can effectively improve the cleaning capacity by 17.0% compared with the existing mechanism dots-bgp-fc, reducing the mis-cleaning traffic/increasing the user access success rate by 31.5%. This mechanism effectively cooperates with the protection capabilities of the existing network and protects the network smoothly and the healthy operation of the business.

5 Conclusion

In this paper, a comprehensive analysis of DDOS attack protection technology is carried out. Based on the DOTS mechanism of IETF, an SE DOTS framework with the capability of sensing and disposing protocol expansion is designed. Based on the

analysis and experimental results, the SE DOTS linkage disposal technology can better identify and handle attacks, ensure the success rate of users accessing services. From the development of the industry, the DOTS linkage disposal technology will be further extended in the scenarios of operators and IDC service providers. It is necessary to further promote industry standardization in subsequent work and reduce the risks brought by DDOS attacks.

References

1. Akamai: How to Protect Against DDoS Attacks - Stop Denial of Service (2016). https://www.akamai.com/us/en/resources/protect-against-ddos-attacks.jsp. Accessed 10 Jan 2017
2. Rodrigues, B.B., Bocek, T., Stiller, B.: Multi-domain DDoS mitigation based on blockchains. In: IFIP International Conference on Autonomous Infrastructure Management and Security, June 2017
3. Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., Stiller, B.: A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In: Tuncer, D., Koch, R., Badonnel, R., Stiller, B. (eds.) AIMS 2017. LNCS, vol. 10356, pp. 16–29. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60774-0_2
4. Mortensen, A., Andreasen, F., Reddy, T., Teague, N., Compton, R.: Draft-ietf-dots-architecture [EB/OL].https://tools.ietf.org/html/draft-ietf-dots-architecture-10
5. Dobbins, R., Migault, D., Fouant, S., Moskowitz, R., Teague, N.: Draft-ietf-dots-use-cases [EB/OL].https://tools.ietf.org/html/draft-ietf-dots-use-cases-16
6. Mortensen, A., Moskowitz, R., Reddy, T.: Draft-ietf-dots-requirements [EB/OL].https://tools.ietf.org/html/draft-ietf-dots-requirements-16
7. Steinberger, J., Kuhnert, B., Sperotto, A., Baier, H., Pras, A.: Collaborative DDOS defense using flow-based security event information. In: NOMS 2016–2016 IEEE/IFIP Network Operations and Management Symposium, pp. 516–522, April 2016
8. Grady, J., Christiansen, C.A., Price, C., Richmond, C.: Worldwide DDoS prevention products and services 2013–2017 forecast. IDC #239954e, vol. 1, March 2013
9. Reddy, T., Boucadair, M., Patil, P., Mortensen, A., Teague, N.: Draft-ietf-dots-signal-channel [EB/OL].https://tools.ietf.org/html/draft-ietf-dots-signal-channel-26
10. Boucadair, M., Reddy, T., Nishizuka, K., Xia, L., Patil, P.: Draft-ietf-dots-data-channel [EB/OL].https://tools.ietf.org/html/draft-ietf-dots-data-channel-24
11. Fayaz, S.K., Tobioka, Y., Sekar, V.: Bohatei: flexible and elastic DDoS defense. In: 24th USENIX Security Symposium, August 2015
12. Jiao, J., Ye, B.: Detecting TCP-based DDoS attacks in Baidu cloud computing data centers. In: IEEE 36th Symposium on Reliable Distributed Systems (SRDS) (2017)
13. Hong, K., Kim, Y., Choi, H., Park, J.: SDN-assisted slow HTTP DDoS attack defense method. IEEE Commun. Lett. **22**, 688–691 (2018)
14. Stevanovic, D., Vlajic, N.: Application-layer DDoS in dynamic web-domains: building defenses against next-generation attack behavior. In: IEEE Conference on Communications and Network Security, October 2014
15. Nagpal, B., Sharma, P., Chauhan, N., Panesar, A.: DDoS tools: classification, analysis and comparison. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) (2015)