Understanding the Behaviors of BGP-based DDoS Protection Services

Tony Miu Tung[1], Chenxu Wang[2,3](✉), and Jinhe Wang[2]

[1] Nexusguard Ltd., Tsuen Wan, Hong Kong
[2] School of Software Engineering, Xi'an Jiaotong University, Xi'an, China
cxwang@mail.xjtu.edu.cn
[3] MoE Key Laboratory for INNS, Xi'an Jiaotong University, Xi'an 710049, China

Abstract. Distributed Denial of Service attacks has been one of the most challenges faced by the Internet for decades. Recently, DDoS protection services (DPS) have risen up to mitigate large-scale DDoS attacks by diverting the vast malicious traffic against the victims to affordable networks. One common approach is to reroute the traffic through the change of BGP policies, which may cause abnormal BGP routing dynamics. However, little is known about such behaviors and the consequences. To fill this gap, in this paper, we conduct the first study on the behaviors of BGP-based DPS through two steps. First, we propose a machine learning based approach to identify DDoS events because there usually lacks data for characterizing real DDoS events. Second, We design a new algorithm to analyze the behavior of DPS against typical DDoS attacks. In the case study of real DDoS attacks, we carefully analyze the policies used to mitigate the attacks and obtain several meaningful findings. This research sheds light on the design of effective DDoS attack mitigation schemes.

Keywords: DDoS attacks · BGP traffic · DPS behavior

1 Introduction

Distributed Denial of Service (DDoS) attacks has been threatening the infrastructure of the Internet for decades. In recent years, DDoS attacks are becoming even more popular with the emergence of the DDoS-as-a-service economy [10,15,17] and the over 1Tbps DDoS attack has been evidenced [2]. These attacks usually bring with victims great financial losses. As a result, the market of DDoS protection services (DPS), which provide the cleansing of traffic through traffic diversion, sees rapid growth in recent days [9].

Traffic diversion allows traffic to be routed through the DPS infrastructure, either in an always-on or on-demand manner. There are two main approaches to divert traffic, including the Domain Name System (DNS)-based method and Border Gateway Protocol (BGP)-based method, respectively. The DNS-based approach diverts network traffic through proper configurations of Domain Name

M. H. Au et al. (Eds.): NSS 2018, LNCS 11058, pp. 463–473, 2018.
https://doi.org/10.1007/978-3-030-02744-5_34

Severs or Anycast techniques. It is similar to what is done in the content delivery networks (CDN). The BGP-based scheme diverts traffic towards the DPS infrastructure for scrubbing by announcing an IP subnet of its customers. Although recent studies have measured the DNS-based approach [9], little is known about the behavior of BGP-based DPS.

To fill this gap, in this paper, we conduct the first study on the behaviors of BGP-based DPS by analyzing the dynamics of BGP messages. BGP is the de facto inter-domain protocol of the Internet and controls how packets are routed through autonomous systems (ASes). To provide a better understanding of BGP dynamics, several projects such as the Route Viewers Project and RIPE keep collecting the update information of edge routers through distributed vantage points. Our analysis consists of two steps. First, we design a machine learning based approach to identify DDoS events from BGP update messages because there usually lacks data for characterizing real DDoS events. It is non-trivial to identify DDoS events from BGP update messages because other disruptive events such as earthquakes, hurricanes, and blackouts may also disturb the BGP dynamics. To address this issue, we first detect BGP anomalies and then design a machine learning based method to determine whether or not a BGP anomaly is caused by DDoS attacks.

To train the classifier, we collect a sufficient number of DDoS attacks and disaster events which are reported to cause abnormal BGP dynamics. For each event, we collect the BGP update messages during the reported time period from the Route views project and then extract features from the BGP update messages within a fixed time interval. After classifying the events into two categories: DDoS attacks and disasters, we use the data to train a random forest classifier, which is utilized to determine the types of other detected abnormal events. More precisely, if a DDoS attack event is identified, we conduct an in-depth analysis of the BGP traffic to characterize how BGP-based DPS leverages BGP to mitigate the attack. To evaluate our approach, we perform retrospective studies on DDoS attacks and the DPS policies, and the experimental results demonstrate the effectiveness of our approach. In summary, we make the following contributions:

(1) We propose a new machine learning based approach to identify DDoS events by analyzing BGP update messages.
(2) We conduct the first analysis on the behavior of BGP-based DPS after DDoS attacks occur.
(3) We develop a new system based on our new algorithms and evaluate it through BGP data associated with real DDoS attacks.

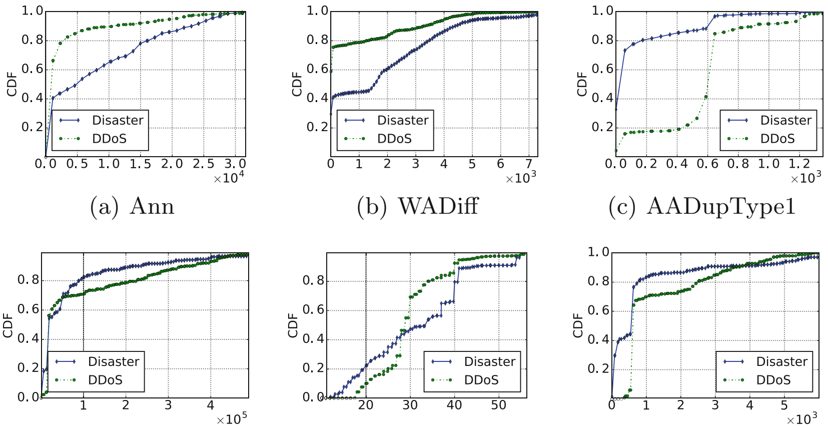
The rest of this paper is organized as follows: In Sect. 2, we analyze the characteristics of extracted features. In Sect. 3, we describe the designed system. Section 4 describes the evaluation results of the system. In Sect. 4, we validate our system with extensive experiments. After reviewing relevant literature in Sect. 5, we conclude this work in Sect. 6.

2 Feature Analysis

We investigate 6 features from BGP update messages to character the fluctuation of the BGP traffic. Table 1 shows the description of the features. These features are borrowed from [12,19]. Figure 1 demonstrates the distributions of features in different types of incidents.

Table 1. Description of features

Features	Definition
Ann	Number of announcements generalized by BGP speakers
WADiff	Number of new announced paths after an explicit withdrawal
AADupType1	Number of duplicate announcements to the same IP prefix
Unq_pfx_as	Number of unique prefixes originated by an AS
Max_AS_path_len	The maximum length of AS-PATHs
pfx_org_chg	Number of Prefix origin change



(a) Ann (b) WADiff (c) AADupType1

(d) Unq_pfx_as feature (e) Max_AS_path_len (f) Asn_prfx_chg

Fig. 1. CDF of the features

Ann is the number of paths announced by BGP speakers in a detection cycle. Figure 1(a) demonstrates that the Ann feature could help the distinction of DDoS events and disaster events. It is shown that DDoS events have about 80% of abnormal databins that have a value of the number of announcements less than 3000. However, no more than 50% of abnormal databins detected in disaster events that have a value less than 3000. This indicates that there will be fewer announcements to be sent in DDoS attacks than that in disaster events. The reason may be that disaster events usually last for a long time, and thus once a route is not available edge routers will announce a new path.

WADiff is the number of newly announced paths after an explicit withdrawal. When a previously announced path is withdrawn, other paths that depend on the withdrawn path may still be chosen and announced, only to be removed one by one [3], which results in the slow convergence of the Internet. We distinguish between explicit or implicit withdrawals based on whether a withdrawal message is sent or not. Explicit withdrawals are those associated with a withdrawal message; whereas an implicit withdrawal occurs when an existing route is replaced by the announcement of a new route to the destination prefix without an intervening withdrawal message. Figure 1(b) illustrates that there are more newly announced routes after an explicit withdrawal during the disaster events. This is because disaster events usually result in unreachability of some BGP routes and thus trigger peer routers to send explicit withdrawals.

AADupType1 is the number of duplicate announcements to the same prefix with all fields unchanged. Park et al. [16] studied the cause of duplicate announcements in BGP traffic and discovered that duplicates are caused by an unintended interaction between eBGP and iBGP. Routers receive updates via iBGP which differ in iBGP attribute values alone, and thus the router believes the updates to be unique. However, once the router processes the update, strips the iBGP attribute values, and sends the update to its eBGP peer, the two updates look identical from the point of view of the eBGP peer [16]. Therefore, the more alternative paths an AS has, the more duplicate announcements. Figure 1(c) presents the distribution of this feature. The distribution of the DDoS attacks shows a sharp increase from 500 to 600. This indicates DDoS attacks usually lead to similar responses of victims, e.g. repeatedly announcing the affected paths.

Unq_pfx_as is the number of unique prefixes originated from an AS in a given time window. The number of announcements and withdrawals exchanged by neighboring peers is an important feature during instability periods. We utilize this feature to model the stable situation of the normal state. From Fig. 1(d), we can see that this feature is more stable during disaster event period than that in DDoS event period. The reason is that when DDoS attacks occur, the DPS provider may well utilize a BGP-based approach by announcing the prefix that belongs to the victim to mitigate the DDoS attack traffic, which leads to the increase of the number of unique prefixes.

Max_AS_path_len is the maximum length of AS paths announced by BGP routers in a specific time window. In a normal state, AS paths announced by BGP routers usually have limited number of hops, since the BGP protocol prefers to short paths. However, when an AS is suffering from attacks, the operator might implicitly withdraw a pre-announced path by pre-pending a number of duplicated ASes in the AS-path field. This could significantly increase the lengths of AS paths. Figure 1(e) shows that the lengths of AS paths for DDoS attack events are concentrated in the range from 25 to 30, which results in the sharp increase of the distribution curve. However, the distribution of the maximum AS path lengths for disaster events is much evener than that for DDoS attacks. This is because that disaster events usually cause outages of the Internet, and thus there are more long paths during disaster events.

ASN (AS number) is a globally unique number that is used to identify an AS. It allows an AS to exchange exterior routing information between neighboring ASes. Asn_prfx_chg is the number of prefix changes of ASes in a time window. This feature is proposed based on the assumption that the Internet topology should not frequently change. It has been used as a single BGP feature to detect prefix hijacking attacks. However, it is also possible for an AS to alter the prefix in order to reroute the traffic of a subnet through the DPS AS. Figure 1(f) demonstrates that there are more prefix origin changes during DDoS attacks. The reason is that when DDoS attack events occur, the DPS provider will announce the prefix that belongs to the victim and scrub the traffic.

3 System Design

Figure 2 gives an overview of our investigation process. It consists of a training phase and a monitoring phase. In both phases, we extract a number of features from the BGP update data within a fixed time interval. We group the extracted features into a vector which is referred to as a databin in the rest of this paper. When a DDoS attack is identified, the BGP update traffic originated from the ASes of DPS will be further analyzed by the mitigation policy analysis module. We develop a prototype of the system, using Python running on a 64-bit Windows 10 system with an Intel(R) CUP Q9550 @2.83GH and 8.0GB RAM.

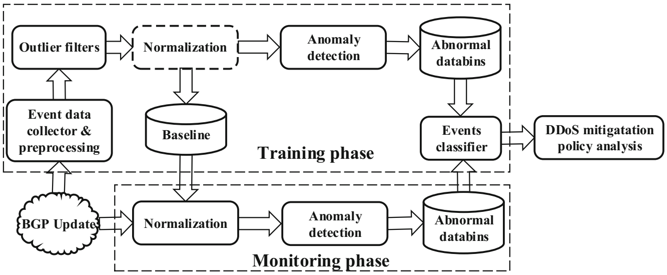


Fig. 2. The architecture of the system

3.1 Training Phase

We first collect many different kinds of events that will cause BGP changes, such as the hurricane, blackout, earthquake, cable cuts, and DDoS attacks. We manually searched the related news about these events to determine the occurrence times of these events. In the training phase, we collect the BGP update data in the time periods that cover the occurrence of these events. Since the BGP traffic is inherently dynamic and there are even some outliers during the normal state, we employ the k-means method to filter out the outlier databins in the normal period [12]. Specifically, the databins in the normal period are clustered into two groups based on their Euclidean distances. The group of the majority is expected to contain only normal databins and is used as the baseline of normality. To ensure that the occurrence periods contains a majority of normal databins, we then mix the normal databins with those in occurrence periods. Again, we employ the k-means method to cluster the mixed databins into two groups. The one of the majority is discriminated as normal and the other as abnormal. We further group the obtained abnormal databins according to the timestamps for obtaining consecutive abnormal databins. Such consecutive abnormal databins fulfill two requirements: (1) their intervals are less than 3 min and (2) they have at least 3 consecutive databins in the cluster. The obtained groups of consecutive abnormal databins are referred to as "incidents".

Second, we manually label the types of the incidents. In this paper, we only distinguish between disaster events and DDoS attacks. We collect 41 historical events and manually label the types of the incidents. The results are summarized in Table 2 and use these events to train the classification model of the random forest method. We only distinguish between disaster events and DDoS attack events. We use 5-fold cross validation method to evaluate the accuracy of the system. The detected abnormal databins in each category is divided into 5 folds and in each test, we use one of the 5 folds as test data and the other 4 folds as training data. The results are obtained by averaging the 5 results. Based on the collected data, we obtained an accuracy of 91.2%.

Table 2. A summary of the dataset

Type	Event number	Detected databins
Hurricane	4	30
Black out	4	14
Earthquake	4	152
Cable cut	9	602
DDoS	20	889

3.2 Monitoring Phase

In the monitoring phase, the newly collected BGP update messages are normalized using the baseline obtained in the training phase. More precisely, in this paper, we utilize a Z-score normalization method to normalize the databins. The Z-score value of a feature is calculated as $z = \frac{x-\mu}{\sigma}$, where μ is the mean of the obtained normal databins and σ is the standard deviation. The calculated mean and deviation are used to normalize the databins in the monitoring phase. The anomaly detection module will detect whether there is an anomaly in the BGP dynamics. If an anomaly is detected, the system utilizes the trained classifier to identify whether the abnormal event is caused by DDoS attacks.

It is worth noting that the system allows practitioners to utilize their experience knowledge to improve the performance of the system. When an alarm is raised, the practitioner could have a judgment on the result based on other external information source. If the prediction agrees with the judgment of the practitioner, the newly incoming databins will be added to the training databins. Otherwise, the prediction will be rejected.

3.3 Mitigation Policy Analysis

We provide a module to analyze the BGP-based mitigation policies utilized by DPS. After a DDoS event is confirmed, we use this module to examine the BGP policies adopted by DPS. It is worth noting that we allow practitioners to utilize their experiences and knowledge to improve the performance of the system. When an alarm is raised, the practitioner could have a judgment on the result based on other external information sources. If the prediction agrees with the judgment of the practitioner, the newly incoming databins will be added to the training databins. Otherwise, the prediction will be rejected.

We develop an algorithm to automatically extract the policies that adopted by DPS providers. When DPS providers find customers are under DDoS attacks, they can perform BGP prepending. Prepending means adding one or more AS numbers to the left side of the AS path. Normally this is done using one's own AS number, using someone else's AS number for this can have unintended side effects. Such protection process would start with a WADiff BGP update message and end with an AW BGP update message. We denote this process as B_0. In the prepending action, the ASN would appear in the BGP routing path, and the WADup BGP update message follows the AW BGP update message. We define the direct protection action as an action that DPS providers' ASN serves as the first hop of the BGP routing path, and the AADiff BGP update message follows the AADiff BGP update message. We denote the prepending action as B_1 and directed protection action as B_2. The algorithm works as follows. First, we label the BGP update records with AW, WWDup, AADupType1, AADupType2, AADiff, WADup, WADiff tags for each victim prefix. After we labeled the BGP update messages, we recognize the B_0, B_1 and B_2 sequences which reflects the policies adopted by DPS providers to protect the victims.

4 Experiments

4.1 Evaluation of DDoS Attack Detection

Our system succeeded to detect the DDoS attack against the Dyn in October, 2016 [8]. On October 21, 2016, the Dyn suffers from DNS queries from a large vast of clients, which consume the ability of the managed DNS network. This caused the unavailability of the DNS service of the Dyn. This further results in the difficulties in connecting numerous websites. During the attack, the traffic going to the other DNS providers increased dramatically and thus caused the wide-spread congestion of network traffic. This congestion eventually results in the abnormal dynamics of BGP traffic, which enables us to detect the Dyn DDoS attack event through the BGP dynamics.

Figure 3 illustrates the impact values versus the time. The impact value, which is the sum of the differences between the normalized features and the baseline, represents the distance of a databin from the normal ones. Three periods of abnormal dynamics are illustrated by three red blocks on October 21, 2016. Our anomaly detection module is able to identify these abnormal databins and correctly classified them as DDoS attacks. The detected abnormal periods are described as follows:

– The first period started at 04:30:22 (PDT), and fluctuations of BGP traffics began. Until around 06:16:00 (PDT), the fluctuations diminished. This coincides with the reported start and mitigation time of the incident [18]. During this period, the Dyn's DNS server platforms in the Asia Pacific and East Europe suffered from massive requests, and then the US-East region, resulting in the vast BGP route dynamics [8].
– According to our system detection results, the second period started at 08:41:44 (PDT) and ended at around 10:32:00 (PDT), which also agrees to the reported DDoS attack period [1].
– Our system also detected the third period of abnormal BGP dynamics which started at 13:19:28 and ended at around 14:08:0 (PDT). This is also consistent with the DDoS attack period reported in the news [8].

We also found some additional obvious fluctuations in the BGP traffic, which started at 01:22:23 (PDT) and 17:47:1 respectively, as shown in Fig. 3 with green blocks. However, these events are not reported by the Dyn.com or other news media. We speculate these events were caused by the initiation and aftershocks of the DDoS attacks (Table 3).

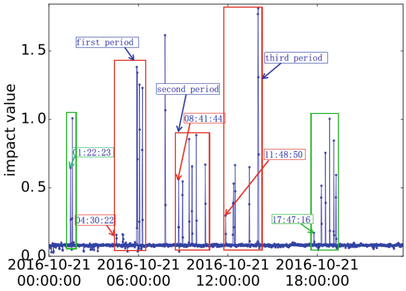


Fig. 3. Dyn DDoS attack overview

5 Related Work

Many studies have addressed the detection of instability or pathological behavior of the BGP dynamics. Labovitz et al. [11] investigated the BGP routing messages and found that the volume of routing update is more redundant than expected.

Table 3. DPS protection behaviors of update pattern sequences of three prefixs

Prefix	Update pattern sequence
58.64.128.119/32	WADiff→B1→B1→B1→B2→B1→AW
58.64.138.186/32	WADiff→B1→B1→B2→AW
58.64.135.102/32	B0→B0

Besides, they revealed several unexpected trends of both forwarding instability and routing policy fluctuations. Deshpande et al. [6] proposed an online instability detection architecture which applies statistical pattern recognition techniques to detect the instabilities of GBP dynamics. They found that features like AS path length and AS path edit distance are very effective in modeling the behaviors of the Internet topology. Chang et al. [4] proposed an algorithm to identify inter-domain path-change events from streams of BGP updates. Feldmann et al. [7] proposed a methodology to identify the origin of routing instability from BGP updates. Several studies utilize statistical pattern recognition techniques to detect the instabilities of BGP routing dynamics [6,11,13]. Compared to these studies, in this paper, we propose a machine learning based method to distinguish between DDoS attack events and disruptive disaster events, which are two main causes of abnormal BGP dynamics. This allows identifying whether there is a DDoS attack going on when a BGP traffic anomaly is detected.

Many retrospective studies have also been conducted by analyzing the impacts brought by historical events such as blackouts, cable cuts, worms, and prefix-hijacking attacks, etc. Cowie et al. [5] analyzed the global BGP routing instabilities caused by the Code Red II and Nimda worms occurred in July and September 2001, respectively. They found that the impact was more serious than publicly revealed in the blacked-out region. Li et al. [14] analyzed the BGP behavior during large-scale power outages from a perspective of both the global and prefix levels. They found there was an increase in the number of withdraws at the global level. Consequently, there was a sharp decrease in the number of edges and nodes at the prefix level. These studies mainly concern the impacts of disruptive events on the performance of BGP routing. In this paper, we focus on the disruptions caused by DDoS attack and impacts of different DPS policies.

6 Conclusion

In this paper, we investigate the behaviors of BGP-based DDoS protection services. To identify the abnormal BGP dynamics caused by DDoS attacks, rather than other disruptive events such as earthquake, blackout, cable cut, etc., we train a proper classifier based on a dataset of more than 40 manually collected events which have been demonstrated to cause abnormal behaviors of BGP dynamics. We also develop a system for detecting DDoS events through abnormal BGP update messages and design a new algorithm to analyze the behavior of DPS against typical DDoS attacks. By applying the system to real

DDoS attacks, we identify the policies used by DPS to mitigate the attacks and obtain several meaningful findings. This research sheds light on the design of effective DDoS attack mitigation schemes.

Acknowledgment. The research presented in this paper is supported in part by National Natural Science Foundation (No. 61602370, 61672026, 61772411, U1736205), Postdoctoral Foundation (No. 201659M2806, 2018T111066), Fundamental Research Funds for the Central Universities (No. 1191320006), Shaanxi Postdoctoral Foundation, Project JCYJ20170816100819428 supported by SZSTI, CCF-Tencent Open Fund WeBank Special Funding (No. CCF-Webank RAGR20180101), CCF-NSFOCUS Kun-Peng Research Fund (No. CCF-NSFOCUS 2018006).

References

1. How friday's massive ddos attack on the U.S. happened. https://en.wikipedia.org/wiki/2016_Dyn_cyberattackcite_note-wired-5/
2. OVH suffers from 1.1Tbps DDoS attack. https://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/532197/. Accessed 11 Mar 2017
3. Chandrashekar, J., Duan, Z., Zhang, Z.L., Krasky, J.: Limiting path exploration in BGP. In: 24th Annual Joint Conference of INFOCOM, vol. 4, pp. 2337–2348. IEEE (2005)
4. Chang, D.F., Govindan, R., Heidemann, J.: The temporal and topological characteristics of BGP path changes. In: ICNP, pp. 190–199. IEEE (2003)
5. Cowie, J., Ogielski, A.T., Premore, B., Yuan, Y.: Internet worms and global routing instabilities. In: ITCom 2002: The Convergence of Information Technologies and Communications, pp. 195–199 (2002)
6. Deshpande, S., Thottan, M., Ho, T.K., Sikdar, B.: An online mechanism for BGP instability detection and analysis. IEEE Trans. Comput. **58**(11), 1470–1484 (2009)
7. Feldmann, A., Maennel, O., Mao, Z.M., Berger, A., Maggs, B.: Locating internet routing instabilities. ACM SIGCOMM CCR **34**, 205–218 (2004)
8. Hilton, S.: Dyn analysis summary of friday october 21 attack. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
9. Jonker, M., Sperotto, A., van Rijswijk-Deij, R., Sadre, R., Pras, A.: Measuring the adoption of DDoS protection services. In: Proceedings of the 2016 ACM on Internet Measurement Conference, pp. 279–285. ACM (2016)
10. Karami, M., McCoy, D.: Understanding the emerging threat of DDoS-as-a-service. In: LEET (2013)
11. Labovitz, C., Malan, G.R., Jahanian, F.: Internet routing instability. IEEE/ACM Trans. Netw. **6**(5), 515–528 (1998)
12. Li, J., Brooks, S.: I-seismograph: observing and measuring internet earthquakes. In: INFOCOM, 2011 Proceedings IEEE, pp. 2624–2632. IEEE (2011)
13. Li, J., Guidero, M., Wu, Z., Purpus, E., Ehrenkranz, T.: BGP routing dynamics revisited. ACM SIGCOMM CCR **37**(2), 5–16 (2007)
14. Li, J., Wu, Z., Purpus, E.: Cam04-5: Toward understanding the behavior of BGP during large-scale power outages. In: IEEE Globecom. IEEE (2006)
15. Noroozian, A., Korczyński, M., Gañan, C.H., Makita, D., Yoshioka, K., van Eeten, M.: Who gets the boot? analyzing victimization by DDoS-as-a-service. In: Monrose, F., Dacier, M., Blanc, G., Garcia-Alfaro, J. (eds.) RAID 2016. LNCS, vol. 9854, pp. 368–389. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45719-2_17

16. Park, J.H., Jen, D., Lad, M., Amante, S., McPherson, D., Zhang, L.: Investigating occurrence of duplicate updates in BGP announcements. In: Krishnamurthy, A., Plattner, B. (eds.) PAM 2010. LNCS, vol. 6032, pp. 11–20. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12334-4_2
17. Santanna, J.J., et al.: Booters-an analysis of DDoS-as-a-service attacks. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 243–251. IEEE (2015)
18. Smith, D.: How friday's massive ddos attack on the U.S. happened. https://blog.radware.com/security/2016/10/fridays-massive-ddos-attack-u-s-happened/
19. Zhang, M.: BGPInspector: A real-time extensible border gateway protocol monitoring framework. CAS (2014)