ATLANTIS PRESS

Advances in Computer Science Research, volume 80

International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)

Characterizing the Impact of DDoS Attack on Inter-domain Routing System: A Case Study of the Dyn Cyberattack

Yujing Liu[1,*], Zhilin Wang[2] and Nan Li[1]

[1]College of Computer, National University of Defense Technology, Changsha, China
[2]Education Department, National University of Defense Technology, Changsha, China
[*]Corresponding author

***Abstract*—The inter-domain routing protocol BGP is sensitive to severe network congestion. In order to study the reliability of BGP under stress, we take the Dyn cyberattack on October 21st, 2016 as a study case to characterize the impact of DDoS attack on inter-domain routing system. We propose several metrics including number of BGP updates, reachability, and variance of AS link betweenness centrality to measure the reachability and stability of the Internet. After performing a thorough analysis based on publicly available BGP data, we obtain key insights about the event. Firstly, the attack affects the reachability from the inter-domain routing perspective, but the effect is very small. Secondly, during the attack, the Internet experiences an unstable routing state in terms of a surge of BGP updates and changes of AS links' betweenness centrality. Finally, route flapping doesn't happen, probably because of anycast routing technique employed by Dyn, balancing high volume of traffic among multiple data centers instead of converging in one single link.**

Keywords—Internet; inter-domain routing system; DDoS; BGP

I. INTRODUCTION

The inter-domain routing system of the Internet consists of thousands of autonomous systems (ASes). Border Gateway Protocol (BGP) is the de facto protocol for inter-domain routing system, transmitting routing information among ASes. Reliability of BGP is very important to achieve stable communications in the Internet. Currently, the routing control packets of BGP, such as keepalive packets, share bandwidth and buffer space with normal data traffic. This co-location of control plane and data plane makes BGP sensitive to severe network congestion [1-3]. Therefore, the distributed denial-of-service (DDoS) attack which generates high volume of traffic will affect the inter-domain routing system. Previous researches about this subject haven't provided thorough analysis, especially in the real Internet environment.

On October 21st, 2016, a series of large-scale DDoS attacks were launched against a DNS provider - Dyn. The cyberattack caused major Internet platforms and services, such as Twitter, Paypal, Github, Amazon, to be unavailable to plenty of users in Europe and North America. These critical services are customers of Dyn [4]. In this paper, we take this event as a study case to characterize the impact of DDoS attack on inter-domain routing system, in order to answer the following questions: Does the attack affect the reachability and stability of inter-domain routing system? Does route flapping happen as mentioned by related work [1]?

We propose several metrics including number of BGP updates, reachability, and variance of AS link betweenness centrality to characterize the reachability and stability of inter-domain routing system under this DDoS attack. By analyzing publicly available BGP data, we find that (1) the attack affects the reachability, but the effect is very small; (2) during the attack, the inter-domain routing system experiences an unstable routing state in terms of a surge of BGP updates and changes of AS links' betweenness centrality; (3) but route flapping doesn't happen, probably because of anycast routing technique among multiple data centers by Dyn, preventing high volume of traffic from converging in one single link.

II. RELATED WORK

Reference [1] introduces the Coordinated Cross Plane Session Termination, or CXPST, attack, a distributed denial of service attack that attacks the control plane of the Internet by using data plane traffic. By carefully choosing BGP sessions to terminate, CXPST induces targeted route flapping, moreover, generates a surge of BGP updates that are seen by nearly all core routers on the Internet. The CXPST attack can be considered as a kind of DDoS attack. The conclusion of their work is based on simulation results. In our paper, we are going to examine whether the conclusions are founded in the real Internet under real DDoS attack.

Reference [5] provides the first evaluation of several IP anycast services under DDoS attack with public data. They employ BGP data to evaluate whether there are route changes during the attack. The metric is simply the amount of BGP route changes over time. However, in order to characterize different perspectives of the Internet, more well defined metrics and characteristics should be proposed and evaluated.

Generally speaking, there is few related work about analyzing impact of DDoS attack on inter-domain routing system. In this paper, we propose several new metrics to characterize the impact by analyzing a real attack in the real environment.

III. METHODOLOGY

The key function of inter-domain routing system is to find a route for a peer of source and destination. Therefore, we define several metrics to characterize how a DDoS attack affects the routing process of the Internet.

A. BGP Routing Data Source

We explore the inter-domain routing data by analyzing BGP RIBs (Routing Information Bases) and updates collected by RIPE RIS [6] and Route Views [7]. These two projects employ multiple Remote Route Collectors (RRCs) to establish BGP peering sessions with many ASes around the world, collect their routing information to all the other destination ASes, and periodically dump their BGP routing tables and updates. Therefore, we can get routes from those monitors to routable IP prefixes in the Internet at a certain period of time. The available data from multiple vantage points reveals a broad and global though necessarily incomplete view of inter-domain routing over time. We use this data to sample the Internet's behavior after DDoS attacks.

B. Number of BGP Updates

BGP is a routing protocol driven by route changes. In other words, routing information carried by BGP update messages are exchanged among routers only when there are some changes in the inter-domain routing system, such as changes of topology and routing policy. Therefore, large amounts of updates indicate an unstable routing state of the Internet. In this paper, we calculate the number of BGP updates associated with particular IP prefixes in every 10 minutes for a period of time *T*. The BGP updates which we concern about consist of announcements and withdrawals. Announcement means appearance of route, whereas withdrawal means disappearance of route.

C. Reachability

Reachability measures whether there is an available route between source and destination in the inter-domain routing system. In this paper, we measure the reachability from monitors to certain IP prefixes. *M* is the set of monitors. It is formally defined as follows:

$$R_{mp} = \begin{cases} 1, \text{ if there is a route from } m \text{ to } p \\ 0, \text{ if there isn't a route from } m \text{ to } p \end{cases} \quad (1)$$

$$R_p = \sum_{m \in M} R_{mp} \quad (2)$$

The reachability from monitor *m* to prefix *p* is equal to 1 if there is an available route from *m* to *p*. It is equal to 0 if there is not. The reachability of prefix *p* is the summation of reachability from all the monitors in *M*. We measure the reachability for a period of time *T* and then obtain a sequence of reachability changes during that time.

D. Variance of AS Link Betweenness Centrality

Not all the BGP updates reflect inter-domain routing changes. Some of them are duplicated from the perspective of inter-domain routing because of intra-domain routing changes or just pathological duplicates. In this paper, we propose a metric named *variance of AS link betweenness centrality* to characterize inter-domain routing changes.

We model the Internet as a graph $G = (V, E)$ where V is the set of all ASes, and E is the set of AS links. Let e be an AS link in E, then its betweenness centrality associated with prefix p is defined as:

$$BC_p(e) = \sum_{m \in M} \sigma_{mp}(e) \quad (3)$$

where $\sigma_{mp}(e)$ denotes the total number of AS paths between monitor *m* and prefix *p* that pass through link *e*. Inter-domain routing changes will result in the changes of some AS links' betweenness centrality. Accordingly, we define the variance of AS link betweenness centrality to measure the difference of it at time *t*-1 and *t* as follows:

$$\Delta BC_{pt}(e) = BC_{pt}(e) - BC_{p(t-1)}(e) \quad (4)$$

We measure the variance of AS link betweenness centrality of every link in *E* for a period of time *T* to construct a variance matrix $\Delta\mathbf{BC}_p$, where every row represents a sequence of betweenness centrality changes associated with each AS link.

Analysis results from different dimensions of the variance matrix reveal useful characteristics such as the aggregated time of routing changes and the dominant routing patterns.

1) Aggregated time of routing changes: Each column of $\Delta\mathbf{BC}_p$ contains every AS link's betweenness centrality change at time slot *t*. We calculate the mean value of all links' absolute variation at time *t*, denoted as μ_{pt}. Large value of μ_{pt} indicates aggregated time of routing changes.

2) Dominant routing patterns: Each row of $\Delta\mathbf{BC}_p$ consists of betweenness centrality changes over time associated with a certain AS link *e*. We split all rows into two clusters using K-Means algorithm according to their absolute value. Because the variance of AS link betweenness centrality often demonstrates a 'power-law' distribution, the smaller cluster contains the dominant routing patterns. Moreover, routing patterns in the smaller cluster often show synchronization of route changes. Further analysis with the value of variation enable us to differentiate the correlative and backup relations.

IV. CHARACTERIZING THE IMPACT OF DYN DDOS ATTACK

The Dyn DNS network consists of four IP routing prefixes – 204.13.250.0/24, 204.13.251.0/24, 208.78.70.0/24 and 208.78.71.0/24. These prefixes are in AS33517. Many critical services, such as Twitter, Paypal, Github, Amazon and so on, employ Dyn DNS servers to be publicly available. As shown in Table 1, the DNS IPs of one customer are dispersed in four

prefixes, ensuring redundancy when a catastrophic failure happens. Unfortunately, the targets of this DDoS attack include all the four prefixes. Therefore, all the critical customers are affected. In this paper, we take these four prefixes as analyzing targets to characterize the impact of this attack.

TABLE I. EXAMPLES OF DYN DNS SERVER IP

Customer	DNS Server	DNS Server IP
twitter.com	ns1.p34.dynect.net	208.78.70.34
	ns2.p34.dynect.net	208.78.71.34
	ns3.p34.dynect.net	204.13.250.34
	ns4.p34.dynect.net	204.13.251.34
paypal.com	ns1.p57.dynect.net	208.78.70.57
	ns2.p57.dynect.net	208.78.71.57
	ns3.p57.dynect.net	204.13.250.57
	ns4.p57.dynect.net	204.13.251.57

A. Number of BGP Updates

According to technical report [4], the DDoS attack starts at 11:15 UTC on October 21st, 2016. We calculate the number of BGP updates associated with the four IP prefixes in every 10 minutes from 00:00 to 24:00 on that day. From the results shown in Figure 1, we can see that the amount of announcement updates increases dramatically after the attack starts. Moreover, the increasing patterns associated with the four prefixes indicate that 204.13.250.0/24 and 204.13.251.0/24 are in the same constellation, whereas 208.78.70.0/24 and 208.78.71.0/24 are in the same constellation. The emergence of updates is an indication that the inter-domain routing system experiences an unstable routing state.

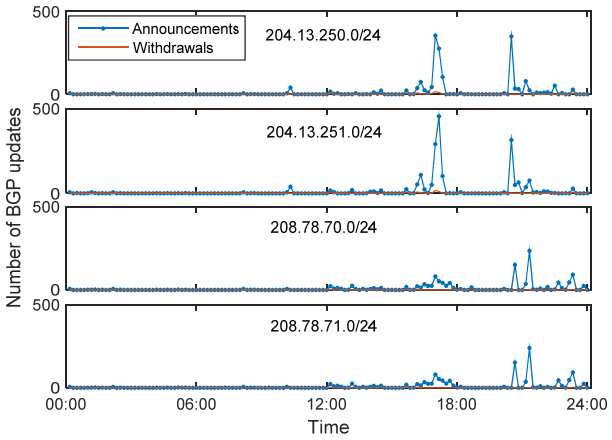


FIGURE I. NUMBER OF BGP UPDATES

B. Reachability

Along with the high volume of DDoS traffic toward the DNS sever, many services become unavailable. In this paper, we examine whether the DDoS affect the reachability from multiple monitors to DNS server prefixes. The measurement results in Figure 2 show that the attack indeed affects the reachability from the inter-domain routing perspective, but the effect is small, which is less than 5% averagely.

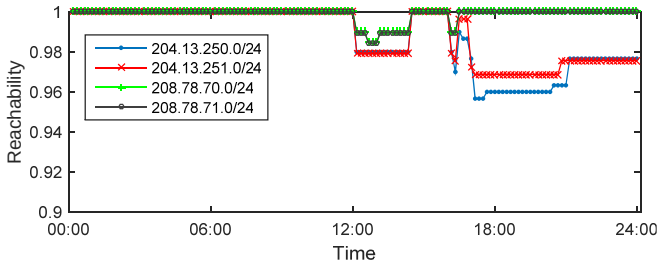


FIGURE II. CHANGES OF REACHABILITY

C. Aggregated Time of Routing Changes

By parsing the BGP RIB and update data associated with the four prefixes during one day, we maintain four variance matrixes of AS link betweenness centrality. These matrixes reflect non-redundant inter-domain routing changes. The values of μ_{pt} associated with the four prefixes are shown in Figure 3. Comparing with Figure 1, we find that routing changes and the emergences of BGP updates appear almost at the same time, but with different changing patterns. Updates of 204.13.250.0/24 and 204.13.251.0/24 contain more duplicated messages from the perspective of inter-domain routing. The aggregated time of routing changes include 16:50-17:20 and 20:20-20:30. We denote the first period as *T1*, and the second period as *T2*.

D. Dominant Routing Patterns

The variance matrix $\Delta \mathbf{BC}_p$ of prefix 204.13.250.0/24 contains 458 rows, representing there are 458 AS links change at least once during that day in terms of inter-domain rerouting. In addition, matrix of 204.13.251.0/24 has 444 rows; matrix of 208.78.70.0/24 has 167 rows; and matrix of 208.78.71.0/24 has 161 rows. We divide the rows of variance values according to our clustering method mentioned before. The dominant routing patterns associated with four prefixes are shown in Figure 4. We infer that because of the high volume of DDoS traffic, BGP keepalive messages may be dropped by neighbor routers, making BGP sessions disconnect. Then routers will choose alternative routes to reach destinations. Therefore, the betweenness centrality of AS links will change accordingly.

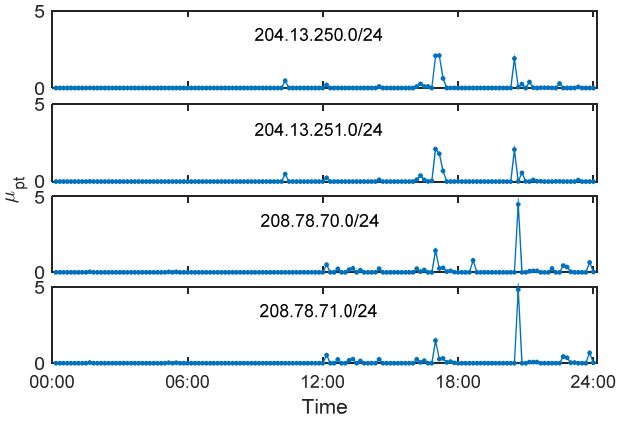
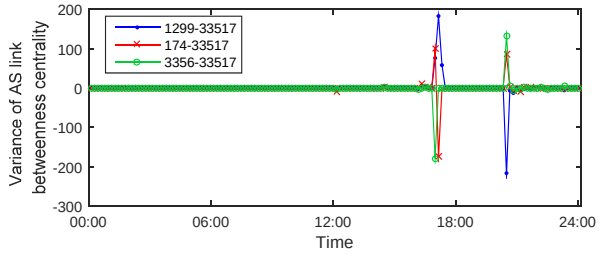
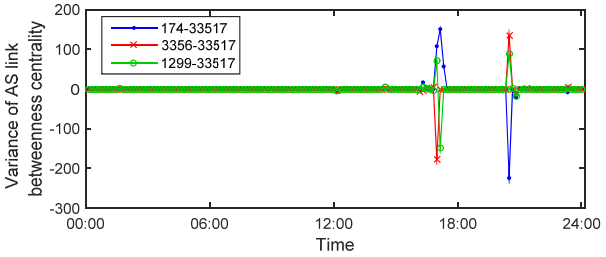


FIGURE III. AGGREGATED TIME OF ROUTING CHANGES

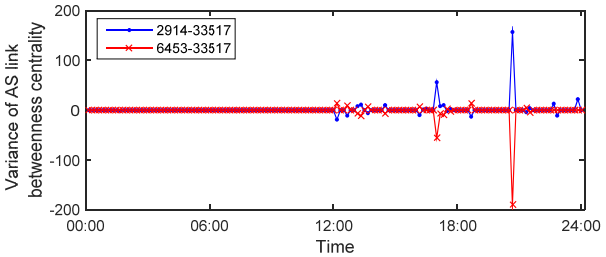
Take the first figure as an example. During period *T1*, paths from AS3356 to AS33517 are rerouted to paths through AS1299. Number of paths from AS174 to AS33517 increases first, and then decreases in the next 10 minutes. During period *T2*, paths from AS1299 to AS33517 are rerouted back to paths through AS174 and AS3356. From the dominant routing patterns we infer that AS1299, AS174 and AS3356 are multi-home providers of AS33517. Disconnection in one neighbor will result in routing changes to another neighbor, making the inter-domain routing system more reliable. Comprehensive analysis of the four figures reveals the fact that during DDoS attack, the Internet experiences more routing changes than usual time, but route flapping mentioned in related work [1] doesn't happen. We infer it is a consequence of anycast routing technique among 20 data centers by Dyn [4], preventing high volume of traffic from converging in one single link.



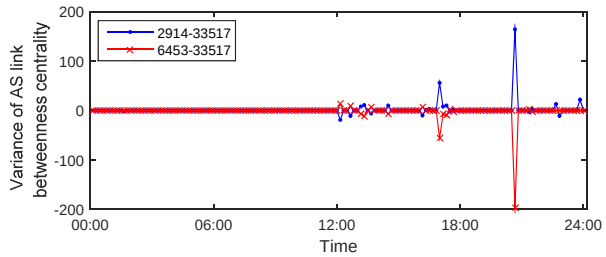
(a) Dominant routing patterns of 204.13.250.0/24



(b) Dominant routing patterns of 204.13.251.0/24



(c) Dominant routing patterns of 208.78.70.0/24



(d) Dominant routing patterns of 208.78.71.0/24

FIGURE IV. DOMINANT ROUTING PATTERNS

V. CONCLUSION

In this paper, we take the Dyn cyberattack event as a study case to characterize the impact of DDoS attack on inter-domain routing system. We propose several metrics to measure the characteristics of the impact including number of BGP updates, reachability, aggregated time of routing changes and dominant routing patterns. After performing a thorough analysis, we find that (1) the attack affects the reachability from the inter-domain routing perspective, but the effect is very small; (2) during the attack, the inter-domain routing system experiences an unstable routing state in terms of a surge of BGP updates and changes of AS links' betweenness centrality; (3) but route flapping doesn't happen, because of anycast routing technique among multiple data centers by Dyn, preventing high volume of traffic from converging in one single link.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China, under Grant No. 61602503 and No. 61472437.

REFERENCES

[1] M. Schuchard, A. Mohaisen, D. Kune, N. Hopper, Y. Kim, and E. Vasserman, "Losing Control of the Internet: Using the Data Plane to Attack the Control Plane," in Proc. of CCS '10, pp. 726–728, 2010.

[2] W. Deng, P. Zhu, X. Lu and B. Plattner, "On evaluating BGP routing stress attack," Journal of Communications, vol. 5, no. 1, pp. 13-22, 2010.

[3] H. Liu, X. Hu, D. Zhao and X. Lu, "Failure Isolation based Defense against Internet CXPST-like Attack," International Journal of Hybrid Information Technology, vol. 5, no. 2, pp. 175–180, 2012.

[4] N. Kephart, "The DDoS Attack on Dyn's DNS Infrastructure," https://blog.thousandeyes.com/dyn-dns-ddos-attack/, 2018.

[5] G. Moura, R. Schmidt, J. Heidemann, W. Vries, M. Muller, L. Wei, and C. Hesselman, "Anycast vs. DDoS: evaluating the November 2015 root DNS event," In Proceedings of the 2016 ACM on Internet Measurement Conference, pp. 255-270, 2016.

[6] RIPE Routing Information Service (RIS), http://www.ripe.net/ris, 2018.

[7] University of Oregon Route Views Project, http://www.routeviews.org, 2018.