A Method of Route Leak Anomaly Detection Based on Heuristic Rules

Jingwei Liu[1, 2 a], Bin Yang[2], Jinju Liu[2], Yuliang Lu[2] and Kailong Zhu[2]
[1]Electronic System Engineering Company of China, Beijing 100079, China;
[2]Electronic Engineering Institute, Hefei 230037, China.
[a]jjszjpsg@163.com

Keywords: inter-domain routing system, anomaly detection, AS relationship, route leak anomaly.

Abstract. This paper presents a method of route leak anomaly detection based on optimized "valley" rule. This paper amended the “valley” rule which used to detect route leak anomaly to improve the route leak detection precision. The experimental results show that the AS relationship recognition algorithm can recognize the AS relationship effectively and the amendment rules of route leak anomaly detection can be used to improve the detection precision effectively.

1. Introduction

As an important infrastructure of Internet, the running status of inter domain routing system will directly affect the operation and security of the internet. The abnormal behavior in the inter domain routing system mainly includes the routing hijacking exception and the route leaking exception① Route hijacking abnormal mainly refers to the interference of the BGP routing table, the attack illegal takeover of IP network, which is the most common abnormal behavior of the inter domain routing system, usually by malicious attacks or configuration errors caused. ②Routing leakage anomaly refers to the violation of the pre specified business relationship between AS. At present, domestic and foreign scholars for routing hijacking anomaly detection method carried out a lot of study [1-4] on leak detection of abnormal routing is relatively less, the main reason is that due to leakage of routing anomaly detection requires a combination of AS business relationship, and the AS for economic and security reasons did not publicly the information.

At present, the abnormal leakage routing is usually carried out according to "valley" rules, namely a AS path between the AS business relationship should meet the "valley" rules, so the detection and leakage between the AS routing business relationship by close contact. Since the AS business relationship is the internal information of each domain, it will not disclose the information. In order to deal with this problem, many researchers focus on the identification of business relationships.

In 2001, Gao[5] for the first time to study the AS relation recognition method, pointed out that the AS path should be consistent with the "mountain" rules, the definition of "uphill" and "downhill path" and proposed based on the maximum "uphill, downhill path thought business relationship recognition algorithm, the experimental results show that, although the algorithm is better able to identification of provider customer relationship, but because the algorithm is based on the maximum" uphill, downhill path of thought, so there are some limitations in identifying peer relationship. Giotsas[6] based on the community attribute of the route, in addition to the business relationship[7] between some of the autonomous domain, and the routing path analysis, found that there are a number of Internet in violation of the "valley" rules of the route. Long term follow-up found that existing in the network part against the "mountain" rules of the routing time is longer, the leak and routing the shorter life cycle of the abnormal phenomenon is not consistent, so whether the routing is legitimate. Further analysis shows that this kind of autonomous domain can be divided into the following four categories: network providers, text providers, IXP and autonomous regions for research purposes.

2. Brief Introduction of Business Relationship between AS and Route Leakage Analysis

2.1 Brief Introduction of as Business Relationship.

Because of financial constraints and other reasons, different types and complex business relationship between the business operations of the AS Gao [5], after a detailed analysis that the AS of the business relationship between the main providers can be divided into customer relationship (provide-to-customer, P2C), peer relationship (peer-to-peer, P2P), sibling relationship (sibling-to-sibling, S2S):

Provider to customer relationship: there are a lot of different sizes in the AS network, the smaller AS may be in the network is the position of the edge, in order to achieve access to the Internet, the need to apply for AS service in the center network or the larger AS, so that their data flow through the AS can realize the normal access to the network. As a price, these AS need to pay a certain fee to large AS, only after the payment access, large AS will provide forwarding traffic to other AS services. The above business relationship is the provider customer relationship, in which the service provider is called the provider, and the AS is the customer.

Peer to peer relationship: peer relationships are equal and mutually beneficial relationships between two similar AS, either party can directly (without the need for providers) to achieve free access to the other party. Peer to peer relationship is an important part of the business relationship, which alleviates the traffic load to some extent.

Sibling relationships: a sibling relationship has the same function as a peer relationship, allowing access to AS. At the same time, to meet the relationship between the compatriots AS can also provide traffic forwarding services to each other, and the same with the same peer relations are free. In the Internet, this kind of relationship is relatively small, usually in the domain of different ISP belongs to the autonomous domain, more in the same ISP between the autonomous domains.

2.2 Analysis of Routing Leakage Anomaly.

An exception is a violation of an input policy or an output policy. At present, there is not an accepted definition of route leakage in the field of research. In this paper [8], a definition is given, but it is not universally accepted. After that, Li Song [9] according to the analysis of the specific route leakage events[10-11], summed up the three characteristics to define the route leakage behavior: ① the route of routing notification is not legal; ②the routing of the routing notification is a violation of the routing policy between AS; ③Route leakage is the result of the redirection of traffic[9]. Obviously, this definition is more objective and easy to understand, and can fully explain the phenomenon of routing leakage. Figure 1 shows an example of route violation that violates the equivalence relationship and provider client relationships:

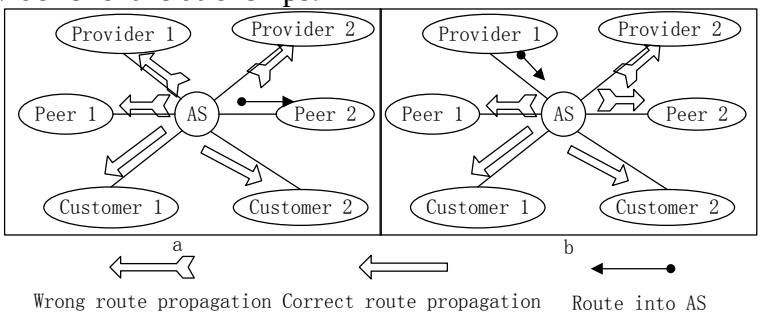

Fig. 1 Example of route leak anomaly

In Figure 1a, from Peer2 to AS routing, the routing domain spread to their providers and Peer1, which is obviously contrary to the output strategy of commercial relations, the autonomous domain AS undertakes the provider and peer traffic load; figure 1b, autonomous domain AS will come from the provider Provider1 routing notice to their outward provider Provider2 and all of the peer domain, apparently contrary to the output routing strategy. Overall, although these routes can meet the BGP protocol routing rules, but due to the violation of the routing input strategy, business relations and output strategies, lead customers still need to provide the service provider relay abnormal

phenomenon after the payment of the cost to the provider, obviously this kind of routing is not normal.

3. Routing leak detection rule

Due to the fact that AS-PATH is a violation of the "valley" rule which exists in the path, the detection method is usually based on the AS relation to detect the anomaly of the route. Pay attention to the literature [8] assertion, that not all AS-PATH can meet the "valley" rules, this paper made some changes in the existing "mountain" rules, proposes a routing leak detection method is as follows:

Step1: The data to be monitored are consistent with the autonomous domain referred to in the literature [8]. In order to facilitate the description, this type of autonomous domain is denoted as shown in table 1.

Table 1 List of $viol\_valleyASs$

AS number	purpose	AS
7575	Education / Research	AARNet
6447	Education / Research	RouteViews
11537	Education / Research	Internet2
12654	Education / Research	RIPE RIS
680	Education / Research	DFN
4608	non-profit	APNIC
1930	Education / Research	FCCN
6881	non-profit	NIX
553	Education / Research	BelWue
11096	Education / Research	FLR
6695	non-profit	DE-CIX
2152	Education / Research	CENIX

Step2: There is no conflict between the sibling relationship and the "valley" rule, so in the process of using the "valley" rule to monitor the route leakage, we ignore the existence of the self-relation. The path to the "valley" rule can be summarized as follows:

①For any autonomous domain pairs in the path $<\alpha_i,\alpha_{i+1}>$, which $i<j$ .Its business relationship is P2C (or C2P);

②If the autonomous domain pair in the path $<\alpha_1,\alpha_2>$ is a peer-to-peer relationship, the other is the path $<\alpha_i,\alpha_j>$ should be P2C relationship, which $i<j$;

③If the autonomous domain pair in the path $<\alpha_{n-1},\alpha_n>$ is a peer-to-peer relationship, the other is the path $<\alpha_i,\alpha_j>$ should be C2P relationship, which $i<j$;

④If exist k , When $j<k$, For the path of $<\alpha_i,\alpha_{i+1}>$ are c2p relationship, which $i<j$, There is only one pair of equivalence relations for subsequent autonomous domain pairs, Namely $<\alpha_k,\alpha_{k+1}>$, The remaining autonomous domain pairs are P2C relations.

Step3: Violation of the above rules of routing data are identified as the path of the existence of abnormal routing leakage.

4. Experiment and Result Analysis

From January 1, 2013 8:00 and February 1st 8:00 when routing data sets, which extract the path information to verify the effectiveness of routing algorithm proposed in this paper is the leak detection and recognition based on the algorithm proposed in this chapter a 2013 inter domain commercial relations, and as the auxiliary knowledge is often different routing leak detection.

4.1 Verification Method for Routing Leakage Anomaly.

Because routing leakage is usually due to configuration errors caused by[14], resulting in the abnormal in the network life cycle is relatively short, therefore, the correctness of the method of tracking abnormal path to verify the results of detection of anomalies detected by long time observation, if the survival period is short, the routing leak algorithm detected abnormal is true and accurate, otherwise, a false alarm. Accordingly, this paper sets up the route leak definition time is 25 days.

4.2 Result Analysis.

In order to measure the effectiveness of this method, the path set is filtered by *viol _ valleyASs* and the *viol _ valleyASs* is used to detect the leakage. The detection results are shown in Table 3, the total number of paths is the total path set, abnormal path number listed in the abnormal path number detected by the algorithm, in parentheses represents the contents of the abnormal path proportion, the proportion of the number of paths for accuracy after verification does exist leak routing:

Table 2 Results of route leaking detection

Data set	Total path number	Unfiltered	accuracy	filter	accuracy
January 1st	1047981	43863(4.19%)	63.31%	34952(3.34%)	79.45%
February 1st	1828820	56531(3.09%)	63,58%	46039(3.01%)	78.07%

The table 2 shows that the contrast filtering algorithm detection result set, detection of leak detection algorithm routing the accurate rate is relatively high, cause analysis, mainly due to the detection method of filtering the path containing domain in the detection, the path of the filter can effectively improve the accuracy of leak routing anomaly detection the results, such as the routing path is 223881940111096, according to the AS results of the identification, the relationship between AS22388 and P2C for AS19401, P2P for the relationship between AS19401 and AS11096, apparently contrary to the "mountain" rules, but after tracking found that this path is effective and correct. The experimental results show that the detection accuracy of the routing leak detection method is higher than 75%, partly because the AS recognition algorithm proposed for AS relationship between the recognition accuracy is relatively high; on the other hand, routing leak detection method proposed in this paper to filter the part containing special domain routing, the autonomous domain due to its intention the establishment, in the path does not comply with the specific "mountain" rules, improve the accuracy of detection results. At the same time, the accuracy of the algorithm is not more than 80%, the main reasons include the following three aspects: ①Some autonomous areas have complex business relationships, and their business relationship cannot be explicitly expressed by P2C, P2P and S2S; ② It is not enough to obtain the complete *viol _ valleyASs* set for the *viol _ valleyASs* domain; ③The result of AS relation recognition needs to be further improved.

Further analysis, the detection of the path of the abnormal path can be divided into the following four categories: ①Type I: p2c-c2p path exists; ②Type II: p2c-p2p path exists;③Type III: p2p-p2c path exists;④Type IV: p2p-c2p path exists. The classification results of the test results are shown in table 3.

Table 3 Three Scheme comparing

Data set	Type I	Type II	Type III	Type IV
January 1st	35.56%	57.55%	1.89%	5.00%
February 1st	43.96%	44.51%	1.41%	10.12%

Table 3 shows that routing leakage two path set exception to type I and type II are analyzed, mainly because the P2C and c2p relations is the main component of AS, in contrast, P2P is relatively small, which is the main reason of type III routing path is relatively less abnormal leakage the. At the same time, this phenomenon indicates that the main reasons causing the path against the "mountain" rule is an autonomous domain from the provider routing after receiving, without any restrictions will spread to the routing of any adjacent domain.

5. Summary

In this paper, we study the method of anomaly detection of routing in inter domain routing system. First of all, this paper introduces the business relationship of autonomous domain, and analyzes the route leakage anomaly, and then proposes a AS relation recognition algorithm based on Forwarding degree, which mainly includes the following three steps: ①Constructing an effective path set;② Analysis of forwarding degree and node degree;③Identification of sibling relationships, provider client relationships and peer relationships. Finally, based on the recognition of the business relationship, put forward a detection method of routing leaks, the algorithm is mainly based on the path of "mountain" rules on the route were analyzed, taking into account the existence of reasonable autonomous domain part does not comply with the rules of the "mountain" in the network, the accuracy of this kind of autonomous domain in filtering to improve the detection results. The experimental results show that the proposed AS algorithm can identify the AS relationship well, and the proposed method is effective and accurate.

References

[1]. YANG B,LU Y L , YANG G Z,et al.Path Forging Detection Approach Based on Aggregation [J].Computer Science, 2014,41(8):158-163. Doi: 10.11896/j.issn.1002-137X.2014.08.035.
[2]. DE Urbina Cazenave I O, KOSLUK E, and GANIZ M C. An anomaly detection framework for bgp[C].Innovations in Intelligent Systems and Applications (INISTA), 2011 International Symposium on. IEEE, Istanbul, Turkey. 2011: 107-111.
[3]. PAPADOPOULOS S, MOUSTAKAS K, and DROSOU A, et al. Border gateway protocol graph: detecting and visualising internet routing anomalies [J]. IET Information Security, 2015. DOI: 10.1049/iet-ifs.2014.0525
[4]. CHEN M, XU M, SONG X, et al. Towards identifying Large-scale BGP Events[C].Local Computer Networks (LCN), 2015 IEEE 40th Conference on. IEEE, 2015: 165-168.
[5]. Gao L. On inferring autonomous system relationships in the Internet [J]. IEEE/ACM Transactions on Networking (ToN), 2001, 9(6): 733-745.
[6]. Giotsas V, Zhou S. Valley-free violation in Internet routing—Analysis based on BGP Community data[C]//2012 IEEE International Conference on Communications (ICC). IEEE, 2012: 1193-1197.
[7]. Giotsas V, Zhou S. Inferring as relationships from bgp attributes[R]. 2011.
[8]. Dickson B. Route Leaks--Definitions [J]. 2012.
[9]. Li S, Zhuge J W, Li X. Study on BGP security [J]. Ruanjian Xuebao/Journal of Software, 2013, 24(1): 121-138.
[10]. Toonk A. How the Internet in Australia went down under [J]. 2012.
[11]. Toonk A. A BGP Leak Made in Canada [J]. 2012.
[12]. LIU X, ZHU P. Analysis of Routing Loops in BGP Table [J]. Computer Engineering, 2005, 14: 025
[13]. Hu X, Mao Z M. Accurate real-time identification of IP prefix hijacking[C]//2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007: 3-17.
[14]. Qiu S Y, McDaniel P D, Monrose F. Toward valley-free inter-domain routing[C]//2007 IEEE International Conference on Communications. IEEE, 2007: 2009-2016.