Evaluating the Topology Coverage of BGP Monitors

Shen Su[1], Zhihong Tian[1], Jing Qiu[1, *], Yu Jiang[1, *], Yanbin Sun[1], Mohan Li[1], Dunqiu Fan[2] and Haining Yu[3]

Abstract: BGP monitors are currently the main data resource of AS-level topology measurement, and the integrity of measurement result is limited to the location of such BGP monitors. However, there is currently no work to conduct a comprehensive study of the range of measurement results for a single BGP monitor. In this paper, we take the first step to describe the observed topology of each BGP monitor. To that end, we first investigate the construction and theoretical up-limit of the measured topology of a BGP monitor based on the valley-free model, then we evaluate the individual parts of the measured topology by comparing such theoretical results with the actually observed data. We find that: 1) for more than 90% of the monitors, the actually observed peer-peer links merely takes a small part of all theoretical visible links; 2) increasing the BGP monitors in the same AS may improve the measurement result, but with limited improvement; and 3) deploying multiple BGP monitors in different ASs can significantly improve the measurement results, but non-local BGP monitors can hardly replace the local AS BGP monitors. We also propose a metric for monitor selection optimization, and prove its effectiveness with experiment evaluation.

Keywords: Autonomous System (AS), border gateway protocol, AS-level topology, visible links.

1 Introduction

The rapid development of the Internet has led to its increased complexity, making its route and traffic behaviors hard to understand. As a complex system, Internet topology is an important foundation for network behavior analysis and modeling. If we depict the Internet as an undirected graph with ASes as the points and the links between the ASes as the edges, the current status is that we have learned the existing ASes on the graph explicitly, but we are not quite sure about the existing links, neither how many links are missing.

A BGP monitor collects the BGP (Border Gateway Protocol) routing table and update

[1] Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, 510006, China.

[2] NSFOCUS Inc., Beijing, 100089, China.

[3] The Department of Computer Science, City University of Hong Kong, Kowloon Tong, Hong Kong.

[*] Corresponding Authors: Jing Qiu. Email: qiugjing@gzhu.edu.cn;
Yu Jiang. Email: jiangyu@gzhu.edu.cn.

packets from the border gateway routers provided by the Internet Service Provider (ISP). To derive a complete topology, we need to increase the number of BGP monitors. However, adding a new BGP monitor requires consultation with the ISP operators and equipment deployment, which is a time consuming and laborious process. Therefore, an in-depth understanding of existing measurement results is particularly important. The current researches on AS-level measurement integrity mainly evaluate the measurement results, but there is no work to evaluate the contribution of a single BGP monitor to the measurement results. Therefore, in this paper, we evaluate the measurement results of a single BGP monitor.

The legal AS paths follows the valley-free model, which is currently recognized as a basic assumption of the BGP routing. Based on this model, we deductively analyze the theoretically observed AS links, and come to the conclusion that an AS links is visible to a BGP monitor, when it is a customer-provider link or a peer-peer link on the provider tree of that BGP monitor (see Section 2 for details). Following this deduction, we are able to estimate the visible up-limit of the topology coverage range of a BGP monitor, which merely includes the visible AS links.

We further compare the range of visible links with the actual measurement results, and use their differences to analyze the measurement integrity of a BGP monitor. Unfortunately, describing the range of visible links requires obtaining ground truth of AS-level topology information, which is difficult to obtain.

The work Ricardo et al. [Ricardo, Pei, Willinger et al. (2010)] founds that when a BGP monitor is placed in an AS, the BGP monitor deployed on it can completely discover its actual AS links, and the existing BGP monitor can almost completely discover the existing customer-provider AS links in the Internet. Based on such two observation experiences, we estimate the lower limit of the actual topology, and then obtain the lower limit of the visible link range of each BGP monitor. The comparison results indicate that the actual measured customer-provider link is very close to the customer-provider links in the visible link range, but the actual measured peer-peer links is much less than the visible link range. We further show that adding BGP monitors within the same AS can improve measurement integrity, but with little help, and adding BGP monitors in different ASes can significantly improve the measurement integrity, but does not guarantee 100% integrity.

The organization structure of this paper is as follows. Section 2 briefly introduces the related works to evaluate AS-level topological integrity. Section 3 states the problem formally. Section 4 discusses the theoretical measurement range of each single BGP monitor. Section 5 compares the theoretical measurement coverage with the de facto topology coverage. Section 6 introduces our monitor selection metric based on the conclusion of the previous sections. Finally, Section 7 concludes the paper.

2 Related works

The Gao [Gao (2001)] proposed that the AS path conforms to the valley-free model, and they classify AS links into three categories according to their business relationships: provider-customer, peer-peer, and sibling-sibling. In a provider-customer relationship, a customer AS needs to pay the provider any traffic between them; in a peer-peer relationship, the two ASs exchange traffic between them free of charge, including traffic between their customers, However, traffic that flows through its provider or peer ASs is not exchanged; in a sibling-sibling relationship, because they belong to the same organization, the two ASs exchange traffic between their providers, customers, peers, or sibling ASes for free. The number of sibling-sibling relationships is very small, so it is generally ignored. An AS path from source to destination conforming to the valley-free model is a directed path consisted of an uphill path, a peer-peer relationship (optional), and a downhill path. Each link of the uphill path is directed from the customer to the provider, and each link of the downhill path is directed from the provider to the customer. Peer-to-peer relationships can only occur between the uphill path and the downhill path. The meaning of valley-free model is that an AS does not pass traffic between its providers or peer relationships. Some ASs in the Internet do not have providers. These ASes are called top-level ASs, and they are peer-to-peer to each other. The subgraphs of such top-level ASes are considered to be the core of the Internet. A list of such ASes is available from [Tier 1 networks (2018)].

During the past decade, some studies have contributed to the study construction of Internet [Tian, Su, Shi et al (2019)] and AS-level topological. Chang et al. [Chang, Govindan and Jamin (2004)] first evaluated the AS-level topological integrity. They compared the BGP data obtained from the BGP monitors with the Internet Routing Registry (IRR) data, and considered that at least the current AS-level topology lost about 25-50% of the links. The work Ricardo et al. [Ricardo, Pei, Willinger et al (2010)] used the routing configuration and system log auxiliary information to compare the gap between the actual topology and the measured topology, and pointed out that 1) the provider-customer link discovery is very complete, and the main loss in the current Internet is Peer-to-peer links; 2) by updating the message, more topology information can be obtained, but there is an upper limit of the accumulated information; 3) when a BGP monitor is cited in an AS, the measured AS-level topology basically include all adjacencies of this AS. He et al. [He, Siganos, Faloutsos et al. (2009)] examines the connection relationship of participants on the Internet exchange point (IXP) and uses traceroute for verification. They found more than 40% new links in the measured topology, with the 300% new found peer-peer links. Rami et al. [Rami and Raz (2006)] also pointed out that the current Internet topology is mainly missing the link of the pee-peer relationship. Enrico et al. [Enrico, Improta, Lenzini et al. (2012)] discussed the optimization of the deployment of Internet topological BGP monitors. One of the basic assumptions of this paper is that a BGP monitor can be completely discovered by its provider's topological relationship. And our experiments prove that this assumption is not always true. In addition, Matthew et al. [Matthew, Tuke and Maennel (2008)] uses the idea of the biological "marker-recapture method" to estimate the Internet topology and predicts that at least 700 BGP monitors are required to obtain the complete topology of the Internet.

3 Problem statements

The AS-level Internet topology is measured by collecting BGP routing tables and update packets on the border router provided by the ISP. These routers are called BGP monitors. Whether it is BGP routing table or update message, it only contains the best route to the target prefix, not all routes. As the network status changes continuously, the BGP routing table changes over time. Therefore, the way to update the packets can increase the integrity of the topology measurement. As shown in Fig. 1, AS 1 has multiple AS paths to the prefixes of “1.0.0.0/24” and “2.0.0.0/24”, and the BGP routing table of AS 1 only contains the best path “1 3 5” and the best path “1 3 6” to the target prefix “2.0.0.0/24”, so the measured topology is only part of the actual topology. When the AS link “1 3” is disconnected for certain reason, the routing table of AS 1 would change. The AS path for the prefix “1.0.0.0/24” turns to be “1 4 5”, and the path towards the prefix “2.0.0.0/24” turns to be “1 2 6”. Therein, by accumulating BGP routing data of AS 1, a more complete AS-level topology can be obtained by using only one BGP routing table.

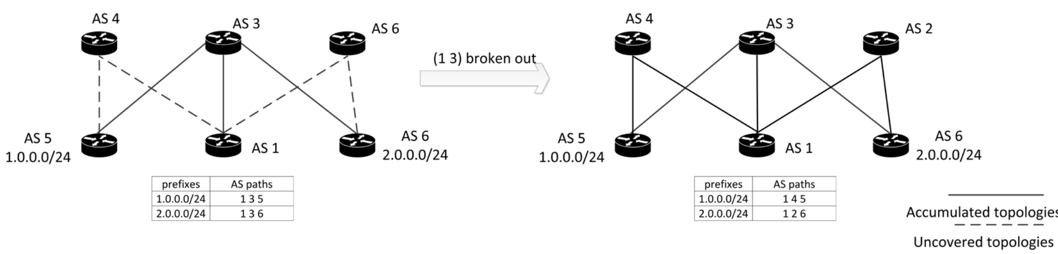

Figure 1: Example of accumulating BGP data for topology measurement

If there is enough BGP data accumulated, then for each BGP monitor, all valley-free AS paths from the AS are visible to the BGP monitor. In this way, the range of AS-level topologies that can be measured by a BGP monitor can be theoretically deducted. However, this theoretical measurement range (denoted as $T(m)$) and the actual measured result (denoted as $A(m)$ may be inconsistent for two reasons:

1) There exists a life cycle for each link, which means $T(m)$ change at real time, but $T(m)$ need to be constant during the accumulation period of $A(m)$. This contradiction leads to the fact that an AS link may never appear in the routing table of m during its lifetime, and it is also possible that measurement result contains the AS link that no longer exist;

2) Although many related studies use the valley-free model as the basic assumption, the complex AS business relationship still would generate the counter-example of the valley-free model, and the accurate inference relies on the accurate AS business relationship inference. If the AS business relationship is erroneous inferred, the measurement result would still be inconsistent with $T(m)$.

In order to predict the measurement result of a BGP monitor more accurately, we evaluate the measurement coverage of a BGP monitor in this paper. Specifically, we hope to answer the questions of what is the measurement coverage of the BGP monitor (i.e., whether $A(m)$ is equal to $T(m)$), or how much the actual measurement result of one BGP monitor is different from the upper limit of the theoretical measurement result.

4 Measurement coverage

In order to facilitate further comparison and analysis, this section first describes the theoretical upper limit (i.e., $T(m)$) of the measurement results of BGP monitors.

4.1 Definition

An AS path from the source point to the destination prefix that conforms to the valley-free model is a directed path consisting of an uphill path, a PP link (optional), and a downhill path. Each link of the uphill path is pointed by the customer. The provider, while each link of the downhill path is directed from the provider to the customer. The P-P link only appears between the uphill path and the downhill path. As shown in Fig. 2, it is an example of an AS-level topology. The path "6→3→1→2→4→5" is an AS path that conforms to the "no bottom" model, "6→3→1". For the uphill path, "2→4→5" is the downhill path (the arrows in Fig. 2 and the AS path have different meanings, the arrows in the path indicate the point from the starting point to the end point, and the arrows in Fig. 2 are used to distinguish the customers. And providers).

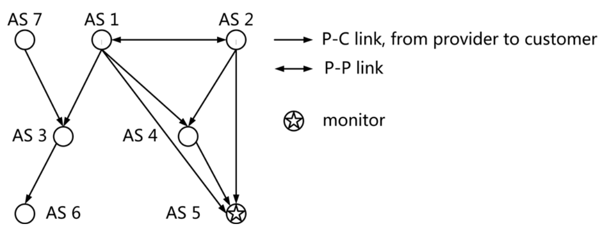

Figure 2: Example of AS topology

Definition 1. For a BGP monitor m, if there is an uphill path from the AS of m to another AS A, AS A is defined as the upstream AS of m; on the contrary, if the path is the downhill path, AS A is defined as the downstream AS of m. The shortest distance of all the uphill paths is defined as the distance from m to AS A. In Fig. 2, the BGP monitor is located at AS 5, and its upstream AS includes AS 1, AS 2, AS 4, and the uphill distance from AS 1 is 1.

Definition 2. The provider tree of the BGP monitor (denoted as $P(m)$) is a collection of all upstream ASs and the ASs in which they are located. In Fig. 2, the provider tree at the BGP monitor of AS 5 is the set {1, 2, 4, 5}.

Definition 3. If a link is on a path that conforms to the valley-free model originating from a BGP monitor, this link is called as the visible link of that BGP monitor. We term the set of all visible links of a BGP monitor as $T(m)$. In Fig. 2, the visible link set of the BGP monitors is {1-2, 1-3, 1-4, 1-5, 2-4, 2-5, 3-6}. Since the AS link 7-3 is not on any of the "no valley paths" originating from AS 5, the link 7-3 is not in the visible link set.

Some ASes are at the core of the Internet and are known as top-level ASes. Such top-level ASes forward traffic for almost all ASes in the Internet, having no providers, and interconnected with each other through P-P links. Except for top-level AS, some non-profit organizations also have no provider ASes. Because the P-C links of such organizations have few P-C links and it is difficult to model them uniformly, we do not consider such P-C links, and assume that all P-C links are on a downhill path originating from a top-level AS. Based on this assumption, it can be inferred that the provider tree of a BGP monitor contains at least one top-level AS.

Theorem 1. A link is the visible link of a BGP monitor, if and only if this link is the P-C link of the P-C link or the provider tree on the provider tree, i.e.,

$$T(m) = CP \cup_{X \in P(m)} PP(X) \quad (1)$$

Here CP represents all C-P link sets, and $PP(X)$ represents all P-P link sets of AS X (X is an AS on m's provider tree).

Proof: We first prove the sufficiency. Assuming that the conclusion is incorrect, there exists a visible link l, which is neither a P-P link on the provider tree of m, nor a C-P link. According to definition 3, l is on a valley-free path originating from m. If l is on the uphill or downhill path, l is a C-P link; if l is a P-P link, one of its endpoint is on the uphill path, i.e., on the provider tree of m.

Then we prove the necessity. For a visible link l, we can construct a valley-free AS path originating from m. If it is a C-P link, according to our assumption, both m and l are on downhill paths originating from a top-level AS, thus there exists a valley-free path traverse l originating from m. If l is a P-P link with one endpoint on m's provider tree, supposing as AS X, there exists an uphill path p from m to X, then "p l" forms a valley-free path originating from m.

Proof done.

2.2 Estimation of topology measurement coverage

The measurement data used in this paper comes from the measurement projects Routeviews and RIPE NCC, which include routing tables and routing update messages on 478 BGP monitors in 339 ASs. Among such monitors, 109 BGP monitors in 77 ASs contain a complete routing table (called full table monitors), and 38 BGP monitors are located in 14 top-level ASs. The data is collected from January 1, 2012 to December 31, 2012. In the rest of this section, we describe how to estimate the theoretical measurement range of a BGP monitor according to the description of Theorem 1. Because of Equation (1), it is necessary to separately estimate all P-C link sets, provider tree of the existing BGP monitors, and P-P link sets of ASes on the provider trees.

1) Estimate of CP:

The work Ricardo et al. [Ricardo, Pei, Willinger et al. (2010)] proposed an algorithm to infer the C-P links according to the BGP data collected by monitors in top-level ASes. Since the AS path observed by the monitors in the top-level AS involves no uphill path, all links should be considered as P-C links except for the first hop. Applying this method, we obtained a total of 110137 P-C links. With no doubt, this method may lead to a certain amount of errors. Generally, such kind of errors is caused by improper BGP configuration leading to the observation of valleyed AS paths.

Fortunately, the BGP misconfiguration always has a short living time, thus could be easily filtered out according to the timestamp of the routing table. In this paper, before we use the collection of BGP routing path for AS business relationship inference, we filter out the AS paths with a lifetime of less than 1 day to reduce the C-P link inference errors (as shown in Algorithm 1). Applying this algorithm, a total of 99, 375 P-C links are obtained, i.e., in order to ensure the accuracy of the inference, about 10% of the P-C links are filtered out. Because the BGP routing table of the top-level AS accumulated over time can cover most P-C links in the AS-level topology of the Internet, we use the P-C link set obtained by Algorithm 1 as the estimation of the P-C link set.

Algorithm 1: The algorithm to infer the set of P-C links

```
Input:  ASpath : AS path set from the top-level ASes;
            usage(p) : living time of AS path p;
Output: CP : P-C link set;
Foreach ( p in ASpath )
  If ( usage(p) >1day)
     Foreach ( l in p )
        If ( l is not first hop of p )
           add l into CP ;
        Endif
     Endfor
  Endif
Endfor
```

2) Estimate of ***P(m)*** **:**

In order to calculate the provider tree of our BGP monitors, we use the P-C link set obtained by Algorithm 1 to perform the depth first searching according to the definition of the provider tree, as shown in Algorithm 2.

Algorithm 2: The algorithm to infer the provider tree of monitor ***m***

```
Input:  CP : P-C link set;
            L : the AS where monitor m is placed;
Output: P(m) : provider tree of monitor m ;
Provider = ∅ ;
Foreach (P-C link (A,B) in CP )
  add A into Provider(B) ;
Endfor
generate_provider_tree ( L );
sub generate_provider_tree ( AS X )
  Foreach (AS Y in Provider(X) )
     If ( Y not in P(m) )
        add Y into P(m) ;
        generate_provider_tree( Y );
```

Endif
Endfor
Endsub

Surprisingly, the provider tree of each BGP monitor according to Algorithm 2 contains the same 2738 ASs, including all 17 top-level ASs and 1,823 ASs connected to the top-level AS. Similar to the problem of the customer cone calculation shown in the work [Matthew, Huffaker, Dhamdhere et al. (2013)], theoretically, the provider tree is quite big. However, a big quantity of observable AS links does not actually exist in the measurement data. Herein, in order to avoid the unrealistic expansion of the provider tree scale, we add an AS to the provider tree of a BGP monitor only when we observe an AS path traverse that AS in the actual BGP data. As shown in Algorithm 3.

Algorithm 3: The improved algorithm to infer the provider tree of monitor *m*

Input: CP : P-C link set;
L : the sited AS of BGP monitor m ;
$ASpath$: AS paths set collected from monitor m ;

Output: $P(m)$: provider-tree AS set of BGP monitor m ;

$Provider = \varnothing$;
Foreach (P-C link (A, B) in CP)
add A into $Provider(B)$;
Endfor
generate_provider_tree (L);
sub generate_provider_tree (AS X)
Foreach (AS Y in $Provider(X)$)
If ($Y \notin P(m)$ && there exists an AS path in $ASpath$ which traverse Y)
add Y into $P(m)$;
generate_provider_tree(Y);
Endif
Endfor
Endsub

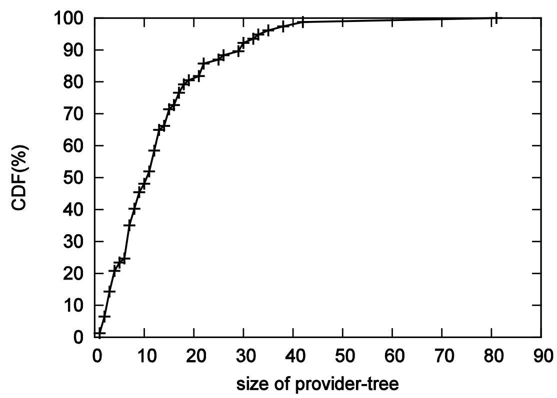

Figure 3: The scale of all monitors' provider tree

As shown in Fig. 3 is the cumulative distribution map of the provider tree size of the monitors calculated according to Algorithm 3. For 97% of the BGP monitors, the provider tree size is smaller than 40. Such provider trees cover 359 ASs, including all top-level ASs and 287 ASs adjacent to the top-level AS.

3) Estimate of *PP(X)*:

It is very difficult to estimate all the P-P links actually connected by an AS. Currently, the relevant research method obtains this information according to the BGP protocol log of an AS. However, the BGP protocol log can only be provided by the ISP provider, which is difficult to obtain. Since if a full routing table BGP monitor is located in certain AS, all its neighboring links of the monitored AS (the AS where the monitor is located) would be observed by accumulating the BGP routing table over time. Therefore, we use the neighboring links of the monitored AS shown in the routing table to estimate the P-P link set of monitored AS.

The AS business relationships can be broadly divided into three categories: P-C links, P-P links, and S-S links. Considering the quantity of S-S links is small, we ignore the links of the S-S type. Considering all P-C links can be estimated according to Algorithm 1, the neighboring links in P-P type of the monitored AS can be estimated by excluding the C-P links from all the neighboring links (as shown in Algorithm 4).

Algorithm 4: The algorithm to infer the P-P links of full monitors

Input: M : the AS set where the BGP monitors are sited;

$ASpath$: AS path set of all monitors;

CP : P-C link set;

Output: $Groundlinks$: P-P links of all ASes in M ;

01 **Foreach** (AS path p in $ASpath$)

02 **Foreach** (AS link (A,B) in path p)

03 **If** ($(A,B) \notin CP$ and $A \in M$)

add (A,B) into $Groundlinks(A)$;
Endif
If ($(A,B) \notin CP$ and $B \in M$)
add (A,B) into $Groundlinks(B)$;
Endif
Endfor
Endfor

4) Estimate of *T(m)*:
The algorithm for estimating $T(m)$ is shown in Algorithm 5. Here $T(m)$ includes all the estimated P-C links (line 1), and the P-P links of the monitored ASes on the provider tree of *m* (line 5-9).

Algorithm 5: The algorithm to infer $T(m)$ for monitor m

Input: M : the AS set where the BGP monitors are located;
$ASpath$: AS path set of all monitors;
Output: $T(m)$: theoretical measurement coverage range of monitor m;
01 Calculate P-C link set of CP ; //According to Alg 1
02 Calculate the provider tree $P(m)$ of monitor m ; //According to Alg 3
03 Calculate the $Groundlinks$ P-P link set of m ; //According to Alg 4
04 $T(m) = CP$;
05 **Foreach** (AS X in $P(m)$)
06 **If** ($X \in M$)
07 $T(m) = T(m) \cup Groundlinks(X)$;
08 **Endif**
09 **Endfor**

Obviously, since only a part of the ASes of *m*'s provider tree is monitored, our estimation of $T(m)$ is only a subset of the ground truth of $T(m)$, and we cannot compare the actual measurement results with the theoretical one directly. However, according to formulas 1, the construction of the visible links (the theoretical measurement result) could be explicitly distinguished, so that we can evaluate the measurement completeness of each part of the visible links separately.

5 Comparison of de facto BGP monitor coverage

In order to evaluate the actual measurement capability of the BGP monitors, this section compares the actual measurement results of the BGP monitors with the visible links estimated by Algorithm 5, and discusses the measurement coverage of the different parts of the visible links. Considering the de facto measurement usually involves multiple monitors to improve measurement coverage of the topology, we also combine the measurement results of multiple BGP monitors in the same AS, and multiple BGP monitors in different ASes to represent the de facto measurement results.

For BGP monitors that only have partial routing tables, the measurement coverage is mainly limited by the measurement project itself, not the location of the BGP monitors. This is not the topic we want to discuss, and we just focus on the full routing table BGP monitors.

5.1 Single monitor

First, we compare the measurement results of a single BGP monitor with the estimated visible links of that monitor. As discussed in Section 4, we need to compare the de facto measurement results with the visible links on aspects of P-C link and P-P link separately. As shown in Fig. 4 is the cumulative distribution of the coverage of the BGP monitors of all the full routing tables. The curve "c2p" represents the coverage of the P-C link, and the curve "p2p" represents the coverage of the P-P link. Here coverage refers to the size of observed AS link set (P-C link set or P-P link set) over the size of visible link set (P-C link set or P-P link set).

As observed in the figure, the P-C link coverage of most full-table BGP monitors exceeds 90%. Considering that we only exclude about 10% of all the P-C links during the estimation of *CP*, we may safely draw the conclusion that a BGP monitor can almost cover all the P-C links. However, for more than 90% of all the BGP monitors, the coverage of P-P links is small than 30%; and the highest coverage is only about 56%. Considering that the visible links estimated in this paper is only a subset of the actual visible links, one BGP monitor has a low P-P link coverage on its provider tree.

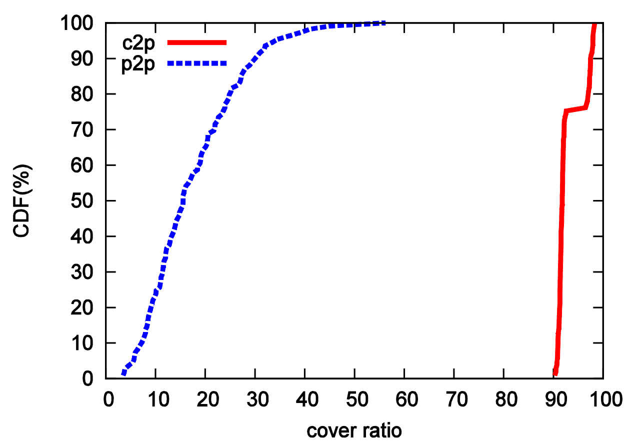

Figure 4: Cover ratio of the visible links from a single monitor

5.2 Multiple monitors in the same AS

Routing diversity is an important factor for BGP, because the routing tables of different BGP routers in the same AS may be inconsistent. Therefore, adding BGP monitors in the same AS may help collect different AS routes to increase the actual measurement result. In this section, we compare whether the sum of the measurement results of multiple BGP monitors in the same AS can cover the theoretical visible links of these BGP monitors (obviously, the theoretical visible links of different BGP monitors in the same AS are the same).

Since the coverage of the P-C link for a single BGP monitor is very high, next we only compare the coverage of the visible P-P links. As shown in Fig. 5, the curve "multiple monitors" represents the cumulative distribution of P-P link coverage (de facto measurement result over visible links) for the case of multiple BGP monitors in the same AS, and the curve "single monitor" represents the P-P link coverage when we random select only one monitor as the de facto measurement results.

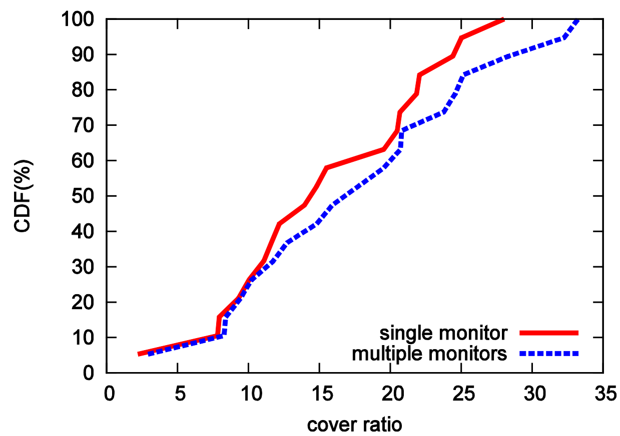

Figure 5: Cover ratio of the visible links from multiple vantage points in the same AS

Obviously, adding BGP monitors in the same AS also does not guarantee the measurement coverage of the P-P links. In Fig. 5, the P-P link coverage for multiple BGP monitors is only 33%. The difference between the multiple BGP monitors and single monitors in this paper is no bigger than 5%. Therefore, we believe that adding BGP monitors in the same AS has a slight improvement in measurement coverage, but it has little effect.

The above analysis can answer the question raised in Section 3, that is, the actual measurement of a BGP monitor can cover most of the P-C link, but only cover a part of the P-P link within its theoretical measurement range. Considering that an AS path contains at most one P-P link, the absence of more than 67% of the P-P link means that for a BGP monitor, most of the valley-free AS paths originating from the monitored AS are not collected. To sum up, the actual measurable range of a BGP monitor can be described as:

$$CP \cup PP(L) < A(m) \ll CP \cup_{X \in P(m)} PP(X) \quad (2)$$

Here L refers to the AS where the BGP monitor is located.

5.3 Multiple monitors in multiple ASes

If the estimation of the measurement range of the BGP monitor only considers the lower limit of the formula (2), it would be difficult to implement a BGP monitor on each AS in order to obtain a complete AS-level Internet topology. Herein, it is worthy to discuss that how to achieve a complete view of an unmonitored AS. Considering that the actual measurement of a BGP monitor can cover a part of the P-P links of one upstream ASes, a question worth answering is that: Combining the actual measurement results of multiple BGP monitors, whether a mutual upstream AS's P-P links of such BGP monitors could be completely obtained?

As shown in Fig. 6 is the coverage of the P-P links of a mutual upstream AS measured for multiple BGP monitors. The X-axis indicates the quantity of BGP monitors in the downstream AS, and the y-axis indicates the coverage of the measurement results of the P-P links. As observed, the P-P links of most ASes can be completely covered by the BGP monitors on its downstream AS. However, there exist some special cases with dozens of BGP monitors in the downstream AS of some ASes and low P-P links coverage (less than 40%). Generally speaking, the BGP monitors on the downstream ASes are able to catch a complete view of the upstream AS, but cannot guarantee a complete coverage of all the P-P links.

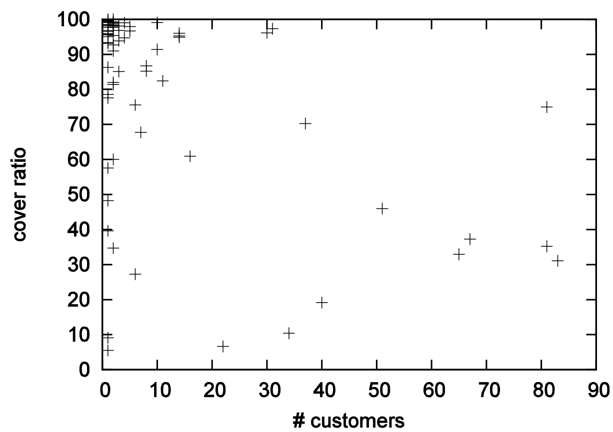

Figure 6: Cover ratio of upstream P-P links from multiple monitors

6 Monitor deployment optimization metric

In order to optimize the BGP monitor deployment, we propose a metric for BGP monitor deployment which aims at maximizing BGP monitor measurement coverage.

Generally, our idea is to propose a metric to quantitatively evaluate the potential gains of a BGP monitor. Since the c2p links are quite completely covered by the existing BGP monitors, we focus on the potential gains of the p2p links, and the metric considers the c2p links of each monitor. Since the customer routes have higher route priority than the peering routes, and the peering routes have higher route priority the provider routes, we believe that a monitor would discover more p2p links when it has fewer customer ASes, and would has more chance to discover p2p links closer to it. Herein, our proposed metric is as Eq. (3):

$$C_0 + \alpha_1 \overline{C_1} + \alpha_2 \overline{C_2} \tag{3}$$

Here, C_0 refers to the quantity of customer ASes of the monitor, $\overline{C_1} = \frac{1}{|P_1|} \sum_{x \in P_1} C_x$, $\overline{C_2} = \frac{1}{|P_2|} \sum_{y \in P_2} C_y$, and C_x refers to the customer ASes of AS x (P_1 is set of provider AS of the monitor, similar for $\overline{C_2}$). α_1 and α_2 are configurable parameters.

To apply the proposed metric for monitor selection, we calculate the metric value for each monitor, and rank the monitors according to the metric value from low to high. In the following, we evaluate the proposed metric based on the dataset we used in this paper. To that end, we select a number of monitors according to our metric and compare the measure results with the rest monitors to see how many more p2p links could be observed. As shown in Fig. 7 is the measurement results of different quantity of selected monitors. The x axis represents the quantity of selected monitors, and y axis represents the quantity of discovered p2p links. In our method, α_1 is set as 0.01 and α_2 is set as 0.001. For comparison, we apply the method proposed in Enrico et al. [Enrico, Improta, Lenzini et al. (2012)] to our experiments (curve "covering ASes d=1" and curve "covering ASes d=2"), and conduct random selection (curve "random"). Here "covering ASes d=1" refers to that we only consider the ASes with one-hop downhill distance.

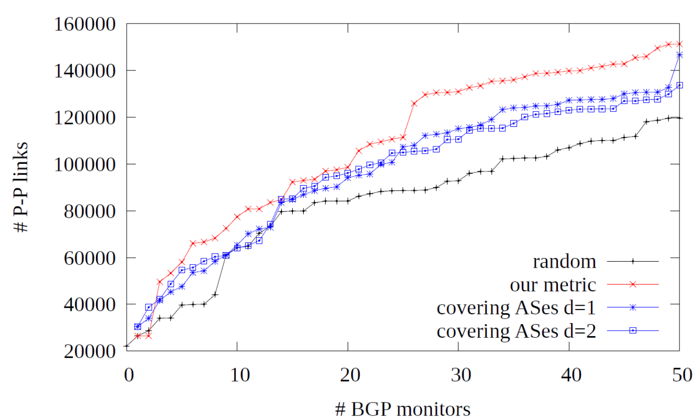

Figure 7: Comparison on # measured P-P links

According to Fig. 7, the random selection performs worst, and our method outperforms the rest methods. When we select more than 3 monitors, we can achieve 11% more p2p links and the work proposed in work [Enrico, Improta, Lenzini et al. (2012)], and achieve 30% more p2p links than the random selection.

7 Conclusion

In this paper, we propose the concept of "visible link" to represent the theoretical measurement result of a BGP monitor and prove that the "visible link" includes all P-C links and P-P links on the provider tree. With experimental comparisons, we found that the actual measurement results for a single BGP monitor include almost all P-C links in the visible links, but no more than 30% of the P-P links on the provider tree. Adding BGP monitors to the same AS can improve the measurement results, but with little help. Deploying multiple BGP monitors in different ASs can significantly improve the measurement results, but non-local BGP monitors cannot completely replace the local AS BGP monitors. We also propose an evaluation metric more monitor selection, and our evaluation proved that our metric outperforms the other existing methods.

Acknowledgement: This work was supported in part by the Guangdong Province Key Research and Development Plan (Grant No. 2019B010137004) and the National Key research and Development Plan (Grant No. 2018YFB0803504).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Chang, H.; Ramesh, G.; Sugih, J.; Scott, J.; Walter, W. (2004): Towards capturing representative as-level internet topologies. *Computer Networks*, vol. 44, no. 6, pp. 737-755.

Chen, J.; Tian, Z.; Cui, X.; Yin, L.; Wang, X. (2018): Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence & Humanized Computing*, vol. 2, no. 1, pp. 1-9.

Cohen, R.; Danny, R. (2006): The internet dark matter-on the missing links in the as connectivity map. *IEEE International Conference on Computer Communications*, pp. 1-12.

Du, X.; Chen, H. H. (2008): Security in wireless sensor networks. *IEEE Wireless Communications Magazine*, vol. 15, no. 4, pp. 60-66.

Gao, L. (2001): On inferring autonomous system relationships in the Internet. *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 733-745.

Gregori, E.; Alessandro, I.; Luciano, L.; Lorenzo, R.; Luca, S. (2012): On the incompleteness of the as-level graph: a novel methodology for BGP route collector placement. *Proceedings of the 2012 Internet Measurement Conference*, pp. 253-264.

Govindan, R.; Anoop, R. (1997): An analysis of internet inter-domain topology and route stability. *International Conference on Computer Communications*, vol. 2, pp. 850-857.

He, Y.; Georgos, S.; Michalis, F.; Srikanth, K. (2009): Lord of the links: a framework for discovering missing links in the internet topology. *IEEE/ACM Transactions on Networking*, vol. 17, no. 2, pp. 391-404.

Luckie, M.; Bradley, H.; Amogh, D.; Vasileios, G. (2013): AS relationships, customer cones, and validation. *Proceedings of the 2013 conference on Internet Measurement Conference*, pp. 243-256.

Oliveira, R.; Dan, P.; Walter, W.; Zhang, B.; Zhang, L. (2010): The (in) completeness of the observed internet as-level structure. *IEEE/ACM Transactions on Networking*, vol. 18, no. 1, pp. 109-122.

Qiu, J.; Chai, Y.; Liu, Y.; Gu, Z.; Li, S. et al. (2018): Automatic non-taxonomic relation extraction from big data in smart city. *IEEE Access*, vol. 6, pp. 74854-74864.

Roughan, M.; Simon, J.; Olaf, M. (2008): Bigfoot, sasquatch, the yeti and other missing links: what we don't know about the as graph. *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement*, pp. 325-330.

Su, S.; Sun, Y.; Gao, X.; Qiu, J.; Tian, Z. (2019): A correlation-change based feature selection method for IoT equipment anomaly detection. *Applied Sciences*, vol. 9, no. 3, pp. 437-450.

Tian, Z.; Su, S.; Shi, W.; Du, X.; Guizani, M. et al. (2019): A data-driven method for future internet route decision modeling. *Future Generation Computer Systems*, vol. 95, pp. 212-220.

Tian, Z.; Cui, Y.; An, L.; Su, S.; Yin, X. et al. (2018): A real-time correlation of host-level events in cyber range service for smart campus. *IEEE Access*, vol. 6, pp. 35355-35364.

Tian, Z.; Shi, W.; Wang, Y.; Zhu, C.; Du, X. et al. (2019): Real time lateral movement detection based on evidence reasoning network for edge computing environment. *IEEE Transactions on Industrial Informatics*, vol. 15 no.7, pp. 4285-4294.

Tier 1 networks. (2018): http://en.wikipedia.org/wiki/Tier_1_network/.

Tier 1 networks. (2018): http://en.wikipedia.org/wiki/Tier_1_network/.

Tan, Q.; Gao, Y.; Shi, J.; Wang, X.; Fang, B. et al. (2018): Towards a comprehensive insight into the eclipse attacks of Tor hidden services. *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1584-1593.

Wang, Y.; Tian, Z.; Zhang, H.; Su S.; Shi, W. (2018): A privacy preserving scheme for nearest neighbor query. *Sensors*, vol. 18, no. 8, pp. 2440-2453.

Xiao, Y.; Du, X.; Zhang, J.; Guizani, S. (2007): Internet protocol television (IPTV): the killer application for the next generation internet, *IEEE Communications Magazine*, vol. 45, no. 11, pp. 126-134.

Yu, Z.; Ricardo, O.; Wang, Y.; Su, S.; Zhang, B. et al. (2011): A framework to quantify the pitfalls of using traceroute in as-level topology measurement. *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, pp. 1822-1836.