

Improved Calculation of AS Resilience Against IP Prefix Hijacking

Matthias Wübbeling

Fraunhofer FKIE & University of Bonn
Friedrich-Ebert-Allee 144, D-53113 Bonn
Email: wueb@cs.uni-bonn.de

Michael Meier

Fraunhofer FKIE & University of Bonn
Friedrich-Ebert-Allee 144, D-53113 Bonn
Email: mm@cs.uni-bonn.de

Abstract—Network prefix hijacking is still a serious threat in the Internet. Confirmed incidents in the recent past have shown that even small autonomous systems (ASs) are able to manipulate routing information with huge global impact. Even though countermeasures exist, they are not established at large scale yet. Monitoring of the actual routing state is the only mean to provide at least information about prefix hijacking events for single ASs. Given topology information the resilience of an AS against prefix hijacking attacks can be determined.

This paper proposes an improved formula to calculate the resilience of an AS against prefix hijacking. Additionally, the role of internet exchange points (IXPs) and the peering opportunities they provide are evaluated. Such opportunities allow for establishing links between ASs at very low cost. Current peering opportunities are derived from a collection of member data gathered from European IXPs.

Furthermore, the effect of additional links on an AS's resilience is investigated by combining actual peering and individual peering opportunities.

I. INTRODUCTION

Claiming ownership of another Autonomous System's IP address space in the Internet is called network prefix hijacking (or prefix hijacking). It leads to connectivity problems for the legitimate owner and its communication partners. Intentionally, an attacker can impersonate parts of another Autonomous System (AS) to redirect traffic to its own domain.

Prefix hijacking is a present threat in Internet routing. Recent revelations indicate that not only intelligence agencies [22] but also small companies [19] are able to hijack prefixes intentionally. Mutual trust between ASs, as assumed by design of the de-facto standard inter-AS routing protocol Border Gateway Protocol (BGP), is a major shortcoming. Comprising more than 50.000 ASs nowadays, the Internet massively grew since its early days. Accordingly, assuming trust between participating ASs is a vulnerable concept nowadays. While other application protocols e.g. HTTP, SMTP or TELNET were updated successively or exchanged, BGP did not experience an update focusing authentication or validation of routing information. Even though mature developments provide means to improve the security of Internet routing, there is no such solution in place yet. Resource Public Key Infrastructure (RPKI), which is the most promising solution, is not widely used but only deployed at levels of 0.6% and about 12% depending on the Internet region [12]. Effectively, ASs have rather small chance to protect their prefixes against hijacking. Therefore,

it is vital to further understand causes, effects and mitigation of prefix hijacking.

The causes of prefix hijacking are well known and twofold. Inadvertent misconfiguration of border routers on the one hand and intended attacks by malicious ASs on the other hand can lead to such events [26]. In contrast, effects and mitigation opportunities are not yet well researched. Regarding the aftereffects of prefix hijacking, e.g. resulting partitioning of the Internet with respect to the prefix in question, the individual resilience of an AS against prefix hijacking, as proposed by Lad et al. [11], could be used as an indicator of an attacker's potential success. Unfortunately, the proposed formula by Lad et al. leads to wrong results as it does not reflect the nature of BGP. Generally, the interconnectedness of an AS seems to have an influence on its individual level of resilience against prefix hijacking. Establishing further links to other ASs might improve an AS's resilience accordingly. To be cost-efficient, AS links are preferable if both ASs are already connected to the same IXP.

The work presented in this paper makes three key contributions:

- 1) The existing formula to calculate prefix resilience is revised due to an error leading to wrong results. Exemplary, a simple AS peering setup is discussed to demonstrate the calculation error.
- 2) An improved formula is presented and used to calculate the resilience for ASs currently active in the Internet. In order to provide comparability of the results of the previous and the newly proposed formula, prefix hijacking is simulated with each formula.
- 3) The proposed formula is used to gain insights about the role of Internet exchange points with respect to the resilience value of ASs.

The remainder of this paper is organized as follows. Section II introduces Internet routing and prefix hijacking as an example for routing anomalies. Section III presents related work including related methods and metrics. The methodology used in this paper as well as the proposed formula to compute prefix hijacking is presented in Section IV. The current resilience of ASs connected to the Internet and the influence of additional AS links at IXPs are discussed in Section V. The final Section VI concludes the paper and points out future work.

II. INTERNET ROUTING AND ROUTING ANOMALIES

This section provides relevant background on Internet routing and routing anomalies that regularly happen in the Internet.

A. Internet routing

Autonomous Systems get IP addresses allocated by regional internet registries. Following the Classless Inter Domain Routing (CIDR) notation, IP addresses allocated to ASs are organized in subnets. Each subnet contains IP addresses sharing the same prefix with a specific prefix length. If prefixes overlap, the most specific one (i.e. the longest prefix) is selected within the routing decision process. To provide access to and from the Internet, prefixes of an AS are publicly announced to other ASs via BGP.

Routing announcements, contain at least one prefix and the AS path to the originating AS (also called the prefix owner AS). They are spread through the Internet following a simple forwarding algorithm. ASs choose a preferable path from all incoming announcements for each prefix. The chosen AS path is extended with the own AS number and is then forwarded to all neighbor ASs, which are not already contained in the path, according to individual peering policies.

Links between ASs can be classified with respect to the business relationship between them. Provider ASs are well connected to many parts of the Internet. Therefore, they are able to provide access to the rest of the Internet, namely ASs that a customer AS itself is not directly connected to. Accordingly, there are three different roles that define the relationship between ASs: customer, provider, peer. While a provider is generally paid for each packet passing the link from or to a customer, traffic exchange with peers is not as expensive or free of charge. It is assumed, that announcements are forwarded with respect to the AS-link classification. Routing policies can be used to implement further rules of how traffic (besides the routing information itself) is forwarded.

Internet exchange points are facilities providing services to establish AS-links. Instead of individual peering between two ASs, which at least requires an appropriately close location, IXPs allow an AS to peer with ASs that are also located at the same IXP. Even if the datacenters of an IXP are geographically distributed, peering is still possible and handled by the IXP backbone network. Usually, the cost of maintaining an IXP link is lower than establishing numerous individual peerings at different locations.

B. Routing anomalies

According to Lad et al. [10] and Qiu et al. [15], a routing announcement is considered an anomaly, if at least one of the following conditions is met:

- 1) An invalid (e.g. reserved or private) AS number is used.
- 2) One or more invalid or reserved prefixes are used.
- 3) The prefix is not owned by the originating AS.
- 4) The same prefix is originated (announced) by two or more ASs.
- 5) The given AS path has no physical equivalent.

- 6) The provided AS path does not match common routing decisions.

Condition 3 and 4 are relevant to prefix hijacking as discussed in this work. Based on condition 4, which also implies condition 3, the term Multiple Origin AS (MOAS) is derived [26]. MOAS describes that two or more ASs originate the same prefix at the same time. Even though the term MOAS conflict indicate a conflict between ASs, the conflict might be set up intentionally, e.g. legitimate MOAS conflicts are set up to realize load balancing between root DNS servers. MOAS also appear if two or more multihoming providers announce the same prefix on behalf of a legitimate owner. In this case, the Internet will be partitioned with respect to the prefix in question. One partition includes the ASs selecting the true, the other partition includes the ASs being deceived by the false origin. In case of more than two origin ASs, the number of partitions increases accordingly.

Prefix hijacking in this work is more specific and consequently a subset of MOAS events. It describes MOAS events where an AS illegitimately announces the prefix owned by another AS. In order to detect prefix hijacking, we assume that the legitimate origin announces the prefix at the same time.

If the legitimate owner, which is the one legitimately holding the prefix, recognizes the hijacking, it has literally no countermeasure that is appropriate to thwart it. Even though it is possible, to announce longer prefixes than the causing AS, which then circumvents the partitioning, an attacker may also lengthen the announced prefix. This game stops at a 24 bits prefix, as longer prefixes are not commonly routed. Thus, the conflict remains unsolved.

III. RELATED WORK

Routing anomalies caused by the BGP shortcomings described above have already been investigated in previous work [14], [27]. Several security related extensions and replacements of BGP have been developed and evaluated [9], [21], [13], [1], [4]; however, none of these proposals have been deployed at large scale. Approaches have been made to detect prefix hijacking [8], [17] based on publicly available routing information. Prefix hijack alert systems for prefix owners are not only academic [10]. Their relevance is demonstrated by commercially available [3], [18] products. A reactive approach promises effective mitigation of prefix hijacking based on cooperation between ASs [25] while other approaches have built overlays to secure communication [7], [20]. Due to the large amount of MOAS conflicts, classification of them allows to distinguish between legitimate and illegitimate routing announcements [8] in advance to further analysis. Causes of MOAS conflicts as directly related to prefix hijacking and their appearance and durations have been studied by Zhao et al. [26]. While related work mainly focus on the legitimate owner of a prefix as victim, it is necessary to consider all ASs victim of prefix hijacking[23].

With respect to the resilience of ASs against prefix hijacking, Lad et al. [11] proposed a formula meant to calculate the

impact of an AS being a prefix hijacker. Their work is cited regularly in academic publications. Unfortunately, the method proposed by Lad et al. is just an approximation of an AS's resilience against prefix hijacking. The method has one serious shortcoming: it does not reflect the nature of BGP being a path vector protocol and consequently it does not take into account the route selection of predecessors on the path and therefore calculates imprecise values, as exemplified in Section IV. At this point, the function should be recapitulated.

Lad et al. [11] propose the β function (1) to calculate the impact I of an AS with respect to one victim AS (the true origin) and one AS that is deceived about the true origin.

$$\beta(a, t, v) = \begin{cases} 1, & \text{if node } v \text{ is deceived by false origin} \\ a & \text{for true origin } t\text{'s prefix} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

They also show that impact I of an AS is equal to its resilience R . This seems reasonable so far, as only the role of true and false origin have to be changed between competing ASs. We prefer the term resilience, as it reflects the defensive focus of this work. If paths share the same length to the true origin as well as to the attacker, the simple β function is no longer suitable, as it does not reflect randomly chosen announcements. The $\bar{\beta}$ function (2), returns the likelihood to choose one of the paths randomly with " $p(v, n)$ being the number of equally preferred paths [...] from the node v to node n " [11].

$$\bar{\beta}(a, t, v) = \frac{p(v, a)}{p(v, a) + p(v, t)} \quad (2)$$

The value of the resilience against prefix hijacking is a simple equation: the number of paths to the true origin and the number of paths to the false origin are each divided by the total number of paths. The sum of all values is divided by the number of ASs to get the final value for the resilience R of an AS, as shown in the resilience function (3).

$$R(t) = \sum_{a \in N} \sum_{v \in N} \frac{\bar{\beta}(t, a, v)}{(N-1)(N-2)} \quad (3)$$

Lad et al. consider the $\bar{\beta}$ function as a likelihood function of the selection process.

To the best of the authors' knowledge, no investigation of the influence of additional peerings, based on real peering opportunities provided by IXPs, on the resilience of an AS against prefix hijacking has been published yet. Membership information reflecting the peering opportunities of IXPs is collected as described in the authors' previous work [24].

IV. ASSESSING THE RESILIENCE OF AUTONOMOUS SYSTEMS AGAINST PREFIX HIJACKING ATTACKS

In order to assess the resilience of AS against prefix hijacking respective routing states are simulated. This section provides an overview of the methodology used in experiments and evaluation of this work. The setup and prerequisites

Table I: AS levels (hop distance from an AS to a Tier 1 AS).

Level	0	1	2	3	4	5
# ASs	22	15,882	29,488	5,842	335	61
% of ASs	0.04	30.80	57.18	11.33	0.65	0.12

Table II: Attacker AS levels.

Level	1	2	3	4	sum
Num. of attackers	31	56	11	2	100

of the simulation system are described in detail. Following, the shortcomings of the existing formula to calculate prefix hijacking resistance are presented and a modified formula is introduced that is proven to provide more accurate results.

A. Prerequisites

The simulation is based on three different data sets that are publicly available: routing data containing BGP announcements observed by different Route Reflector Clients (RRCs) that is provided by the RIPE Routing Information System (RIPE RIS) [16], AS link classification computed by CAIDA [5] and IXP membership information included from the authors' BGP Anomaly Research Toolkit (BART) [2].

We used RIPE RIS archives dating back to February 1st, 2015 08:00 retrieved for RRCs {00, 01, 03, 04, 05, 06, 07, 10, 11, 12, 13, 14, 15}. The data is then enriched with the CAIDA relationship listing labeled with "20150201", which holds data gathered throughout January 2015, according to the website. If relationships are listed for unknown AS links, these AS links are assumed to be valid and also added to the simulation.

As mentioned in Section II, the Internet is typically divided into Tier 1, 2 and 3 ASs. For the sake of clarity this (informal) hierarchy should be replaced by a more topological one. For the remainder of this paper, ASs are associated to levels. These levels represent the depth of an AS in relation to the top tier ASs that are classified as level 0 ASs. The set of top tier ASs is rather equal to the set of Tier 1 ASs of the informal hierarchy: it is the clique of ASs not needing a provider to reach any other AS. In addition, alias AS numbers of the Tier 1 ASs are added to the set. This is necessary to compute the correct hierarchy, as alias AS numbers are equally used in AS paths, which would lead to strange results and circles. For the simulation the corresponding hierarchy contains 6 AS levels in total, as shown in Table I. Additionally, the simulation of path distribution follows the well-known valley-free paradigm [6].

In order to get comparable results over several runs, the set of 100 attacker ASs for the simulation is chosen in advance. They have been randomly selected so that their distribution is representative, as shown in Table II. Each of the attackers hijacks one prefix of each of all other ASs per simulation run.

B. Weakness of existing formula

As described in Section III, Lad et al. proposed a formula to calculate prefix hijacking resilience [11]. The resulting likelihood approximately reflects AS peering but is not as

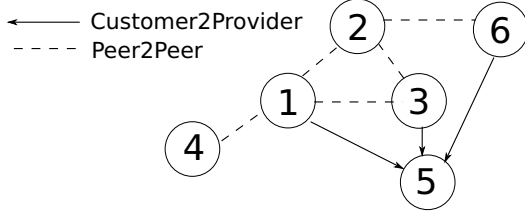


Figure 1: Example AS peering graph.

Table III: Resilience value calculated with the formula by Lad et al.

$a \in AS$	1	2	3	4	5	6
$R(a)$	0.65	0.4875	0.425	0.1375	0.65	0.3

accurate as possible. Practically, it does not reflect the path vector element of BGP. Routing decisions made by predecessors in the distribution path of a routing announcement are not considered appropriately. In the evaluation by Lad et al. each possible path is assumed to reach an AS. A realistic scenario must take the route decision process of preceding ASs into account. As there is no ground truth available to provide evidence, the following paragraphs argue about the shortcomings. Figure 1 sketches a graph supporting the discussion.

Applying the formula proposed by Lad et al. the resilience values will be calculated as shown in table III. When investigating the route distribution, the value of AS 2 seems conspicuous. To demonstrate the problem, some values should be calculated by hand for true origin AS 2, false origin AS 4 and currently considered deceived AS 5.

Three shortest paths lead from AS 5 to the true origin AS 2. Only one shortest path leads to AS 4, the false origin. Calculating Lad et al.'s $\bar{\beta}$ function results in $\frac{3}{4}$ as the likelihood to choose a path to AS 2 and $\frac{1}{4}$ to choose a path to AS 4.

With respect to routing dynamics, this result looks odd. The path actually being chosen from AS 1 is the only path forwarded to AS 5. This means, AS 1 decides which path might be received by AS 5 from this direction. Regarding the unquestioned paths via AS 3 and AS 6, both of them are directly forwarded to AS 5, leading to the true origin. Next, the likelihood for AS 5 to be deceived by AS 4 has to be calculated with respect to the selection of AS 1. As AS 1 is directly connected to both origins, the likelihood to select one of them is $\frac{1}{2}$ each. As a result, AS 5 receives 3 announcements, leading to the true origin AS 2 with a likelihood of $\frac{1}{2} \times \frac{1}{3} + \frac{2}{3} = \frac{5}{6}$. The likelihood to be deceived by AS 4 is $\frac{1}{2} \times \frac{1}{3} = \frac{1}{6}$. Compared to the values calculated by the $\bar{\beta}$ function, the difference between both values is 0.0833 which is an error of more than 8%. Finally, the error for the given topology shown is 0.8% in total.

Furthermore, the notation of sets used by Lad et al. is ambiguous. Utilized sets are not clearly defined, which hinders easy comprehension.

Table IV: Resilience value calculated with the improved formula.

$a \in AS$	1	2	3	4	5	6
$R(a)$	0.65	0.4917	0.425	0.1333	0.65	0.3

C. Improvement of resilience calculation

As presented, the existing formula to calculate prefix hijacking resilience does not comprehensively reflect all possible AS topologies. To provide more accurate results, it is necessary to take the routing decisions of peering ASs into account. Therefore, a new function to calculate an AS's resilience is proposed.

Beforehand, $\beta(t, a, n)$, indicating the likelihood for AS n selecting the route to the true origin t instead of the false origin a is redefined (4). It is worth noting, that in contrast to the formula given by Lad et al.[11] the definitions of the sets V , A and P are necessary to prevent ambiguity: V , the set of all ASs (vertices). $A = V \setminus \{t\}$, the set of all possible attackers for a given true origin $t \in V$. $N = V \setminus \{t, a\}$, the remainder of V for chosen origin $t \in V$ and attacker $a \in A$. $P_{(t,a,n)}$, the set of connected ASs providing shortest paths to the origins $t \in V$ or $a \in A$ to $n \in N$.

$$\beta(t, a, n) = \begin{cases} 0 & , \text{ if Case 1} \\ \frac{1}{|P_{(t,a,n)}|} & , \text{ if Case 2} \\ \sum_{p \in P_{(t,a,n)}} \frac{1}{|P_{(t,a,n)}|} \times \beta(t, a, p) & , \text{ if Case 3} \end{cases}$$

Case 1: t is not, but a is directly connected to n .
Case 2: t is and a might be directly connected to n .
Case 3: both, t and a are not directly connected to n . (4)

Based on the more accurate calculation of path distribution, the new resilience formula is proposed (5). With respect to the exemplary used network (Figure 1), the resilience values are calculated as in Table IV.

$$R(t) = \sum_{a \in A} \sum_{n \in N} \frac{\beta(t, a, n)}{|A| \times |N|} \quad (5)$$

V. PREFIX HIJACKING AND THE ROLE OF IXPS

Before examining the peering opportunities provided by IXPs, it is necessary to consider the current situation of MOAS conflicts. Furthermore, the current resilience against prefix hijacking is calculated using Lad's traditional formula as well as the formula newly presented in this work to illustrate the different results. Finally, the establishment of AS links at IXPs is evaluated. The latter results have been calculated with the resilience formula proposed in Section IV.

A. Multiple Origin AS

MOAS conflicts are a common phenomenon in Internet routing. The data sets used for evaluation also contain MOAS conflicts between several ASs. Actually, 7,149 prefixes are affected by conflicts with 1,983 involved ASs. The number of

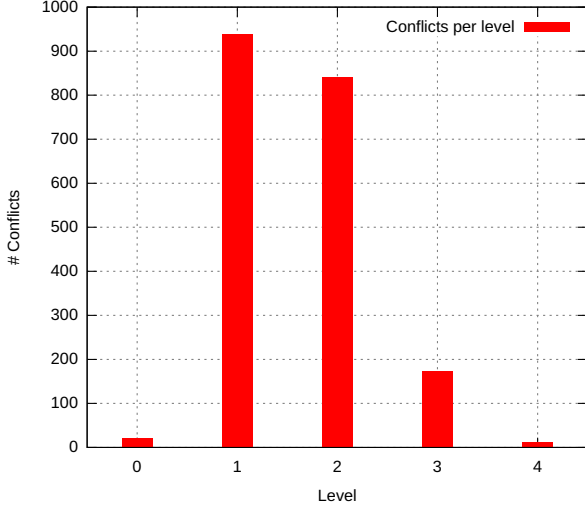


Figure 2: ASs involved in MOAS conflicts by their topological position.

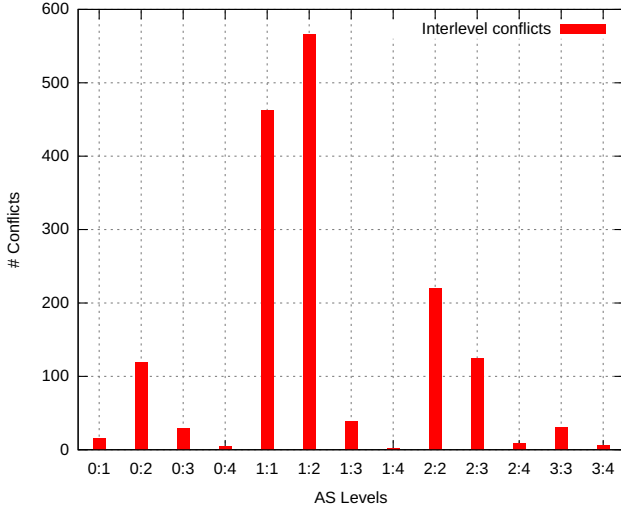


Figure 3: Number of MOAS conflicts between ASs in different levels.

ASs involved in MOAS conflicts for each level, as described in Section IV, is shown in Figure 2.

Accordingly, topological positions (as indicated by the given levels) between rival ASs are presented in Figure 3.

Most conflicts appear between ASs of Level 1 and Level 2, directly followed by the number of conflicts between ASs within Level 1. The difference of prefix hijacking resilience between competing ASs in level 1, is computed with the new formula solely (Figure 4).

Most of the conflicts exist between ASs having a similar resilience, i.e. within a range of 0.2. This might be a hint of the reasons for such a situation. For load balancing, ASs with rather equal resilience should cooperate. This would lead

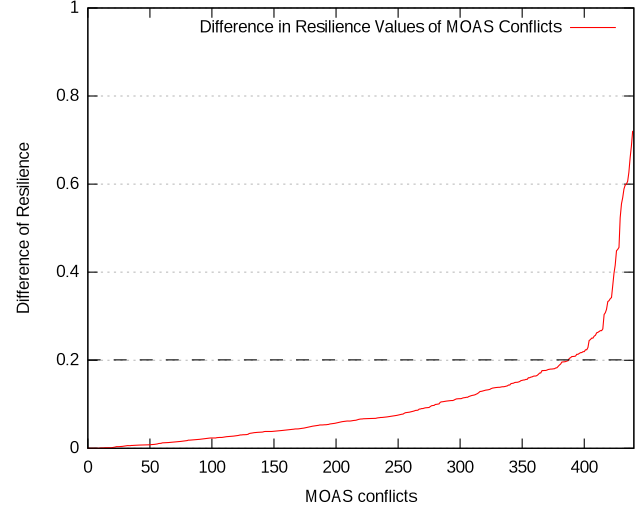


Figure 4: Resilience difference between competing ASs.

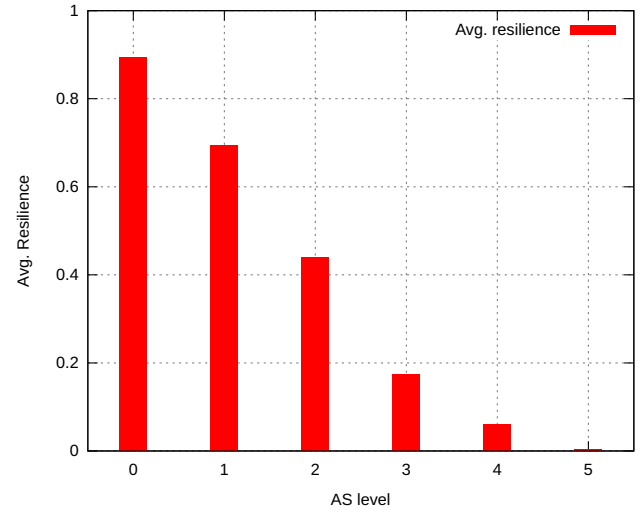


Figure 5: Average resilience per AS level.

to partitions that are equal in size (in terms of the number of ASs contained). Only few conflicts involve ASs with a higher difference of resilience from 0.2 up to 0.72. There might also be reasons for legitimate cooperation of such ASs but it may also be an indicator of a hijacking event. The number of conflicts with more than two ASs involved is 264, which is 3.67% of all conflicts. It is worth mentioning, that in contrast to Lad's approach the new formula is easily adjustable to calculate the resilience even when three or more ASs are involved.

B. AS resilience

Figure 5 presents the mean resilience values of each level resulting from the new formula as an overview.

The resilience of each AS currently participating in the Internet has been calculated with both formulas described in

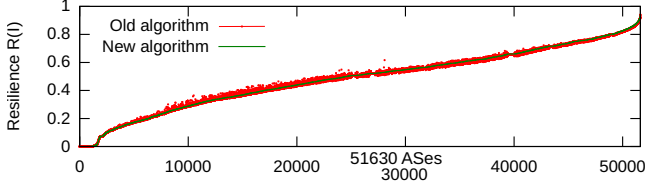


Figure 6: Difference of AS resilience between both formulas.

Section IV. As shown in Figure 6, the tendency of Lad's algorithm is quite near the correct values. Interestingly, the new formula calculates slightly lower values in the lower resilience region and slightly higher values near the upper bounds.

The results of Lad et al. [11] indicate that ASs directly connected to multiple Tier 1 ASs are the most resilient ASs for the evaluated data. This indication is also supported by the results computed for the current Internet peering graph.

C. The role of IXPs

The assessment of the role of IXPs when it comes to prefix hijacking resilience can be used to anticipate possible future states of Internet routing. IXPs provide low cost opportunities to establish links between multiple ASs that are already located on site. Peering opportunities for level 1 ASs are derived and applied for four different scenarios. This work is reduced to peering between level 1 ASs only, as many level 1 ASs experience high resilience values. In case of peering between different levels, the lower level AS most likely pays the higher level AS as an upstream provider. As this work focuses on cost-efficient peering, inter level peering opportunities are not regarded. Based on the selection of 1%, 10%, 50% and all of the possible links, the resilience of ASs is computed.

Peering opportunities are only seen as such, if two ASs are already located at the same IXP. This allows establishing links between them at very low additional cost and is therefore considerable. In most of the cases, it is technically no more than a few lines in the configuration of the border routers in charge. This seems to be a good reason to prefer peering with ASs residing nearby at the same IXP. The peering opportunities are derived from the BART IXP member database as mentioned in Section IV. 978,256 peering opportunities at IXPs located in Europe are provided for 1,960 level 1 ASs. These links are further classified as peer-to-peer relationship between ASs.

Accordingly, the change of an ASs resilience also changes the de-facto resilience of all the other ASs, as the resilience value is equal to its impact with respect to prefix hijacking. Consequently, a complete prefix hijacking scenario has to be simulated for each of the considered cases.

The evaluation focused on the resilience value of the selected 1,960 ASs. Randomly, 1%, 10%, 50% and 100% of possible additional AS links are selected for simulation.

On establishing 1% (i.e. 9,591) additional peer-to-peer links, 30 ASs experience an increment of their resilience

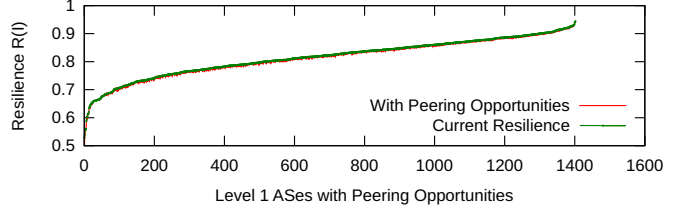


Figure 7: Level 1 ASs after establishing 1% peering opportunities.

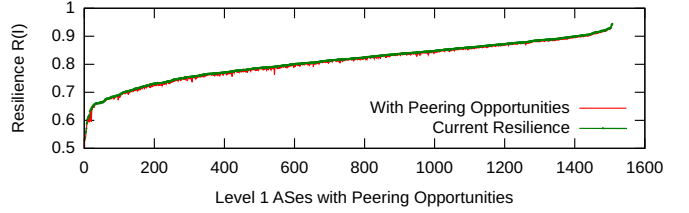


Figure 8: Level 1 ASs after establishing 10 % peering opportunities.

(avg. 0.1786%) while 1373 ASs had decreasing values (avg. 0.1786%) as shown in Figure 7.

AS 41883 has the highest gain of resilience with 0.3540%. It actually peers with two other ASs, none of them is a level 1 AS. One peer is a level 0 AS and the other one is a level 2 AS. The highest loss of resilience is experienced by AS 20672. The value decreases by 1.5195% from 0.7040 to 0.6933.

97,883 additional links between 1,508 ASs have been created when simulating 10% chosen peering opportunities. Compared to the current routing state, the resilience of the corresponding ASs decreases (Figure 8).

44 ASs achieved an increment of prefix hijacking resilience (avg. 0.21%). 1,464 ASs experience a lower resilience value in the simulation (avg. 0.4825%). AS 41883 has the highest gain of resilience by 0.46% with 19 additional peers. AS 59865 has the highest loss of resilience. The value decreases by 6.8797% from 0.6395 to 0.5954 with 109 additional peers in this simulation.

The creation of 50% of the peering opportunities led to 489,005 additional links for 1,510 ASs. The resilience of ASs slightly suffers from the higher number of AS links compared to the current routing state (Figure 9).

55 ASs achieved a higher resilience (avg. 0.23%). 1,455

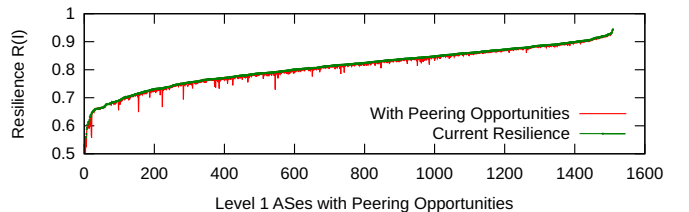


Figure 9: Level 1 ASs after establishing 50 % peering opportunities.

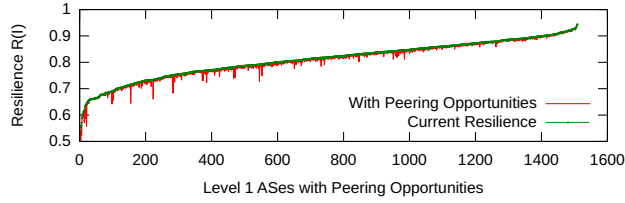


Figure 10: Level 1 ASs after establishing all peering opportunities.

ASs experience a lower resilience value (avg. 0.61%). Again, AS 41883 has the highest gain of resilience in this simulation scenario. The value increased by 0.56% this time. In this simulation, it establishes additional links to 53 other ASs. 4,749 of the remaining ASs without additional links have a resilience growth of 0.3442% in average. AS 1200 experiences the largest loss of resilience losing 14.07% from 0.5533 to 0.4751. It has been selected to peer with additional 402 level 1 ASs for the simulation. Regarding the remaining ASs, a resilience loss by 0.5133% is calculated for 9,623 ASs.

The establishing of all opportunities of AS links at IXPs has a huge effect on the resilience of level 1 ASs. The AS resilience calculated in this simulation is shown in Figure 10.

In this step, the average loss reaches its highest value, while the average gain is still around 0.23%. This simulation leads to a higher resilience value for 56 ASs (avg. 0.23%) and a lower value for 1454 ASs (avg. 0.6715%). As well, AS 41883 has the highest value added to its originating 0.6127. It increases by 0.58% up to 0.6163. This time, additional links to 71 ASs were simulated. AS 1200 again suffers from the highest loss. Its value decreased by 31.5% from 0.5533 to 0.3783 with 875 additional links added.

VI. CONCLUSION

This paper focussed on the resilience of ASs against network prefix hijacking. Prefix hijacking resilience is directly related to the interconnectedness as well as the topological level of an AS. This relationship is considered based on cost-efficient the peering opportunities provided by IXPs. Shortcomings of the existing formula proposed by Lad et al. [11] to calculate the resilience are demonstrated and discussed for an example AS graph. The discussion results in the proposal of an improved formula to accurately calculate prefix hijacking resilience in the Internet. The difference between the values calculated by both formulas is evaluated based on real peering graph of the Internet that has been derived from publicly available routing information. Therefore, more than 30,000,000 hijacking events were simulated and the results evaluated accordingly.

As IXPs allow cost-effective set up of links between ASs, their role was investigated regarding the resilience value of connected ASs. Peering opportunities were derived from publicly available member lists of Internet exchange points and provided to the simulation system. The set of IXPs is limited to those geographically located in Europe. Opportunities were

investigated for Level 1 ASs. The simulation for the evaluation is performed with established links for 1%, 10%, 50% and 100% of the ASs' peering opportunities.

It is shown, that it is possible to influence the resilience of an AS through establishing or abolishing links. As the simulations indicate, no general statement can be given about the number of links and the relation to the resilience value. Establishing additional links based on the presented work is easy and causes nearly no cost. The improved formula can be used to compute the resulting resilience value. The proposed approach shows substantially that IXPs can influence the resilience of Level 1 ASs if they take their peering opportunities.

A. Future work

Prefix hijacking events need to be investigated with respect to resulting partitions and the resilience level of ASs in the one or the other partition. In case of ongoing events, the value of this information should be considered with respect to mitigation mechanisms that are able to manipulate the resulting partitions.

IPX member lists provide valuable information about peering opportunities for ASs. As this work focuses on peering between same level ASs, peering opportunities between ASs in different levels should be evaluated on cost-effectiveness.

Acknowledgements: The authors would like to thank Arnold Sykosch for the helpful comments on a previous version of this paper.

REFERENCES

- [1] W. Aiello, J. Ioannidis, and P. McDaniel, "Origin authentication in interdomain routing," in *Proceedings of the 10th ACM conference on Computer and communications security*, ser. CCS '03. New York: ACM, 2003, pp. 165–178.
- [2] BGP Anomaly Research Toolkit, "http://bgp.cs.uni-bonn.de/," Jun. 1st 2016.
- [3] BGPMonitor, "http://www.bgpmon.net/," Jun. 1st 2016.
- [4] R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol," RFC 6810 (Proposed Standard), Jan. 2013. [Online]. Available: <http://www.ietf.org/rfc/rfc6810.txt>
- [5] CAIDA AS Relationships, "http://www.caida.org/data/as-relationships/," Jun. 1st 2016.
- [6] L. Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, Dec. 2001.
- [7] M. Grey, M. Rossberg, and G. Schaefer, "Automatic Creation of VPN Backup Paths for Improved Resilience Against BGP-attackers," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. New York: ACM, 2012, pp. 613–620.
- [8] X. Hu and Z. M. Mao, "Accurate Real-time Identification of IP Prefix Hijacking," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP '07. Washington, DC: IEEE Computer Society, 2007.
- [9] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, pp. 582–592, Apr. 2000.
- [10] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: a prefix hijack alert system," in *Proceedings of the 15th conference on USENIX Security Symposium - Volume 15*. Berkeley, CA: USENIX Association, 2006.
- [11] M. Lad, R. Oliveira, B. Zhang, and L. Zhang, "Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks," in *Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, ser. DSN '07. Washington, DC: IEEE Computer Society, 2007, pp. 368–377.

- [12] NIST, "<http://rpki-monitor.antd.nist.gov/?p=0&s=1>," Jun. 1st 2016.
- [13] P. v. Oorschot, T. Wan, and E. Kranakis, "On Interdomain Routing Security and Pretty Secure BGP (psBGP)," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 3, Jul. 2007.
- [14] B. A. Prakash, N. Valler, D. Andersen, M. Faloutsos, and C. Faloutsos, "BGP-lens: Patterns and Anomalies in Internet Routing Updates," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '09. New York: ACM, 2009, pp. 1315–1324.
- [15] J. Qiu, L. Gao, S. Ranjan, and A. Nucci, "Detecting bogus BGP route information: Going beyond prefix hijacking," in *Third International Conference on Security and Privacy in Communication Networks and the Workshops*, 2007, pp. 381–390.
- [16] RIPE Routing Information Service (RIS), "<http://www.ripe.net/data-tools/stats/ris/>," Jun. 1st 2016.
- [17] X. Shi, Y. Xiang, Z. Wang, X. Yin, and J. Wu, "Detecting Prefix Hijackings in the Internet with Argus," in *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, ser. IMC '12. New York: ACM, 2012, pp. 15–28.
- [18] Team Cymru, "<http://www.team-cymru.org/bogon-reference-bgp.html>," Jun. 1st 2016.
- [19] Toonk, A., "How Hacking Team Helped Italian Special Operations Group with BGP Routing Hijack," Aug. 2015. [Online]. Available: <http://www.bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/>
- [20] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford, "Don't Secure Routing Protocols, Secure Data Delivery," in *Proc. 5th ACM Workshop on Hot Topics in Networks (Hotnets-V)*, Irvine, CA, Nov. 2006.
- [21] R. White, "Securing BGP through secure origin BGP," *Internet Protocol Journal*, vol. 6, no. 3, Sept. 2003.
- [22] WIRED, "Revealed: The Internet's Biggest Security Hole," Jun. 1st 2016.
- [23] M. Wübbeling, "Visibility of Routing Anomalies for End Users," SR-2013-01, GI FGSIDAR, Tech. Rep., 2013.
- [24] M. Wübbeling, T. Elsner, and M. Meier, "Inter-AS Routing Anomalies: Improved Detection and Classification," in *Proceedings of 6th International Conference on Cyber Conflict*, J. S. P. Brangetto, M. Maybaum, Ed., 2014.
- [25] Z. Zhang, Y. Zhang, Y. C. Hu, and Z. M. Mao, "Practical defenses against BGP prefix hijacking," in *Proceedings of the 2007 ACM CoNEXT conference*, ser. CoNEXT '07. New York: ACM, 2007, pp. 3:1–3:12.
- [26] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An analysis of BGP multiple origin AS (MOAS) conflicts," in *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, ser. IMW '01. New York: ACM, 2001, pp. 31–35.
- [27] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "Detection of Invalid Routing Announcement in the Internet," in *Proceedings of the 2002 International Conference on Dependable Systems and Networks*, ser. DSN '02. Washington, DC: IEEE Computer Society, 2002, pp. 59–68.