# Concurrent Prefix Hijacks: Occurrence and Impacts*

Varun Khare
vkhare@cs.arizona.edu
The University of Arizona

Qing Ju
qingju@cs.arizona.edu
The University of Arizona

Beichuan Zhang
bzhang@cs.arizona.edu
The University of Arizona

## ABSTRACT

A *concurrent prefix hijack* happens when an unauthorized network originates IP prefixes of *multiple* other networks. Its extreme case is leaking the entire routing table, *i.e.*, hijacking all the prefixes in the table. This is a well-known problem and there exists a preventive measure in practice to safeguard against it. However, we investigated and uncovered many concurrent prefix hijacks that didn't involve a full-table leak. We report these events and their impact on Internet routing. By correlating suspicious routing announcements and comparing it with a network's past routing announcements, we develop a method to detect a network's abnormal behavior of offending multiple other networks simultaneously. Applying the detection algorithm to BGP routing updates from 2003 through 2010, we identify five to twenty concurrent prefix hijacks every year, most of which are previously unknown to the research and operation communities at large. They typically hijack prefixes owned by a few tens of networks, last from a few minutes to a few hours, and pollute routes at most vantage points.

## Categories and Subject Descriptors

Computer Systems Organization [**Computer-Communication Networks**]: Network Operations—*Network Monitoring*

## General Terms

Algorithms, Measurement, Verification

## Keywords

BGP Security, Prefix Hijacking

*The material in this article is based upon the work partially supported by DHS grant N66001-08-C-2028 and by Open Project of Shenzhen Key Lab of Cloud Computing Technology & Applications (SPCCTA). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.


*IMC'12,* November 14–16, 2012, Boston, Massachusetts, USA.


## 1. INTRODUCTION

The Internet is an interconnection of tens of thousands of independently administered Autonomous Systems (ASes), which originate their allocated IP prefixes to the Internet via the Border Gateway Protocol (BGP). Due to the lack of authentication of BGP messages, an unauthorized network can originate prefixes owned by other networks [24, 18], *i.e.*, hijacking other prefixes, to divert traffic for those prefixes towards unauthorized network. Malicious attackers have been known to use prefix hijacking to hide their network identity in sending spam [28], inflict denial-of-service attacks by dropping traffic, or even manipulate content of the traffic before forwarding it to destination [14]. Configuration errors in BGP routers have also caused prefix hijacking, leading to service outages for other networks.

A concurrent prefix hijack is an event where an unauthorized network announces prefixes of *multiple* other networks. Its extreme case is leaking the entire routing table, *i.e.*, hijacking all the prefixes in its BGP table. The first well-known case of such prefix hijacking is the full table leak from AS 7007 [1] on April 25, 1997, which lasted for hours and disrupted services for many networks. A more recent event was in September 2008 when AS 8997 falsely announced 117K prefixes [3].

A commonly held belief is that full-table or near full-table leaks is becoming rare. The wide awareness of the problem helps reduce configuration errors and a new BGP configuration option called "max-prefix limit" helps stop such leaks. Once configured for a BGP session, the max-prefix limit specifies the maximum number of prefixes that can be received from a peer, and if that limit is exceeded, the BGP session by default is reset to stop the potential table leak. However without actual data on prefix hijacks it is unclear if such a belief is close to reality. Furthermore it is unclear whether concurrent prefix hijacks of medium or small scales happen on the Internet or not. If they do occur then what are their characteristics, *e.g.*, when did they occur, who instigated them, how many victim prefixes were hijacked, how often did they happen and how long did they last, etc.

Detecting prefix hijacks is a hard problem. Existing techniques fall into two categories. In schemes such as [16, 23, 10, 32, 34], authoritative prefix ownership is known a priori and is used to compare against observed routing messages or forwarding paths. The knowledge of prefix ownership allows accurate detection of prefix hijacks, but in many scenarios complete and up-to-date ownership information is not available. Detection schemes such as [6, 4, 29, 27] do not require such authoritative information. They collect prefix origin

information from routing updates or Internet registrars and apply various filters to identify suspicious events. However, since prefix hijacks and some legitimate operational practices have similar behaviors [33], pinpointing real hijacks without prefix ownership information has been a notoriously hard problem. These schemes usually generate a large number of alarms, many of which may be false positives.

While individual hijacks are difficult to identify, concurrent hijacks are relatively easier even without prefix ownership information. When a network originates prefixes of another network, it can be a hijack or due to an operational arrangement not known to the public. But when a network simultaneously originates prefixes of *many* other networks, it is highly likely to be a real hijack since operational arrangements with many different networks are unlikely to take effect at the same time. Based on this observation, we develop a scheme that detects concurrent prefix hijacks by correlating suspicious origin announcements and identifying networks that are offending many other networks simultaneously. In order to facilitate real-time detection and reaction, we tune the scheme's parameters to minimize false positives.

Applying this scheme to RouteViews Oregon BGP data from 2003 through 2010, we detect 5 to 20 concurrent prefix hijacks each year. They typically hijack prefixes of a few tens of other networks, last from a few minutes to a few hours, and pollute routes at most vantage points, meaning that the damage to data traffic could be widespread. We verify detected events in 2008, 2009, and 2010 via email communication with network operators. We sent 582 emails and received 63 valid replies, from which 53 confirmed prefix ownership, and 51 of those confirmed an individual prefix hijack. All the 21 detected events were confirmed as real hijacks as each event had at least one confirmed individual prefix hijack. This means that our scheme detected concurrent prefix hijacks with zero false positive in these three years . Interestingly most events are not mentioned in operator mailing lists such as NANOG [9] or identified in research literature, implying that the network community in general is not aware of these hijacks. Furthermore, most operators of victim prefixes told us that they were unaware of their prefixes being hijacked. To our best knowledge, this is the first time these under-radar prefix hijacks are discovered, verified, and documented.

The rest of the paper is organized as follows. Section 2 describes the detection scheme. Section 3 reports detected incidents and analyzes the results. We discuss related work in Section 4 and conclude the paper in Section 5.

## 2. THE DETECTION ALGORITHM

While our current focus is to identify and analyze concurrent prefix hijacks from archived data, we also have a long-term goal of being able to automatically detect and resolve these hijacks based on real-time BGP updates. Therefore we have the following two requirements on the detection algorithm: (1) requiring no authoritative prefix ownership information, and (2) minimizing false positives. The first one allows anyone who has access to BGP updates to be able to detect prefix hijacks. For example, if YouTube prefixes are hijacked, any ISP or monitoring service (*e.g.*, Cyclops [16]) that has received the false routing announcements would be able to detect it. The second requirement allows fast response to hijacks. If there are significant false positives, operators have to be involved to judge whether a detected event is a real hijack or not, which takes time. For instance, when a YouTube prefix was hijacked in 2008, it took 80 minutes for YouTube to launch the first countermeasure [13]. Minimizing false positives helps automate and speed up response to detected hijacks. Inevitably our detection algorithm will have more false negatives. These are easily covered by existing detection schemes which report a large number of suspicious events and can be examined by operators later.

The current detection algorithm processes archived BGP tables and updates in five steps to detect routing events where one network hijacks prefixes of multiple other networks at the same time.

### *Step A: single view of origin changes.*

We collect prefix origin changes observed from a single BGP monitor. Every BGP update contains a prefix and an AS path, and we treat the last AS in AS path as origin of the prefix. As we process data yearly, the algorithm reads all BGP tables and updates from a single monitor in one year and records which AS originates which prefix during which time period. This time series of (prefix, origin AS) set forms a single monitor's view of origin changes.

### *Step B: global view of origin changes.*

Since BGP is a path vector protocol, different monitors see different things depending upon where they are relatively to the routing events. When a network hijacks prefixes of multiple other networks, some monitors may not see it at all, and some monitors may only see part of it. Therefore in the second step we combine the single views of individual monitors into a global view of origin changes. The result is a time series of (prefix, origin AS) set over the entire year. It is origin AS *set* because a prefix can be announced by multiple ASes for legitimate reasons [33].

### *Step C: filter out potentially legitimate changes.*

Since many origin changes are legitimate, in this step we try to filter them out to reduce noise in later steps. Accurately identifying all legitimate origin changes is almost impossible, otherwise we would be able to identify all prefix hijacks accurately. What we do here is to run a few best-effort heuristics to discard origin changes that are likely to be legitimate. As long as the heuristics are reasonable, their accuracy is not critical to final results. If some legitimate origin changes are kept, they will become noise and be filtered out in a later step. If some illicit origin changes are discarded in this step, the worst case is some more false negatives in the final results, and as we explained earlier, false negatives can be captured by existing schemes and our scheme focuses on minimizing false positives.

Every prefix is associated with a stable set and a related set containing ASes that probably can legitimately announce the prefix.

**Stable Set** captures ASes that are likely owners of a prefix. Usually the owner AS of a prefix is expected to announce the prefix persistently for a long duration. Figure 1 shows the CDF of cumulative announcement duration of every (prefix, origin AS) pair in 2009. While about 55% of prefix-origin AS pairs are live throughout the entire year, 25% are live for somewhere between one day and one year, and 20% are extremely short-lived, lasting less than one day. Further analysis shows that the middle section of the curve

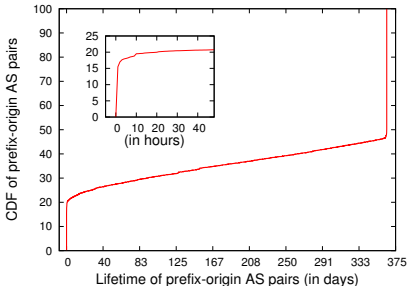


**Figure 1: Lifetime of Prefix-Origin pairs in 2009**

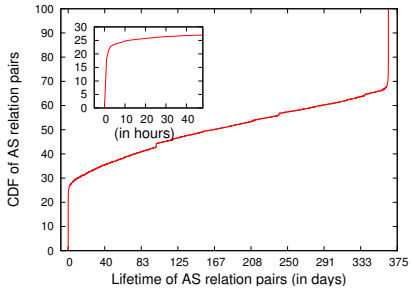


**Figure 2: Lifetime of AS relation pairs in 2009**

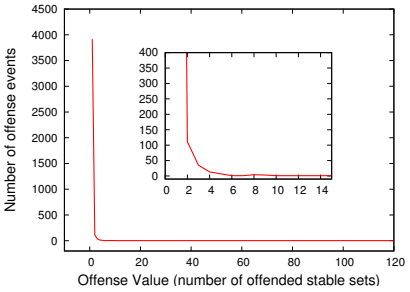


**Figure 3: Offense Value of Events in 2009**

are due to new prefixes that start to be announced during the year or prefixes that ceased to be announced sometime in the middle of the year. This leaves about 20% short-lived announcements that are deemed to be suspicious. Therefore any AS announcing a prefix cumulatively for one day or more within a year is included in the prefix's stable set. We choose one day as a threshold because (1) it is near the knee point of the curve, and (2) we assume operators are watching their networks and hijacks are dealt with within 24 hours mostly.

**Related Set** captures ASes that are not the owner of the prefix but can legitimately announce it in operation. It is impossible to enumerate all operational practices that lead to such legitimate announcements. We have found the following four cases useful for our detection algorithm.

First, an AS in a prefix's stable set also belongs to related set of all its sub-prefixes. This captures the case where ISPs de-aggregate prefixes and announce the sub-prefixes. Sometimes operators implementing TE de-aggregate prefixes to steer traffic within particular IP address range through specific paths [25].

Second, for all ASes in a prefix's stable set, their direct provider ASes also belong to this prefix's related set. This captures the case where a provider network may announce its customer's prefixes, *e.g.*., during failures.

For this purpose we use a simple heuristic to identify stable provider-customer inter-AS links. We start with a list of well-known tier-1 ASes, and given an AS path, the link from a tier-1 AS to a non-tier1 AS is provider-customer, and any link after that is also provider-customer due to the commonly deployed No-Valley policy. This can be considered as a subroutine in most of the existing AS relationship inference algorithms (*e.g.*, [19]), and thus the accuracy in inferring provider-customer relationship should be similar, although we do not need to infer peer-peer or sibling-sibling relationship, which is the challenging part of general AS relationship inference.

Since we are processing continuous routing updates, there is an issue that existing relationship inference algorithms do not deal with: the lifetime of links and relationships. Figure 2 presents CDF of the announcement duration of every AS relation pair in 2009. About 33% of AS relation pairs are live for the entire year, about 41% are live for somewhere between a day and a year, and nearly 26% are extremely short-lived, lasting less than a day. The short-lived links are more likely to be caused by configuration errors or route leaks. Thus we consider a provider-customer relationship stable if the link has been announced for one day or more cumulatively in a year. One day is chosen as the threshold since it is near the knee point of the curve. Only when the relationship is stable will the provider AS be added into the related set of customer's prefixes.

Third, ASes participating in an Internet Exchange Point (IXP) (as listed on IRL [7]) can legitimately announce the IXP's prefixes, and similarly the IXP AS can also legitimately announce the prefixes of its participating ASes.

Fourth, ASes belonging to the same organization are related and can legitimately announce each others prefixes. We simply infer such relation from the domain name of the contact emails listed in the WHOIS [12] database.

### *Step D: offense value.*

Any AS not belonging to a prefix's stable set or related set but originating the prefix is deemed to be an *offending AS*, attempting to potentially hijack the prefix. In such case, we also say that the AS is offending the prefix's stable set, which represents the owner of the prefix. For an offending AS, we define its **offense value** as the number of unique stable sets that this AS is offending at any given moment. The offense value captures how many other networks are being potentially hijacked simultaneously. Based on the filtered global view of origin changes, we compute offense value for every AS for the entire year.

### *Step E: concurrent prefix hijacks.*

Figure 3 presents the distribution of offense values of all possible concurrent hijack events in 2009. Most events pose small offense values of less than three and some of them are found to be legitimate cases after detailed analysis. We choose 10 as a threshold for identifying real concurrent prefix hijacks: if the offense value is no less than 10, then the event is reported as a concurrent hijack. This value is chosen because (1) it is close to the knee point in Figure 3, (2) it is conservative than the actual knee point so as to minimize false positive, and (3) it is not too conservative to capture non-trivial hijacks, that is, hijacks other than full-table or near-full-table leaks.

### *Summary.*

Algorithm 1 summarizes the above steps. It uses one year of archived BGP tables and updates, available at Route Views Oregon monitors [11], to construct stable and re-

| Date mm/dd/yy | Offender ASN | Type of Network | Offense Value | Victim ASes | Victim Prefixes | Victim IP Addresses | Duration | Monitor Pollution |
|---|---|---|---|---|---|---|---|---|
| 04/08/10 | 23724 | Small ISP | 2365 | 2289 | 12115 | 113,924,096 | 21 mins | 94.4% |
| 04/22/10 | 11269 | Small ISP | 19 | 19 | 83 | 731,904 | 2.32 mins | 94.6% |
| 05/19/10 | 10834 | Small ISP | 15 | 14 | 85 | 141,824 | 42.90 mins | 94.6% |
| 08/12/10 | 5 | Stub | 15 | 15 | 32 | 98,816 | 5.28 mins | 10.8% |
| 09/10/10 | 27986 | Small ISP | 18 | 18 | 356 | 628,480 | 9.07 mins | 94.6% |
| 10/04/10 | 33770 | Small ISP | 20 | 20 | 188 | 393,216 | 20.67 mins | 91.9% |
| 02/14/09 | 8895 | Small ISP | 27 | 31 | 243 | 289,280 | 1.96 hours | 95.35% |
| 04/07/09 | 36873 | Stub | 13 | 15 | 45 | 27,392 | 9.98 mins | 95.12% |
| 05/05/09 | 10834 | Small ISP | 99 | 91 | 1108 | 1,713,664 | 3.06 hours | 95.23% |
| 07/12/09 | 29568 | Small ISP | 15 | 17 | 56 | 20,480 | 23.45 mins | 50.00% |
| 07/22/09 | 8997 | Small ISP | 170 | 173 | 351 | 101,500,416 | 1 min | 4.76% |
| 08/12/09 | 4800 | Small ISP | 13 | 13 | 39 | 18,176 | 0.53 mins | 95.23% |
| 08/13/09 | 4800 | Small ISP | 75 | 68 | 492 | 685,568 | 7.82 hours | 95.23% |
| 12/04/09 | 31501 | Small ISP | 18 | 19 | 77 | 1,574,400 | 1.02 mins | 21.43% |
| 12/15/09 | 39386 | Large ISP | 23 | 24 | 67 | 664,064 | 1 min | 88.10% |
| 04/28/08 | 44237 | Small ISP | 13 | 13 | 21 | 82,688 | 7.91 mins | 86.4% |
| 06/17/08 | 8953 | Small ISP | 105 | 113 | 218 | 113,920 | 2.12 mins | 90.9% |
| 08/26/08 | 24739 | Small ISP | 16 | 16 | 42 | 107,008 | 17.98 mins | 95.3% |
| 09/22/08 | 8897 | Small ISP | 17686 | 15270 | 116,753 | 1,511,397,056 | 21.95 hours | 40.5% |
| 12/31/08 | 1967 | Stub | 17 | 17 | 49 | 469,504 | 5.72 mins | 26.2% |
| 12/31/08 | 6849 | Large ISP | 37 | 38 | 52 | 25,856 | 2.21 hours | 85.7% |

**Table 1: Concurrent Prefix Hijacking Events in 2008, 2009 and 2010 (all confirmed)**

**Algorithm 1** Concurrent Prefix Hijacks Detection

```
for all BGP routing message
  if AS X announces prefix p at time t
    if AS X ∉ StableSet(p) or RelatedSet(p)
      Update AS X offense value by StableSet(p)
  elsif AS X withdraws prefix p at time t
    if AS X ∉ StableSet(p) or RelatedSet(p)
      Reduce AS X offense value by StableSet(p)
Report hijack: if AS offense value >= 10
```

lated sets. Thereafter every BGP routing announcement is checked whether it is suspicious or legitimate by checking origin AS against stable and related set of prefix. Anytime the offense value of an AS exceeds the threshold of 10, it is reported to be a concurrent hijack.

# 3. CONCURRENT PREFIX HIJACKING RESULTS

In this section, we report detected concurrent prefix hijacks and the verification, followed by some major characteristics and a case study.

## 3.1 Concurrent Prefix Hijacks in 2008–2010

Table 1 lists concurrent prefix hijacks detected in 2010, 2009 and 2008 using BGP data collected by RouteViews Oregon collector. For each event, we classify offending AS as a large ISP if it has more than 50 customers, or a small ISP if it has less than 50 customers, or a stub network if it has no customers. Most of these events are caused by small ISPs with 50 or less customers.

To verify the detection results, we contacted operators of victim networks via emails. The email addresses were extracted from WHOIS [12] records of victim prefixes. Given that prefix ownership, ISP peering relationship and operation practices change over time, older results may not be reliably verified. Thus we did not attempt to verify results older than 2008. We are in the process of verifying results of 2011 and 2012, and plan to publish them online [8] once available.

In the emails we asked about two things: (1) whether the victim prefix is owned by AS(es) in its stable set or not, and (2) whether the hijack routing announcement on the given date and time is legitimate or not. The first question is intended to evaluate the accuracy of stable set inference (i.e., prefix ownership), and the second question is to evaluate the accuracy of detecting individual hijack announcement. A hijack *event* is confirmed if at least one prefix origination by the offending AS is illicit. For each email reply received, we first check the response to the first question. Only after the operator has confirmed prefix ownership will we consider the response to the second question.

We sent out 582 emails in total and received 63 valid replies, among which 53 networks confirmed that they own the prefixes but 10 networks said that they did not own the prefixes. The latter was caused by outdated or inaccurate WHOIS [12] records. For example, some operators said that the prefix was an old allocation that had been returned to their providers. Among the 53 responses that confirmed prefix ownership, 51 networks reported that all ASes in the prefix's stable set are legitimate, while 2 networks reported that some ASes in the stable set are not legitimate. This shows that in most cases the stable set captures prefix ownership correctly, but there exist cases (2 out of 53) where ASes in the stable set do not own the prefix, *i.e.*, their prefix origination are not legitimate, which may cause small false negatives in the final detection result.

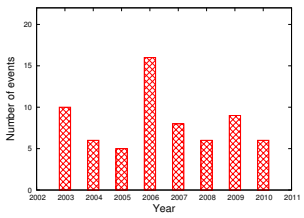


**Figure 4: Hijacks per year**

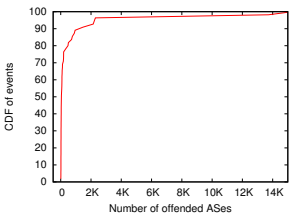


**Figure 5: Offended ASes**

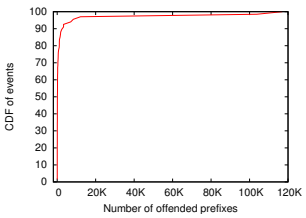


**Figure 6: Victim Prefixes**

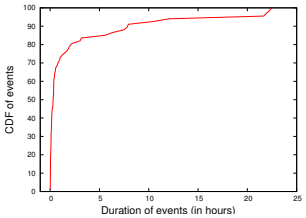


**Figure 7: Event Duration**

In the 53 emails that confirmed prefix ownership, 51 of them confirmed that the suspicious routing announcement was indeed false, *i.e.*, individual prefix hijacks. The other 2 emails explained that the suspicious routing announcements were legitimate. In one case the prefix owner peered with the offending AS, and in the other case the prefix owner and the offending AS belonged to the same company. However, these 2 cases did not cause any false positive in the final result. All the 21 events listed in Table 1 were confirmed as real hijack events since each event had at least one confirmed individual prefix hijack. Therefore by correlating suspicious routing announcements along the time dimension, our algorithm was able to identify a significant number of concurrent prefix hijacks with zero false positive.

Among the 51 confirmed individual prefix hijacks, 49 operators stated that they were unaware of the hijacks; only 2 operators had knowledge of the hijacks and had resolved it by contacting the provider of attacker AS. To some extent this is expected since when a prefix is being hijacked, the prefix owner network does not see the false routing announcement due to BGP's path vector routing. We made attempts to verify whether the network community knew about these events. NANOG is a forum where network operators regularly discuss and attempt to resolve network problems. We scanned the NANOG mailing list on the dates when these prefix hijacks occurred in 2008, 2009 and 2010 and only found discussions about a couple of very large leaks by AS 8997 in 2008 [3] and by AS23724 in 2010 [2]. Furthermore research literature does not report more events than NANOG. The fact that many hijacks happened but went unnoticed highlights the need for fast and accurate detection schemes.

## 3.2 Concurrent Prefix Hijacks in 2003–2010

Applying our algorithm to BGP data collected by RouteViews Oregon collector, we detect totally 60 concurrent prefix hijacks from 2003 through 2010, with about 5 to 20 events each year (Figure 4). The details of all the events are provided online [8]. Here we present some major characteristics of the events.

### 3.2.1 General Impacts

We measure the impacts of these hijack events by the number of ASes, the number of prefixes, and the number of monitor they affected and also the duration of the events. Figure 5 shows the CDF of the number of ASes whose prefixes were hijacked during these events. The top 20% of hijacks affected thousands of ASes, while the next 20% affected between 30 to 100 ASes and finally the remaining 60% affected 30 or less ASes. During these events multiple victim prefixes were hijacked.

Figure 6 shows the CDF of the number of victim prefixes per event. The top 20% of concurrent hijacks involve thousands of prefixes and sometimes as much as half the size of global routing table. The next 20% involve 100 or more prefixes and the remaining 60% involve less than 100 prefixes.

Figure 7 presents the CDF of the duration of each event. Most concurrent prefix hijacks are short-lived, lasting from a few minutes to a couple of hours, but still 20% of them lasted for more than 3 hours. The very short-lived events might be caused by typos in router configurations and were quickly caught and fixed. Adopting tools like router configuration checker [17] may help prevent these from happening. However, the existence of hijacks that lasted for a few hours or more raises the concern of serious damage to the prefix owner's network service.

Figure 8 shows the CDF of the percentage of monitors that were polluted in each hijack event. We say a monitor is *polluted* if it accepts at least one of the hijack routing announcements. In other words, if the monitor is a real router, it would forward traffic towards the hijacker. Since the RouteViews Oregon collector peers with BGP monitors in many different ISPs, the percentage of polluted monitors reflects the scope of the hijack's impacts. The figure shows that the top 70% of hijacks pollute 85% or more monitors, which means most hijack announcements propagate to most of the Internet.

### 3.2.2 Locality of Victim Prefixes

Concurrent prefix hijacking is caused by an AS falsely originating multiple victim prefixes at the same time. But what are the geographical locations of these victim prefixes? For instance, are these prefixes close to the attacker AS or distributed across the globe? We capture the locality of victim prefixes by the percentage of victim prefixes that are originated within the same country as the attacker AS. The geographic locations of victim prefixes were found by using Geo-Lite City [5], and the geographic location of attacker AS was found by looking up its WHOIS [12] record.

Majority of concurrent hijacks involved victim prefixes in the same country as offending AS. Figure 9 presents locality of victim prefixes for hijack events in years 2008 to 2010. For 55% of events more than 80% of victim prefixes are within the same country as attacker AS. Furthermore for about 35% of events every victim prefix is within the same country as attacker AS. This suggests that the false routing announcements do not involve random prefixes but are most likely meant to affect traffic for networks within a local region. Note that though victim prefixes are often in the same country as the attacker AS, the false routing updates are propagated to most of the Internet, causing wide-spread reachability problem to victim prefixes.

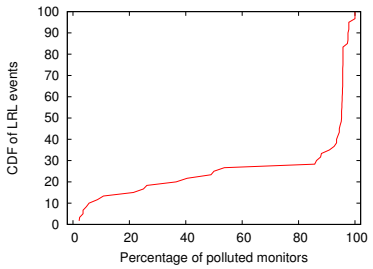


**Figure 8: Monitor pollution**

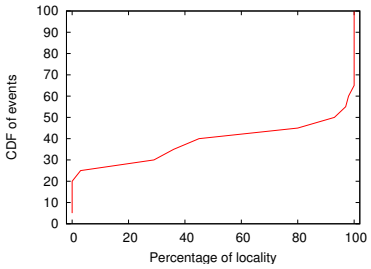


**Figure 9: Locality of victim prefixes**

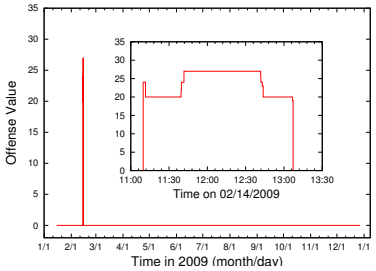


**Figure 10: Prefix Hijacks by AS 8895 in 2009**

### 3.2.3 *A Case Study*

Based on received operator emails, we now present an in-depth study of a verified concurrent prefix hijack that occurred in 2009. This event was caused by AS 8895 on February 14th, 2009 when it falsely originated 243 prefixes, which could potentially impact 289K IP addresses belonging to 34 ASes in Saudi Arabia. The event lasted for nearly 2 hours during which network services of all the involved Saudi ASes were interrupted. The scope of event was global as 41 out of 43 RouteViews Oregon monitors reported the false announcements. Most individual suspicious announcements were confirmed by offended ASes as illegitimate thereby verifying the event.

The network operators of victim prefixes and the offending AS confirmed that the stated hijacks were due to router misconfiguration. The network operator of AS 8895, *i.e.*, ISU/KACST stated that they used to be the major Internet gateway in the Saudi Arabia region and therefore an upstream provider for many local Saudi ISPs. In the past two years other Internet gateways have been launched within the region, one of them being AS 39386, *i.e.*, Saudi Telecom. In that period ISU/KACST shifted focus on educational sectors, universities, libraries and etc. Both these things resulted in many local ISPs switching providers to Saudi Telecom. But due to router misconfiguration AS 8895 kept announcing prefixes of many of its ex-customers which had switched providers to AS 39386.

Figure 10 illustrates how the offense value of AS 8895 reveals this event. Recall that *offense value* is the number of stable sets whose prefixes are hijacked by the offending AS. The offense value of AS 8895 was zero for the entire year except February 14th, 2009 when the leak occurred. The false announcement started at 11:10AM when AS 8895 announced prefixes of an increasing number of its ex-customers. The offense value fluctuated a couple of times but remained near constant at 34 for more than an hour. Finally offense value started to drop and got back to zero at 1:10 PM when the misconfiguration was fixed and false routing announcements stopped.

## 4. RELATED WORK

False BGP routing announcements are a well-known problem [15]. It includes hijacking allocated address space, as well as unallocated or private address space [18]. A number of solutions have been proposed to eradicate the problem of false routing announcements. They can be categorized into two categories: prevention [22, 26, 30, 21, 31], and detection [32, 23, 27, 16, 6].

The prevention techniques attempt to restrict ASes from making false routing announcements. Many prevention proposals [22, 26, 30] require extensive cryptographic key distribution infrastructure, and/or a trusted central database, and hence are difficult to deploy. PGBGP [21] and QBGP [31] attempts to prevent propagation of suspicious announcements. Each router monitors the origin AS for each prefix, any new prefix origination is considered anomalous, and router avoids using anomalous routes if old route is available.

The detection techniques focus on identifying prefix hijack events through monitoring of control plane or data plane and therefore can be categorized as (a) traceroute based solution and (b) control-plane based solution. These detection solutions do not require changes to BGP protocol and thus are more easily deployable. Traceroute based solutions, such as iSPY [32] and Lightweight Probing [34], periodically probe data paths to a specific prefix. Thus they are best to be used by prefix owners to protect their allocated prefix block.

Control-plane-based solutions, such as [27], can monitor the entire routing table passively, but they usually suffer from too many false positives as well as false negatives due to limited vantage points and the lack of ground truth of operational practices [20]. Certain control-plane-based solutions, such as PHAS [23] and MyASN [10], use information provided by prefix owners to filter out false positives, thus they are most effective when prefix owners register their prefixes and keep the registration up to date.

## 5. CONCLUSIONS

By identifying networks that announce prefixes of multiple other networks, we are able to discover 5 to 20 concurrent prefix hijacks every year from 2003 through 2010. For most of these events it is the first time they are discovered, verified, and documented. They typically last from a few minutes to a few hours and affect most monitors, implying these events may inflict significant damage to data traffic. Email communication with network operators verifies that the results of 2010, 2009, and 2008 have no false positives. Encouraged by the success of this method, we are implementing an online detection system that will process real-time BGP updates to generate up-to-date results.

## 6. ACKNOWLEDGEMENT

We are grateful to our shepherd, Sharon Goldberg, for her guidance and help in revising the paper. We would also like to thank anonymous reviewers for their valuable comments.

## 7. REFERENCES


[1] AS 7007 incident. http://en.wikipedia.org/wiki/AS_7007_incident.

[2] ASN 23724. www.merit.edu/mail.archives/nanog/msg07826.html.

[3] ASN 8997. www.merit.edu/mail.archives/nanog/2008/msg00704.html.

[4] BGPmon. http://www.bgpmon.net.

[5] GeoLite City. http://www.maxmind.com/app/geolitecity.

[6] Internet Alert Registry. http://iar.cs.unm.edu/.

[7] Internet Topology Collection. http://irl.cs.ucla.edu/topology.

[8] LRL. dyadis.cs.arizona.edu/projects/lsrl-events.

[9] North American Network Operators' Group. http://www.nanog.org.

[10] RIPE myASn System. http://www.ris.ripe.net/myasn.

[11] Route Views Project. http://www.routeview.org.

[12] Whois Database. http://www.whois.net/.

[13] YouTube Hijacking: A RIPE NCC RIS case study. http://www.ripe.net/news/study-youtube-hijacking.html.

[14] Ballani, H., Francis, P., and Zhang, X. A Study of Prefix Hijacking and Interception in the Internet. In *ACM SIGCOMM* (2007).

[15] Butler, K., Farley, T., McDaniel, P., and Rexford, J. A survey of bgp security issues and solutions. *Proceedings of the IEEE 2010*, 1 (Jan. 2010), 100–122.

[16] Chi, Y.-J., Oliveira, R., and Zhang, L. Cyclops: AS-level Connectivity Observatory. *SIGCOMM CCR 38*, 5 (2008), 5–16.

[17] Feamster, N., and Balakrishnan, H. Detecting BGP Configuration Faults with Static Analysis. In *Proc. NSDI* (2005).

[18] Feamster, N., Jung, J., and Balakrishnan, H. An empirical study of "bogon" route advertisements. *SIGCOMM Comput. Commun. Rev. 35*, 1 (Jan. 2005), 63–70.

[19] Gao, L. On Inferring Autonomous System Relationships in the Internet. In *IEEE ACM Transactions on Networking* (2000), vol. 9, pp. 733–745.

[20] Hu, X., and Mao, Z. M. Accurate Real-time Identification of IP Prefix Hijacking. In *IEEE Symposium on Security and Privacy* (2007).

[21] Karlin, J., Forrest, S., and Rexford, J. Pretty Good BGP: Improving BGP by Cautiously Adopting Routes. In *ICNP* (2006).

[22] Kent, S., Lynn, C., Mikkelson, J., and Seo, K. Secure Border Gateway Protocol (S-BGP). *IEEE JSAC 18* (2000), 103–116.

[23] Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., and Zhang, L. PHAS: A Prefix Hijack Alert System. In *USENIX Security* (2006).

[24] Mahajan, R., Wetherall, D., and Anderson, T. Understanding bgp misconfiguration. In *SIGCOMM '02* (2002).

[25] Meyer, D., Zhang, L., and Fall, K. Report from the IAB Workshop on Routing and Addressing. draft-iab-raws-report-01.txt, 2007.

[26] Ng, J. BGP Extensions for Secure Origin BGP, April 2004. ftp://ftp-eng.cisco.com/sobgp/drafts/draft-ng-sobgp-bgp-extensions-02.txt.

[27] Qiu, J., Gao, L., Ranjan, S., and Nucci, A. Detecting Bogus BGP Route Information: Beyond Prefix Hijacking. In *SecureComm* (2007).

[28] Ramachandran, A., and Feamster, N. Understanding the Network Level Behavior of Spammers. In *ACM SIGCOMM* (2006).

[29] Siganos, G., and Faloutsos, M. Neighborhood Watch for Internet Routing. In *IEEE INFOCOM* (2007).

[30] Subramanian, L., Roth, V., Stoica, I., Shenker, S., and Katz, R. Listen and Whisper: Security Mechanisms for BGP. In *NSDI* (2004).

[31] Zhang, M., Liu, B., and Zhang, B. Safeguarding Data Delivery by Decoupling Path Propagation and Adoption. In *INFOCOM* (2010).

[32] Zhang, Z., Zhang, Y., Hu, Y. C., Mao, Z. M., and Bush, R. iSPY: Detecting IP Prefix Hijacking on My Own. In *SIGCOMM* (2008).

[33] Zhao, X., Pei, D., Wang, L., Massey, D., Mankin, A., Wu, S., and Zhang, L. BGP Multiple Origin AS Conflicts. In *IMW* (2001).

[34] Zheng, C., Ji, L., Pei, D., Wang, J., and Francis, P. A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time. In *ACM SIGCOMM* (2007).