Poster: MOAI: Multiple Origin ASes Identification for IP Prefix Hijacking and Mis-Origination

Hironori Imai  
Toho University  
65180021@st.toho-u.ac.jp

Masayuki Okada  
Japan Network Information Center (JPNIC)  
okadams@nic.ad.jp

Akira Kanaoka  
Toho University  
akira.kanaoka@is.sci.toho-u.ac.jp

I. INTRODUCTION

In BGP, which controls the Internet routing information, the presence of inappropriate routing information in advertisements is a significant problem. Inappropriate route advertising in BGP is called Mis-Origination. In this research, we focused on IP Prefix Hijacking caused by IP prefix collisions, which is a typical case of Mis-Origination. The existence of Mis-origination has been pointed out[1], [2], and prevention and detection methods have been actively studied. IP prefix conflicts are caused by Multiple Origin ASs (MOAS), in which the IP address range is advertised by multiple ASs. In recent years, services have diversified, such as DDoS mitigation and IP address leasing, and they are generating MOAS with a clear intention without malice. Due to the intentional increase in MOAS, the IP prefix hijacking technology using MOAS suffers from performance degradation and an increase in false detection rate. The proposed method MOAI (Multiple Origin ASes Identification) classifies MOAS as a detection method corresponding to service diversification, and judges whether the MOAS is benign or malignant from multiple viewpoints. As a result of applying this method to actual route information as a verification experiment, it was achieved to narrow down route advertisements with the possibility of hijacking to 155,399 from over 5 billion route advertisements.

The prototype system of MOAI was developed and evaluated using route advertisement information during 2018. The results show its feasibility with fully operational performance. New findings include followings:

- Increase of MOAS advertisements over the past 10 years (32.6 times),
- Benign nature of many MOAS advertisements (98.8%) 
- Expansion of MOAS advertisements in response to DDoS mitigation and CDN use,
- Emergence of IP leasing services
- Frequent occurrence of the MOAS advertisements due to Typo.

II. MOAI OVERVIEW

Fig.1 shows an overview of the proposed method. First, information about the two types of routes is obtained from the BGP monitoring infrastructure, such as RIPE RIS and RouteViews. One is the full route, which is all the route information that the route collector has at a certain point in time. The other is update information, which accumulates a new route advertisement and route advertisement cancellation. New route advertisements and cancellation of route advertisements included in updates are separated, and new route advertisements are extracted. The obtained route advertisement and route information included in the nearest full route is analyzed. Then, the advertisements are classified into five Advertisement Type (AT) using the information of IP address, origin AS information advertisement included in updates, and full route (Table. I).

Among them, AT3 and AT5 are MOAS advertisements. These advertisements are further analyzed. A detailed discussion of each AT is omitted for the sake of space. Multiple origin route advertisements are appended with information about the country or region to which the AS belongs and Whois information.

MultipleOrigin route advertisements may be IP Prefix Hijacking, but there are route advertisements that are not or are very unlikely to be IP Prefix Hijacking for various reasons. Based on the risk of IP Prefix Hijacking, conflicts were classified into 18 types based on the combination of AS number and country code, and AS-related information. This classification is defined as Conflict Type (CT). The 18 CT types are classified into ”No Risk”, ”Low Risk” and ”High Risk”. For the sake of space, the description of 18 CT types is omitted. See the poster for details. Some of CTs such as IP prefix conflict in the same area can be classified mechanically from AS number and country code, but the example, conflicts caused by DDoS mitigation service and collision of IP prefix caused by IP address lease service are classified heuristically. On these conflicts, the heuristic whitelist/blacklist is made by the specialist, and the expansion of the whitelist is continuously carried out at present. In addition, when the operator of the
TABLE II. NUMBER OF ROUTE ADVERTISEMENTS PER ROUTE COLLECTOR

<table>
<thead>
<tr>
<th>Advertise Type</th>
<th># of Ads</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT1</td>
<td>4,799,451</td>
<td>(0.09%)</td>
</tr>
<tr>
<td>AT2</td>
<td>5,132,754,735</td>
<td>(99.58%)</td>
</tr>
<tr>
<td>AT3</td>
<td>2,945,955</td>
<td>(0.06%)</td>
</tr>
<tr>
<td>AT4</td>
<td>10,958,344</td>
<td>(0.21%)</td>
</tr>
<tr>
<td>AT5</td>
<td>3,056,347</td>
<td>(0.06%)</td>
</tr>
<tr>
<td>AT3 + AT5 (MOAS Ads)</td>
<td>6,002,302</td>
<td>(0.12%)</td>
</tr>
</tbody>
</table>

BGP router mistypes the AS number (Typo), a conflict of the IP Prefix also occurs. Since it is not a malicious activity, contact with the operator is considered to be easy. It is desirable to treat it as a different classification from a malicious attack. In our observation, the following three species were designated as Typo: “Skip entering a number”, “Entering a number twice in succession”, and “Entering a number for an adjacent key on the keyboard”.

Finally, the possibility of hijacking is estimated by using the number of hops between the countries or regions of the conflict advertisement transmission AS, and the conflicted AS for the remaining unclassified conflict advertisements.

III. FILTERING EFFECT EVALUATION

To evaluate the filtering effect, analysis is performed using actual advertisement data published by the BGP monitoring infrastructure. We applied MOAI to the advertisement data from January 1, 2018 to December 31, 2018 from RIPE RIS and RouteViews. Detailed explanations are omitted for the sake of space. Table II shows the results of AT classification for route advertisements. 6,002,304 MOAS advertisements (conflicted advertisements) are extracted from 5,154,694,832 advertisements. The information of the country or area was added to the route advertisement of AT3 or AT5, then CT classification and ASN Typo detection were carried out. The results of CT classification and Typo detection are shown in Table III.

Thus, we estimate the likelihood of hijacking by the number of area hops for unclassified advertisements. The results are given in Table IV.

IV. CURRENT EFFORTS

MOAI achieved passive detection using observation data of BGP route advertisement and achieved a high reduction rate by identifying intentional IP prefix collision by CT classification using a whitelist. In the future, in order to further improve the reduction rate and its accuracy, the so-called "correct answer data" of whether the collision of the past IP prefix was intentional or not becomes indispensable. At present, it is planned to carry out hearing to AS on whether the collision was intentional or not on past IP prefixes not generally known. In the future, we will aim to improve further the reduction rate and accuracy based on this data.

REFERENCES


Fig. 1. Overview of MOAI (Multiple Origin ASes Identification) System
MOAI: Multiple Origin ASes Identification for IP Prefix Hijacking and Mis-Origination

Hironori Imai†, Masayuki Okada††, Akira Kanaoka†
(Toho University, 1, Japan Network Information Center)

Introduction

BGP (Border Gateway Protocol) has serious operational problems in terms of Mis-Origination caused by hijacking of network prefixes or misconfiguration of operators.

MOAI Overview

Classify advertisements into 18 CT focusing on ASN and country code
Detect type of adjacent keys based on Levenshtein distance

Verification of Filtering Effect

Over 5 billion route advertisements were obtained from one of two RIPE RIS route collectors (ripe_rc00, ripe_rc01) and RouteViews from January to December 2018. As a result of applying MOAI to these data, 6,002,302 Multiple Origin advertisements were extracted and the route advertisements with the possibility of hijacking were reduced to 155,399 (High Risk advertisements and unclassified advertisement).

Current Efforts

MOAI achieved passive detection using observation data of BGP route advertisement, and achieved high reduction rate by CT classification using white list. In the future, to improve the reduction rate and accuracy, it is planned to conduct a hearing with the AS operator whether conflicts occurred in the past, which are found by MOAI and not generally known, were intentional.