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

Hironori Imai
Toho University
6518002i@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*** (*M*ultiple *O*rigin *A*Sses *I*dentification) 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.

Network and Distributed Systems Security (NDSS) Symposium 2020
23-26 February 2020, San Diego, CA, USA
ISBN 1-891562-61-4
https://dx.doi.org/10.14722/ndss.2020.23xxx
www.ndss-symposium.org

TABLE I. ADVERTISEMENT TYPE (AT) CLASSIFICATION

AT	IP Prefix in update	AS number in update
AT1	Not Found	-
AT2	Exact Match in Full Route	Match in Full Route
AT3	Exact Match in Full Route	Differ from Full Route
AT4	Included in Full Route	Match in Full Route
AT5	Included in Full Route	Differ from Full Route

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 for 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

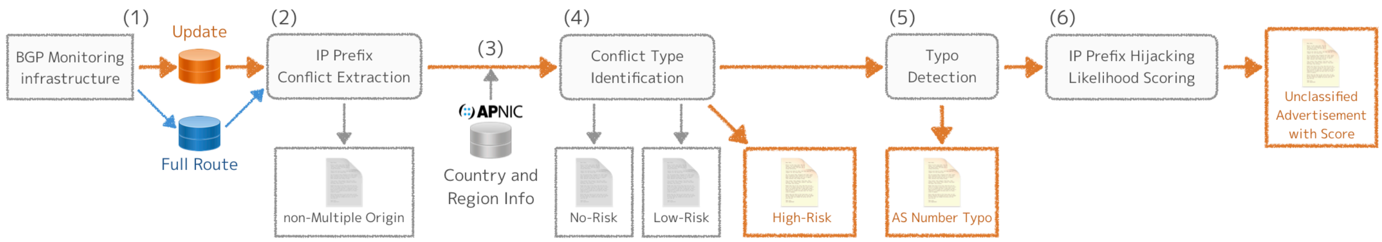


Fig. 1. Overview of MOAI (Multiple Origin ASes Identification) System

TABLE II. NUMBER OF ROUTE ADVERTISEMENTS PER ROUTE COLLECTOR

Advertise Type	# of Ads	(%)
AT1	4,799,451	(0.09%)
AT2	5,132,934,735	(99.58%)
AT3	2,945,955	(0.06%)
AT4	10,958,344	(0.21%)
AT5	3,056,347	(0.06%)
AT3 + AT5 (MOAS Ads)	6,002,302	(0.12%)

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.

TABLE III. ROUTE ADVERTISEMENTS PER CONFLICT TYPE AND TYPO

Conflict Type	description	total	(%)
CT-NR1	Same Org.	39,955	(0.67%)
CT-NR2	CDN	36,699	(0.61%)
CT-NR3	DDoS Srv. Provider	236,483	(3.94%)
CT-NR4	DDoS Srv. Customer	9,610	(0.16%)
CT-NR5	Friendly AS	8	(0.00%)
CT-NR6	Against Hijacking	454	(0.01%)
CT-NR7	Academic	12,595	(0.21%)
CT-NR8	Agency Blocking	1,236	(0.02%)
CT-NR9	IP Addr. Lease	7,786	(0.13%)
CT-LR1	Private AS	279,526	(4.66%)
CT-LR2	Same Area	4,624,204	(77.04%)
CT-LR3	Adjacent Area	236,872	(3.95%)
CT-LR4	Submarine Cable	285,539	(4.76%)
CT-LR5	MANRS	21,555	(0.36%)
CT-LR6	Near AS	54,381	(0.91%)
CT-HR1	IANA Reserved	11,069	(0.18%)
CT-HR2	AS_TRANS	231	(0.00%)
CT-HR3	Unassigned	18,889	(0.31%)
-	Typo	7,270	(0.12%)
-	unclassified	117,940	(1.96%)

TABLE IV. IP PREFIX HIJACKING LIKELIHOOD ESTIMATION OF UNCLASSIFIED ADVERTISEMENTS BY AREA HOP COUNT

Number of Hops n	total	(%)
2 ($P(2)$=0.3)	72,297	(61.30%)
3 ($P(3)$=0.5)	25,245	(21.40%)
4 ($P(4)$=0.5)	2,251	(1.91%)
$\geq$ 5 ($P(n)$=1)	0	(0%)
Unknown	6,086	(5.16%)
EU	12,061	(10.23%)

References

[1] Pierre-Antoine Vervier, Olivier Thonnard, and Marc Dacier. Mind your blocks: On the stealthiness of malicious bgp hijacks. In *NDSS*, 2015.

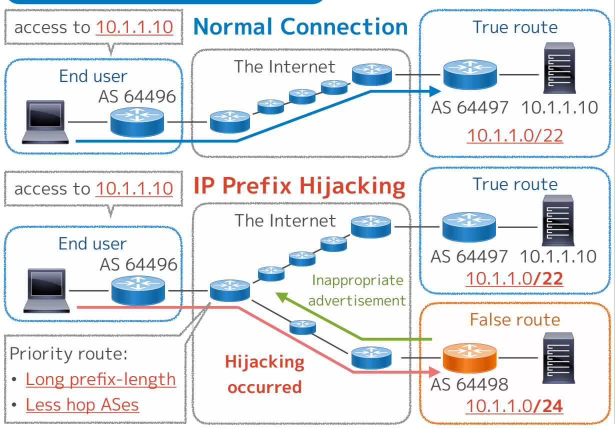
[2] Tao Wan and Paul C Van Oorschot. Analysis of bgp prefix origins during google’s may 2005 outage. In *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, pages 8–pp. IEEE, 2006.

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

Hironori Imai†, Masayuki Okada††, Akira Kanaoka†
(† Toho University, †† 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.



Related Works

- Cannot avoid false detection of intentional IP Prefix collision*1
- cannot detect passive hijacking on any AS

*1 M. Lad, et.al, Phas: A prefix hijack alert system, USENIX Security symposium, 2006.
X. Hu, et.al, Accurate real-time identification of ip prefix hijacking, 2007 IEEE Symposium on Security and Privacy, 2007
S. Hong, et.al, Ip prefix hijacking detection using idle scan. Asia-Pacific Network Operations and Management Symposium, 2009.
*2 Z. Zhang, et.al, slspy: detecting ip prefix hijacking on my own. ACM SIGCOMM Computer Communication Review, 2008.
P. Sermpezis, et.al, Artemis: Neutralizing bgp hijacking within a minute. IEEE/ACM Transactions on Networking, 2018.

Actual Case of IP Prefix Hijacking

- YouTube Hijack (2008)
  Can not access the YouTube
  Damage to content services
- Bitcoin Hijack (2008)
  Take away the missing result of Bitcoin
  The attacker benefit of more than $83,000
- Amazon Route 53 (2018)
  DNS server of Amazon AWS was hijacked
  DNS reply about myetherwallet.com was falsified

MOAI（Multiple Origin ASes Identification）

- Detection of BGP route advertisement using **observation data** (passive detection)
- Classification into 18 collision types, including intentional and non-malicious collisions
- Detection of **any inappropriate route advertisement at any time**

MOAI Overview

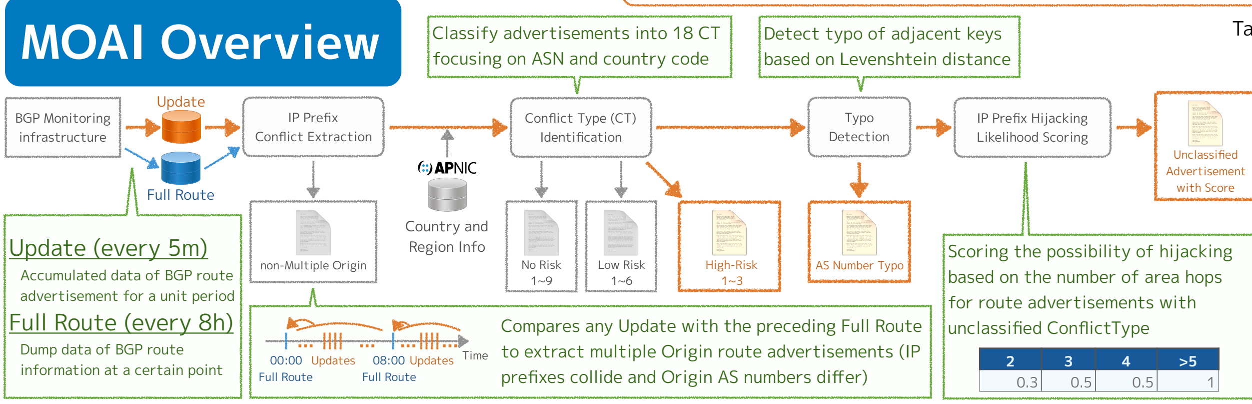


Table1. Conflict Type Classification

CT		Description
No Risk	1	Same Organization
	2	CDN
	3	DDoS Mitigation (Provider)
	4	DDoS Mitigation (Customer)
	5	Friendly AS
	6	Against Hijacking
	7	Academic Project
	8	Agency Blocking
	9	IP address Lease service
Low Risk	1	Private ASN
	2	Same Country/Area
	3	Adjacent Country/Area
	4	Submarine Cable Connected
	5	MANRS
	6	Near AS
High Risk	1	IANA Reserved ASN
	2	AS_TRANS (ASN: 23456)
	3	Unassigned ASN

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** MultipleOrigin advertisements were extracted and the route advertisements with the possibility of hijacking were reduced to **155,399** (High Risk advertisements and unclassified advertisement).

Table2. The Number of Collected Data

	ripe_rc00	ripe_rc01	routeviews	total
Full Route	1,095	1,095	1,094	3,284
Update	105,109	105,107	34,966	245,182
Advertisement	2,460,825,619	924,620,092	1,769,249,121	5,154,694,832

Table3. Number of Route Advertisements per Route Collector

Description	ripe_rc00	%	ripe_rc01	%	routeviews	%	total	%
New Route	3,310,083	0.13	316,491	0.03	1,172,877	0.07	4,799,451	0.09
Same IP / Same ASN	2,451,057,018	99.60	918,760,368	99.37	1,763,117,349	99.65	5,132,934,735	99.58
Same IP / Different ASN	1,137,208	**0.05**	870,895	**0.09**	937,852	**0.05**	2,945,955	**0.06**
Included IP / Same ASN	4,319,553	0.18	3,615,373	0.39	3,023,418	0.17	10,958,344	0.21
Included IP / Dirrefent ASN	1,001,757	**0.04**	1,056,965	**0.11**	997,625	**0.06**	3,056,347	**0.06**

Table4. of Route Advertisements per Route Collector

CT		ripe_rc00	%	ripe_rc01	%	routevie	%	total	%
No Risk	1	15,476	0.72	13.938	0.72	10,541	0.54	39,955	0.67
	2	11,785	0.55	8,127	0.42	16,787	0.87	36,699	0.61
	3	19,133	0.89	19,971	10.4	197,379	10.20	236,483	3.94
	4	3,671	0.17	2,791	0.14	3,148	0.16	9,610	0.16
	5	4	0.00	0	0	4	0.00	8	0.00
	6	106	0.00	273	0.01	75	0.00	454	0.01
	7	4,605	0.22	3,420	0.18	7,570	0.24	12,595	0.21
	8	162	0.01	33	0.00	1,041	0.05	1,236	0.02
	9	3,153	0.15	2,187	0.11	2,446	0.13	7,786	0.13
Low Risk	1	159,233	7.44	40,922	2.12	79,371	4.10	279,526	4.66
	2	1,672,844	78.21	1,657,946	86.00	1,293,414	66.83	4,624,204	77.04
	3	55,798	2.61	33,964	1.76	147,110	7.60	236,872	3.95
	4	102,852	4.81	84,337	4.37	98,350	5.08	285,539	4.76
	5	11,622	0.54	3,880	0.20	6,053	0.31	21,555	0.36
	6	20,918	0.98	15,539	0.81	17,924	0.93	54,381	0.91
High Risk	1	5,503	0.26	1,940	0.10	3,626	0.19	11,069	0.18
	2	189	0.01	4	0.00	38	0.00	231	0.00
	3	6,795	0.32	4,836	0.25	7,258	0.37	18,889	0.31
Typo		2,652	0.12	2,143	0.11	2,475	0.13	7,270	0.12
unclassified		42,464	1.99	31,609	1.64	43,867	2.27	117,940	1.96

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.

Toho University

Contact: Hironori Imai
E-mail: 6518002i@st.toho-u.ac.jp