多源 AS 冲突的分析与分类

孙娜[1]，丁伟[2]

（1.东南大学 网络空间安全学院，南京，211189；2.东南大学 网络空间安全学院，南京，211189；）

摘　要：论文首先对多源 AS 冲突现象进行了讨论。在此基础上，对 AS 关系进行了推导，依据自治系统间关系和路由通告原则，通过分析 BGP 路由的 AS 路径属性来发现违反 AS 关系的路径，依据自治系统间关系发现前缀委托，提出了对于检测到的多源 AS 冲突的进一步分类方案。

关键词：BGP 协议；自治系统；AS 连接关系；无效路由

Analysis and Classification of Multiple Origin AS Conflicts

Sun Na[1], Ding Wei[2]

(1. School of Cyber Science and Technology, Southeast University, Nanjing 211189;

2. School of Cyber Science and Technology, Southeast University, Nanjing 211189)

Abstract: The dissertation had discussion over the phenomenon of multiple origin AS conflicts. On this basis, the AS relationship is deduced. According to the relationship between autonomous systems and the principle of route advertisement, the path violating the AS relationship is found by analyzing the AS path attributes of BGP routes. The prefix delegation is found according to the relationship between autonomous systems. A further classification scheme for detected multiple origin AS conflicts was proposed.

Key words: BGP protocol; autonomous system; the AS connection relationships; invalid route

1 绪论

Internet 由大量的自治系统（Autonomous System，简称 AS）组成，一个自治系统是同一机构网络的集合，也是接入互联网的基本单位。每个自治系统都有唯一的自治系统号 ASN（Autonomous System Number），一开始 ASN 由两个字节组成，理论上取值范围为 1-65535，2009 年 1 月后增加到了四字节。每一个互联网用户都置身于 AS 内，比如 CERNET 的 ASN 为 4538，那么 CERNET 的用户就置身于 4538 这个自治系统内，如果用户访问的服务器也是在这个 AS 内，那双向的流量都在这个自治系统内穿梭。

自治系统之间会使用 BGP（Border Gateway Protocol）路由协议来交换各自的 IP 路由表，ASN 就是 BGP 协议用来辨识不同自治系统的唯一标识，在交换的路由表信息里体现。在 BGP 协议中，每条路由通告消息都包含地址前缀和 AS 序列，AS 序列表明通向目标前缀的路由所经过的 AS。

由于最初的 BGP 协议没有考虑路由信息的安全性问题，建立在所有的 AS 都是彼此信任的基础上，没有有效的机制来证明交换路由信息的有效性，经常能发现很多异常现象。多源 AS（Multiple Origin AS，简称 MOAS）是导致异常的原因之一，本文将对 MOAS 冲突进行解释，说明其合法性与非法性，并分析和分类 MOAS 冲突。

基金项目：国家重点研发计划（2018YFB1800200）：互联网基础行为测量与分析

作者简介：丁伟，（1962-），女，教授，E-mail: wding@njnet.edu.cn；孙娜，（1994-），女，硕士研究生，E-mail: nsun@njnet.edu.cn.

2 自治系统关系

2.1 自治系统间关系

自治系统根据彼此之间签订的商业服务合同，形成了不同的依赖关系，这个关系决定了 AS 间的路由策略，这一关系随着互联网的商业化发展应运而生。主要包括客户-提供者关系（customer-to-provider），提供者-客户关系（provider-to-customer），对等者关系（peer-to-peer）和兄弟关系（sibling-to-sibling）。

如果用无向图 G=（V，E）表示 Internet，其中，V 表示自治系统，E 表示自治系统间的连接，则 AS 间的定义如下。

定义 2.1 对∀u, v∈V，且{u, v}∈E，如果 v 从 u 购买接入 Internet 的服务，利用 u 的资源访问 Internet 上的其他网络，这时称 v 与 u 为客户-提供者关系（customer-provider，简称 C2P）；称 u 为提供者，v 为客户。反之，如果 u 为 v 提供有偿连接服务，称之为提供者-客户关系（provider-to-customer，简称 P2C）。

定义 2.2 对∀u, v∈V，且{u, v}∈E，如果 u 和 v 之间相互为对方提供无偿的针对各自内部网络以及各自客户网络的访问服务，这时称 u 与 v 为对等者关系（peer-to-peer，简称 P2P）。

定义 2.3 如果两个 AS，相互之间提供接入服务，这种关系有时也称为兄弟关系（sibling-to-sibling，简称 S2S）。具有兄弟关系的两个 AS 往往属于同一个 ISP 或具有相同的提供者。

在对等关系中，两个对等体通常是两个较大的 ISP，每个 ISP 拥有一定的客户，如果这两个 ISP 传输流量的不少部分是去往其他 ISP 的直接相连的客户，这两个 ISP 就可能签订一种对等协议，两个 ISP 之间不用互相付费而各自的用户可以互相访问。而兄弟关系中，两个较小的自治系统由于经费的原因，愿意为对方提供一个备份通道，这样当一个自治系统到他的提供者之间的连接失效时仍然可以与 Internet 相连。

2.2 BGP 路由输出原则

自治系统根据营运模式和价格模式所体现的商业关系来制定自身的路由策略，即路由策略应该与自治系统之间的关系相一致。只有当 AS1 愿意 AS2 利用它的资源去访问某些网络时，AS1 才把到目的网络的路由通告给 AS2。Huston[4]给出了配置路由输出策略时需要遵守的原则：

（1）输出给一个提供者：当一个客户向提供者通告路由信息时，作为客户的自治系统可以输出自己的路由和它客户的路由，但不能输出从其他提供者或对等者获得的路由。

（2）输出给一个客户：当提供者向客户通告路由信息时，作为提供者的自治系统可以输出自己的路由和它客户的路由，也可以输出从其他提供者或对等者获得的路由。

（3）输出给一个对等者：当与对等者交换路由信息时，可以输出自己的路由和客户的路由，但不能输出从其他提供者或对等者获得的路由。

2.3 路由扩展原则

定义 2.4 prefix(u)为自治系统 u 所拥有的前缀。

定义 2.5 把从提供者获得的路由称为提供者路由，记为 P，类似可以得到客户路由、对等者路由和兄弟路由，分别记做 C、R 和 S，用 ε 表示空路径，即不存在到目的网络的路径。

定义 2.6 提供者到客户的边称为提供者边，用 l_p 表示；从客户到提供者的边称为客户边，用 l_c 表示；连接对等者的边称为对等边，用 l_r 表示；连接兄弟的边称为兄弟边，用 l_s 表示。

表 1 路由扩展原则

	P	R	C	S	ε
l_p	P	P	P	P	P
l_r	Φ	Φ	R	R	R
l_c	Φ	Φ	C	C	C
l_s	P	R	C	S	S

根据路由输出原则，可得到表的路由扩展原则，其中第一行为路由类型，第一列为边的类型。例如：第二行第二列的“P”表示提供者路由可以沿着提供者边通告，得到一个提供者路由，“Φ”表示相应的路由扩展不允许，如：提供者路由不能沿着客户边通告。

2.4 AS 关系推导

主要依靠 No-Valley 准则，即无谷准则，最先由 Gao[3]在 2001 年提出，该准则用于自治系统间的路由策略，这个准则估计 P2C 和 P2P 关系的路由信息交换方向。这个准则有四个小项：

准则一：一条 AS 路径中最多只有一条 P2P 连接；

准则二：一条 AS 路径中，如果有一条 P2C 连接，它后面就不可能是 C2P 连接，只可能是 P2C 或 S2S 连接；

准则三：P2C 连接后不可能是 P2P 连接；

准则四：P2P 连接后不可能是 C2P 连接，只可能是 P2C 或 S2S 连接。

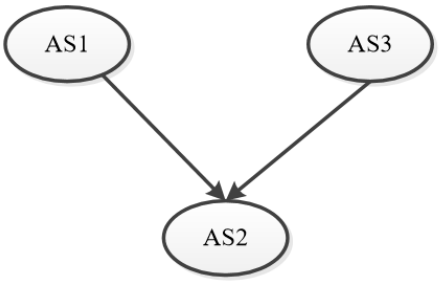

图 1 No-Valley 准则下的 AS 路径

例如，图 1 中假设 AS1 和 AS2 是 P2C 关系，AS2 和 AS3 是 C2P 关系，那这条路径{AS1，AS2，AS3}就是一条无效路径，因为 P2C 连接之后不可能是 C2P 连接，这就是 No-Valley（无谷）准则这个名字的由来。

3 MOAS 冲突的分类方案

3.1 MOAS 定义

多源 AS 冲突是指一个 IP 前缀由多个 AS 发起，即有多个源 AS 对前缀 P 进行了宣告。假如有这样两条宣告同一条前缀的路由的 AS-PATH 属性：

$$asph_1=\{p_1,p_2,\ldots,p_n\}$$

$$asph_2=\{q_1,q_2,\ldots,q_n\}$$

那么当 $p_n \neq q_n$，那么我们称发生了多源 AS 冲突现象。比如，前缀 1.6.136.0/24 有{2497 6453 9583i}和{2497 2914 9583 132215i}两条 as PATH，表示 AS9583 和 AS132215 都对此前缀进行了宣告，这就是多源 AS 冲突现象。

3.2 MOAS 冲突的合法性与非法性

一般来说，一条前缀只能由一个 AS 合法地宣告，但在实际的 BGP 路由表中，MOAS 异常出现的比例并不低。MOAS 有可能预示潜在的前缀劫持，对其进行检测可以有效地发现潜在的前缀劫持事件。

MOAS 可能会导致前缀劫持，造成互联网路由混乱。这主要是由于 BGP 在安全方面存在着设计缺陷，即 BGP 无法对路由信息的真实性和完整性进行验证。MOAS 只是 IP 劫持的一种可能。但在有些情况下，MOAS 的存在是合理的。图 2，3 描述了两个这种情况下最常见的实例。

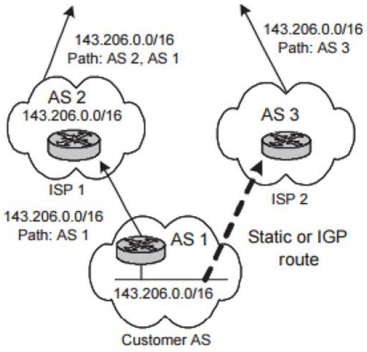

图 2 合法 MOAS：使用静态链接的多宿主

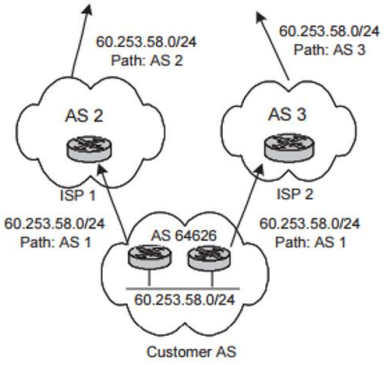

图 3 合法 MOAS：使用私有 AS 的多宿主

不合法的情况可能是由于 IP 前缀劫持和路由器配置错误，如图 4：

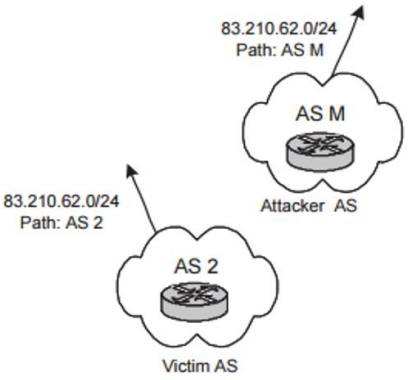

图 4 非法 MOAS：前缀劫持

其他不太常见的合法 MOAS 的原因很有很多，比如地址聚合和 IP 任播等，但是由于缺乏关于地址所有权的权威信息，仅观察 MOAS 例子，无法深入分析 MOAS 现象。

3.3 MOAS 冲突的分类

虽然期望 MOAS 冲突只是高度期望和合理配置的副作用，但非法冲突导致路由中断是网络运行中非常严重的事故。即使大多数事件的范围非常有

限，并且只涉及局部的地址空间，但仍会影响大量的 AS 及其服务。这使我们尽快、尽早发现非法的 MOAS 冲突成为一项重要的工作。为了能够准确识别 MOAS 冲突，本文将其为以下五类：

（1）无效路由（非法 IP）：此类主要是指一个 AS 通告了私有地址、未被分配的 IP 地址。

（2）无效路由（AS 路径无效）：自治系统根据商业关系制定路由策略，一个 AS 只有愿意为某个 AS 承载到目的网络的流量时，才向该 AS 通告路由。路由输出策略在送出路由更新信息之前对路由进行过滤和属性修改。如果路由输出违反路由输出策略，那么路由的发送者就会无偿转发到目的网络的流量，浪费网络资源。

（3）使用私有 AS 的多宿主：为了防止 AS 号用尽，建议多宿主的客户使用所有的提供商都公认的私有 AS 号，如果部署成功，这个方法就会产生多源 AS 冲突现象，因为 UPDATE 更新消息中这个私有的 AS 号会被上级的服务提供商剥掉，真正的源 AS 信息就丢失了。

（4）前缀委托：提供商 AS 将其地址空间的子范围委托给客户系统，提供者 AS 产生某些 IP 前缀，客户 AS 产生相同或特定（子）前缀，所涉及的 AS 保持提供者-客户关系，则已识别的 MOAS 冲突可以归类为合法的前缀委托。

（5）其他：未被归于以上类别的可疑 MOAS 记录。

4 分类方案的实施与结果

4.1 方案实施数据来源

4.1.1 Route Views 项目

Route Views 项目是由 Oregon（俄勒冈）大学开展的项目，这个项目设计的初衷是作为一个工具从不同位置为网络运营商获得实时信息，从而对全球路由系统从几个不同的角度来解释。

Route Views 监测效果受限于数据采集点的数量和覆盖范围，运营商出于保护商业隐私的考虑,很少有 AS 愿意无条件地公开自己的 BGP 数据。绝大多数 Route Views 的采集点都仅公开了部分路由数据，所以该方法得到的 AS 级拓扑数据不尽完善，只反映了全球的部分 AS 级网络拓扑信息，但该项目的研究成果依然受到很多其他机构的认可。

4.1.2 分类方案实施数据

本文分类方案的实施数据选取了 Route Views 项目五个采集点的 BGP 路由表，经处理后检测出的 MOAS 冲突记录，约为 11 万条，每条 MOAS 冲突记录是一个三元组(IPb, IPe, asn)，其中 IPb 代表地址前缀也就是 IP 地址段首地址，IPe 是 IP 地址段尾地址，asn 表示程序处理后得到的宣告此地址前缀的自治系统号码集合，包含 2 个或多个 ASN。

4.2 AS 关系库的建立

本文从多个 BGP 路由表进行 AS 关系推导，获得相对稳定的 AS 关系库。由于申请地址空间和邻居协商连接关系要很长时间，并且 AS 也不可能总是改变与邻居的关系，所以 AS 的地理位置和邻居关系会在很长时间保持相对稳定，这种相对稳定为检测路由有效性提供了可能。

根据 GAO 的启发式算法，对 BGP 路由表进行处理，得到 peer-to-peer 和 provider-to-customer 关系对约 36 万条，最终 AS 关系库示例如表 2 所示：

表 2 AS 关系实例

AS1	AS2	rel
34572	39351	0
34572	39830	-1
34572	42308	-1
34572	43531	0
34572	49605	0
34572	50036	-1
34572	51706	0

其中 AS1、AS2 代表不同的自治系统号码，rel 表示自治系统间的关系，rel 如果等于 0，代表 AS1 和 AS2 为 peer-to-peer 关系，rel 如果等于-1，代表 AS1 和 AS2 为 provider-to-customer 关系，且不是 customer-to-provider 关系。

4.3 实施分类方案

4.3.1 无效路由（非法 IP）

定义 4.1 保留地址，主要包括未被分配地址、私有地址和组播地址等，此集合记为 RA，包含以下地址段：[0.0.0.0/8, 10.0.0.0/8, 100.64.0.0/10, 127.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.0.0.0/24, 192.0.2.0/24, 192.31.196.0/24,

192.52.193.0/24, 192.88.99.0/24, 192.168.0.0/16, 192.175.48.0/24, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24, 240.0.0.0/4, 255.255.255.255/32]。

故此类的判定规则为：

$$[IPb, IPe] \cap RA \neq \Phi$$

4.3.2 无效路由（AS 路径无效）

设节点 v 和节点 u 为两个相邻节点，u 接收 v 输出路由 r。无效路由检测算法如下：

（1）u 接收来自 v 的路由 r；

（2）如果路由 r 的 AS 路径长度是 1，且前缀属于 v，该路由有效。

（3）否则，如果 AS 路径长度大于 1，根据 AS 关系，对 AS 路径内的 AS 序列进行检测，如果构成 AS 路径的 AS 链路符合 AS 关系，转到（4）。

（4）如果 AS 路径内的链路符合路由输出原则，则该路由有效。

（5）如不符合以上条件，则为无效路由。

按照上述无效路由检测算法，对于 MOAS 冲突记录中的每一个路由，回到 BGP 路由表提取其 AS 路径属性值，分解出其 AS 链路，按照无效路由检测算法，判定出 AS 路径无效的无效路由 MOAS 冲突。

4.3.3 使用私有 AS 的多宿主

定义 4.2 私有 ASN，类似于私有 IP 地址，不能用于公网，范围是 64512-65534，此集合记为 PA，故此类的判定规则为：

$$asn \cap PA \neq \Phi$$

4.3.4 前缀委托

查询 AS 关系库，MOAS 记录中所涉及的所有 AS 保持提供者-客户关系或客户-提供者关系，则已识别的 MOAS 冲突可以归类为合法的前缀委托。

4.3.5 其他

未被归于以上类别的 MOAS 冲突记录则被分为此类。

4.4 分类方案结果

经过 4.3 节分类方案实施后，结果如下：

（1）无效路由（非法 IP）

表 3 无效路由（非法 IP）

IPb	IPe	asn
192.88.99.0	192.88.99.255	1103,53704,6939

此类仅有一条 MOAS 记录。

（2）无效路由（AS 路径无效）

检测到的 AS 路径无效的无效路由 MOAS 记录示例如下：

表 4 无效路由（AS 路径无效）

地址前缀	AS path
24.246.0.0/17	701 7018
24.246.128.0/18	701 7018
192.40.105.0/24	701 1299 1759 12582
66.117.8.0/24	4637 174
69.31.152.0/24	4637 4436 26627
198.23.26.0/24	1239 4390
192.188.208.0/20	1239 4390

此类得到的 AS 无效路径大约是 BGP 路由表的 1.3%。

（3）使用私有 AS 的多宿主

检测到的使用私有 AS 的多宿主的 MOAS 记录示例如下：

表 5 使用私有 AS 的多宿主

IPb	IPe	asn
5.104.168.0	5.104.169.255	65502,57344
31.148.150.0	31.148.150.255	65001,44546,61031
31.171.126.0	31.171.127.255	65456,199311
41.215.130.0	41.215.130.7	64515,36866
41.215.135.0	41.215.135.127	64515,36866
47.228.0.0	47.228.11.255	65150,7224
47.228.12.0	47.228.12.255	65400,7224
66.74.160.0	66.74.175.255	65400,20001,7224

此类共有 38 条 MOAS 记录。

（4）前缀委托

检测到的前缀委托的 MOAS 记录示例如下：

表 6 前缀委托

IPb	IPe	asn
1.6.136.0	1.6.136.255	132215,9583
1.24.32.0	1.24.39.255	4837,139007
1.24.80.0	1.24.39.0	4837,139007
1.44.0.0	1.44.7.255	7474,4804
1.81.0.0	1.81.7.255	134768,4134

2.188.22.0	2.188.22.255	12880,49666,48159
5.149.139.0	5.149.139.255	6696,49964,48844

此类共有 36783 条 MOAS 记录。

5 结论

MOAS 冲突可能是合法的，也可能是不合法的。能够检测到 MOAS 冲突，并对其合法性进行判断，有助于及时发现路由中断，提高 BGP 的健壮性。由于 MOAS 冲突影响了大量前缀，因此自动检测和分类是非常必要的。从长远看，我们希望能够对可以观察到的大多数 MOAS 冲突给出更加合理的解释。

参考文献：

[1]Rekhter Y,Li T.RFC 1771:A Boarder Gateway Protocol(BGP version 4)[S].March 1995.

[2]The route views project.[EB/OL](2008-1-12) http://www.routeviews.org/routeviews/.

[3]Gao L X. On inferring autonomous system relationships in the Internet[J]. IEEE/ACM Transactions on Networking,2001,9(6):733~745.

[4]Huston G. Interconnection, peering, and settlements.[EB/OL](2007-9-21) http://www.potaroo.net/papers/1999-6-peer/peering.pdf.

[5] 银伟, 胡湘江, 朱培栋. 多源 AS 冲突问题研究与 MOAS LIST 机制实现[J]. 计算机工程与设计, 2008, 29(8):1910-1912.

[6] Zhao X , Pei D , Wang L , et al. An analysis of BGP multiple origin AS (MOAS) conflicts[C]// Acm Sigcomm Workshop on Internet Measurement. ACM, 2001.

[7] 胡照明, 刘磊, 尚博文, et al. 一种 AS-IP 宣告关系真实性评估方法研究[J]. 信息网络安全, 2015(11):33-39.

[8] Sankar A U P, Poornachandran P, Ashok A, et al. B-Secure: A Dynamic Reputation System for Identifying Anomalous BGP Paths[J]. 2017.

[9] Zhang J, Rexford J, Feigenbaum J. Learning-based anomaly detection in BGP updates[C]// ACM Workshop on Mining Network Data, Minenet 2005, Philadelphia, Pennsylvania, Usa, August. DBLP, 2005:219-220.

[10] Zhang G, Zhang D, Lu L, et al. A Framework for the Analysis of BGP Data over Long Timescales[C]// International Conference on Future Internet Technologies. ACM, 2016:104-108.

[11] Chin K . On the Characteristics of BGP Multiple Origin AS Conflicts[C]// Australasian Telecommunication Networks & Applications Conference. IEEE, 2008

[12] Zhao X , Pei D , Wang L , et al. Detection of Invalid Routing Announcement in the Internet[C]// International Conference on Dependable Systems & Networks. IEEE, 2002..

[13] Jacquemart Q , Urvoykeller G , Biersack E . A Longitudinal Study of BGP MOAS Prefixes[M]// Traffic Monitoring and Analysis. Springer Berlin Heidelberg, 2014.