doi: 10.3969/j.issn.1005-3026.2017.04.008

Internet 路由前缀宣告的特征挖掘与分析

邓文平, 李竹村, 王 宏, 高先明
(国防科学技术大学 计算机学院, 湖南 长沙 410073)

摘 要: 基于大量的历史 BGP 路由表快照,对 BGP 路由宣告信息进行深度挖掘. 提出了前缀宣告稳定性度量方法,验证了绝大多数路由宣告是稳定的,历史上发生的路由劫持事件都是瞬时的(不具备稳定性);设计了前缀宣告的相似性测度算法,对大量历史 BGP 路由宣告进行了分析,结果表明大多数大型 AS 宣告的路由前缀具有自相似性,即,同一个 AS 宣告的多个路由前缀有一定的连续性. 基于以上两个特征,从历史路由信息中可进一步提取前缀宣告的可信集,构造 BGP 路由宣告的可信知识库,为后续的路由前缀劫持检测和路由安全监测提供依据.

关 键 词: 前缀宣告;AS;路由前缀劫持;RouteViews;特征挖掘
中图分类号: TP 393.08 **文献标志码**: A **文章编号**: 1005-3026(2017)04-0492-05

Characteristics Mining and Analysis for Internet Prefix Announcements

DENG Wen-ping, LI Zhu-cun, WANG Hong, GAO Xian-ming
(School of Computer, National University of Defense Technology, Changsha 410073, China. Corresponding author: DENG Wen-ping, E-mail: wsfdwp@163.com)

Abstract: The BGP routing information was dogged deeply on the basis of a large number of the history of BGP routing table snapshot. A method to measure stability of prefix announcements was designed, it was verified that vast majority of routing announcement was stable, and the historical routing hijacking was short lived (without stability). A similarity measuring algorithm of prefix announcement was presented, and a large number of the history BGP routing announcements were analyzed. The results showed that the announced prefixes of most large ASes are in line with the property of self-similarity, i.e., the same AS declaring multiple routing prefixes with certain continuity. A trustworthy set of prefix-AS mapping was extracted on the basis of these two characteristics, and a trustworthy knowledge base of BGP routing announcement was designed to provide the basis for prefix hijacking detection and routing security monitoring.

Key words: prefix announcement; autonomous system; prefix hijacking; RouteViews; characteristics mining

Internet 以自治系统(autonomous system, AS)为单位进行管理[1],每个自治系统有全局唯一的 AS 号标识. AS 内部使用域内路由协议交换路由信息,如 ISIS[2]等;AS 间使用域间路由协议交换路由信息,目前大多数 AS 是使用边界网关协议(border gateway protocol, BGP[3])交换各自的网络可达信息,最新版本是 BGP-4.

BGP 存在的设计缺陷主要分为两个方面:

1) BGP 协议无法保证路由前缀宣告的完整性. BGP 协议漏洞包括 BGP 本身的漏洞及其他协议带来的漏洞[4]. BGP 本身的安全漏洞带来的攻击包括重放攻击、消息注入攻击等;其他协议如 TCP 安全漏洞带来的攻击及 SYN 洪泛攻击等.

2) BGP 协议默认接收 AS 宣告的全部路由宣告,AS 默认接收 BGP 协议通告全部路由宣告. BGP 和 AS 本身都没有额外的安全机制来对路由

收稿日期: 2015-04-29
基金项目: 国家自然科学基金资助项目(61202486,61472438).
作者简介: 邓文平(1981-),男,湖南耒阳人,国防科学技术大学博士研究生; 王 宏(1964-),男,湖南益阳人,国防科学技术大学研究员.

前缀的合法性进行验证.

这两个方面的问题很容易让一个 AS 可随意发布其他 AS 拥有的前缀,形成前缀劫持攻击. 多年来,前缀劫持攻击现象经常发生,许多大规模的网络瘫痪事故都与路由前缀劫持有关,如 2012 年的加拿大路由泄露事件[5]. 前缀劫持攻击是当前 Internet 域间路由系统所面临的最严重的安全威胁之一,目前仍缺乏有效的防护手段.

业界防范前缀劫持攻击在控制层大致分为两大类:一类是路由认证技术[6]. 比如:利用数字签名机制如 S – BGP[7],清华大学的 GesBGP[8]等,或者利用路由注册思想的 IRV[9],以及基于反向 DNS 的 ROVER[10]等. 另一类是增加额外监测机制的前缀劫持检测技术,如通过统计路由数据在发生异常时给用户发出警报的 Cyclops[11]. 前者在部署上存在一定的难度,并且在密钥的管理上易产生新的漏洞;后者存在冒称前缀所有权的可能. 此外,部分研究者提出了信任机制来提高域间路由抵御路由前缀劫持的能力,如国防科大胡宁等提出的基于信任机制的域间路由协同管理方法[12]信任值的产生以及检测准确性方面存在的挑战. 文献[13]对现有安全路由机制的部分部署进行了全面分析与评估.

由于域间路由的复杂化,目前针对域间路由的安全措施或多或少存在一系列的问题,并不能完全满足需求. 检测和发现路由劫持等异常路由的关键在于构建一个可信的知识库. 目前的检测知识库都是基于 RIR/IRR 数据. Internet 对于网络资源的管理和分配是通过 RIR(regional Internet registry)进行的, IRR(Internet routing registry)允许每个 ISP 在此注册自己的路由策略和规则. 但是,资源一旦分配给具体运营商后,网络运营商可独立对网络资源进行再分配. 并不是所有的 ISP 情愿发布自己的路由策略到 IRR 上,而 Internet 对于并没有强制要求 ISP 网络资源再分配的时候到 IRR 登记. 因此,IRR/RIR 数据存在“不新鲜、不完整、不准确”的问题,导致基于 RIR/IRR 数据的知识库的路由劫持检测的准确性和实时性不高. 构造一个可信的路由知识库仍然是异常路由监测系统和路由安全监测系统面临的关键性挑战.

本文通过统计和分析大量的历史 BGP 路由表快照,对 BGP 路由前缀宣告信息进行深度挖掘,提取验证路由宣告的特征,进一步用于提取前缀宣告的可信集,构造 BGP 路由前缀宣告的可信知识库,为后续的异常路由监测和安全监测提供信息支撑.

1　实验方法

1.1　BGP 路由表

由于 TCP 提供可靠传输机制,BGP 使用 TCP 协议作为承载协议,端口号为 179. BGP 采用“增量式”的更新机制,通过 OPEN 报文建立邻居,KEEPALIVE 维持邻居,UPDATE 更新维护路由信息,NOTIFICATION 通知对端检测到错误. AS 通过使用 BGP 协议向它的邻居 AS 宣告 IP 地址前缀,并且将它从邻居 AS 学到的路由信息传播给其他的邻居 AS. 图 1 给出了 RouteViews[14]下载的 BGP 路由表实例.

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	0.0.0/0	95.140.80.254	0	0	0	31500 30751 i
*	0.0.0/0	96.4.0.55	0	0	0	11686 19151 i
*	1.9.0.0/16	4.69.184.193	0	0	0	3356 1273 4788 i
*	1.9.0.0/16	213.248.83.252	0	0	0	1299 1273 4788 i
*	1.9.0.0/16	129.250.0.11	302	0	0	2914 4788 i
*	1.9.0.0/16	12.0.1.63	0	0	0	7018 4788 i
*	1.9.0.0/16	147.28.7.1	0	0	0	3130 2914 4788 i
*	1.9.0.0/16	144.228.241.130	0	0	0	1239 7018 4788 i
*	1.9.0.0/16	147.28.7.2	2	0	0	3130 2914 4788 i
*	1.9.0.0/16	202.232.0.3	0	0	0	2497 2914 4788 i
*	1.9.0.0/16	85.114.0.217	0	0	0	8492 9002 3549 4788 i

图 1　BGP 路由表

Fig. 1　BGP routing table

每个 BGP 路由器会维护一个与图 1 类似的路由表,路由表中包含着到目的网络的路径信息. 每条路由条目中包含以下属性:Network 表示目的网络前缀;Next Hop 表示下一跳的 IP 地址;Metic 表示度量值;LocPrf 表示本地优先级;Weight 为 cisco 私有参数;Path 表示 AS 路径信息. 在通常情况下,一条路由记录中,Path 属性从左到右表示从当前 AS 出发到达目的 AS 所要穿越的 AS,因此,Path 最右边的 AS 号即为目的网络的源宣告者. 图 1 的第三条记录中,从当前 AS 到目的网络 1.9.0.0/16,需要穿越 AS 3356 和 AS 1273 之后,到达目标网络所在 AS 4788,则 AS 4788 就是目的网络的源宣告者.

1.2　IP – AS 映射活跃度的构造方法

定义 1 活跃度(ActiveString):假设样本 A 中共有 n 个路由表,若 IP – AS 映射 p 在第 k 个路由表中出现,则该映射活跃度的第 k 位为 1,反之,如果没有出现,则为 0.

活跃度可以反映 IP – AS 映射在样本中的出现规律. 根据数据源的路由表构造 ActiveString 的过程,就是统计 IP – AS 映射在该样本中的出现时间和次数. 例如前缀“1.0.0.0/24”与 AS 15169 的映射在 2014 年 1 月份每天的第一个路由表中

均有出现,则该映射的 ActiveString 为 11111111111111111111111111111111. 根据路由表快照构造 IP – AS 的 ActiveString 过程大概分为以下几个步骤:

1)遍历所有的路由表,从路由表中提取所有的 IP – AS 映射;

2)如果在 k 路由表中出现该 IP – AS 映射,则当前第 k 位置为 1,反之,置为 0.

1.3 IP – AS 映射的稳定性计算方法

IP – AS 映射的稳定性计算基于 ActiveString,主要是通过对 ActiveString 进行处理,统计从第一次出现到最后一张表映射的出现次数,得到 IP – AS 在该样本空间的稳定性参数. 假设一组给定的 IP – AS 映射,在 ActiveString 中,它的出现次数为 n,第一次出现位置为 1,样本空间大小为 c,则该映射的稳定性 v 为

$$v = n/(c - l + 1). \tag{1}$$

映射出现的次数越多,参数越大,表示该映射越稳定,显然,越稳定的映射,其一定程度上可信度越高. 例如,前缀"1.0.0.0/24"与 AS 15169 映射的 ActiveString 为 1111111,则该映射的稳定性值是 1. 基本计算过程如下:

1)读取 ActiveString,统计映射出现的次数及第一次出现的位置;

2)根据公式计算映射稳定性.

1.4 路由前缀宣告的变化性测度方法

通过统计路由表之间的差异来测度路由宣告的变化性,检测域间路由的异常. 路由表的变化分为两种情况:一种是减少的前缀宣告;一种是新增的前缀宣告. 假设定义样本中第 k 个表中 IP – AS 映射的集合为 A,第 $k+1$ 个表中 IP – AS 映射的集合为 B,则减少的前缀宣告为 $A - B$,数目为 $(|A - B|)$,减少的比例为 $(|A - B|)/(|A|)$,称之为差集;反之,新增的前缀宣告为 $B - A$,数目为 $(|B - A|)$,新增的比例为 $(|B - A|)/(|B|)$,称之为反差集. 通过统计路由表中前缀宣告的增减,计算差集与反差集,得到路由表的变化规律. 显然差集越小,稳定性越高,路由表的变化就越小. 该计算的基本过程如下:

1)读取第 k 个表得到路由表 k 中的 IP – AS 映射 A;

2)读取第 $k+1$ 个表得到路由表 $k+1$ 中的 IP – AS 映射 B;

3)计算差集与反差集.

1.5 路由前缀宣告的相似性测度方法

通过统计历史路由表信息,得到路由表中每个 AS 宣告的地址块. RIR 分配多个地址块给运营商,运营商将地址块再次划分为多个小的地址块分配给其他 AS. 因此,AS 宣告的前缀间存在一定的内在联系,即存在一定的相似性. 从另一方面可以看出,如果路由表中新出现一个 IP – AS 映射,而在该 AS 宣告的地址块中不存在一个相似度极高的前缀路由宣告,且稳定性高,则新出现的 IP – AS 映射的可信度存在一定的问题.

定义 2 前缀路由宣告的相似性:假设 AS1 宣告两个前缀 p 和 q,长度分别为 m 和 n,而 p 和 q 的最长父前缀长度为 len,则 p 和 q 的相似度 s 为

$$s = \text{len}/((m+n)/2). \tag{2}$$

计算路由前缀相似度的实现过程见图 2.

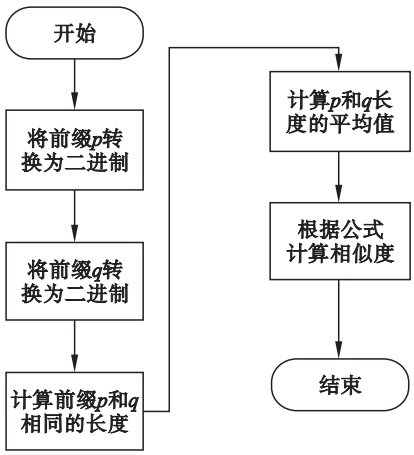

图 2 计算路由前缀相似度流程图

Fig. 2 Flow chart of computing route prefix similarity

统计路由表中每个 AS 的路由前缀宣告的相似度的基本过程如下:

1)读取路由表中的每个 AS 宣告的地址块,遍历每个 AS 的每个地址块;

2)根据公式计算每个地址块与其他所有地址块的相似性,并记录每个地址块与其他地址块的最大相似度.

该计算的实现过程如图 3 所示.

2 结果与分析

2.1 数据源

本文实验数据来自于 Oregon 大学的 RouteViews 项目[14]. 实验所使用的四组数据分别是 2005 年 1 月到 2014 年 12 月、2014 年 1 月 1 日到 2014 年 12 月 31 日、2014 年 12 月 1 日到 2014 年 12 月 31 日、2014 年 1 月 1 日. 其中第一组数据使用每月第一个路由表作为一个月数据的代表;第二组和第三组数据使用每天第一个路由表作为

当天的数据代表;第四组数据为全天所有的路由表.

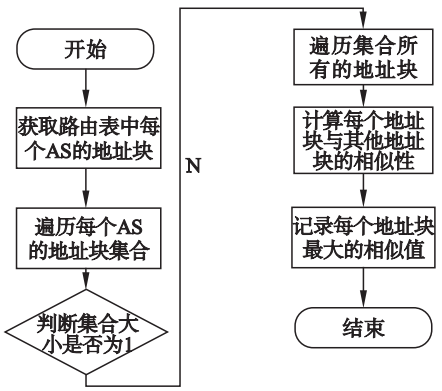

图 3　统计 AS 路由前缀相似度流程图

Fig. 3　Flow chart of counting prefix similarity of AS

2.2　路由宣告稳定性统计分析

通过用统计的分析方法分析样本数据,得到以下结果:①2005 年到 2014 年 10 年期间的 IP – AS 映射的稳定性分析结果表明,大概有 50 万条 IP – AS 映射在 10 年时间的样本里是非常稳定的. ②2014 年 365 天的路由表统计分析结果表明,45 万多条 IP – AS 映射在 1 年中每天同一个时间点稳定出现. ③2014 年 12 月的路由历史信息统计结果表明,有 54 万多条 IP – AS 映射在该月内同一个时间出现,是非常稳定的. ④2015 年 1 月 1 日全天的前缀稳定性分析结果表明,在一天的时间里,99. 7% 的 IP – AS 前缀是稳定的,约 63 万条 IP – AS 在一天的时间内会在路由表中连续出现.

综上,绝大多数 IP – AS 映射是非常稳定的,出现的时间段是相对规律的,不稳定的 IP – AS 映射所占比例相对较小. 并且样本时间间隔越短,IP – AS 映射相对更加稳定.

2.3　路由宣告变化性测度分析

利用自相似的分析方法分析样本的正反差集,得到以下结果.

图 4 是 2014 年的 IP – AS 映射的差集与反差集统计图. 结果表明,2014 年路由表整体稳定,在 2014 年 11 月 5 号时,差集和反差集达到最高峰. 意味着,在 2014 年 11 月 6 日较 11 月 5 日,新增了较大数量的 IP – AS 映射.

2.4　路由宣告相似性测度分析

利用自相似性的分析方法分析 2014 年 11 月 6 日全天的历史路由信息,如图 5 所示. 分析结果显示,AS 宣告的地址块中,大约 41 万条前缀宣告在宣告该前缀的 AS 中存在相似度 90% 以上的前缀宣告,占总前缀宣告的 74% ;其中 29 万多条前缀宣告在宣告该前缀的 AS 中存在相似度 95% 以上的前缀宣告,占总前缀宣告 52% ;大约只有 0. 49 万条前缀宣告在宣告该前缀的 AS 中存在相似度 5% 以下的前缀宣告,占总前缀宣告的 0. 89% ;大约 2. 7 万个 AS 在该路由表中只出现一个路由宣告(大约 4%).

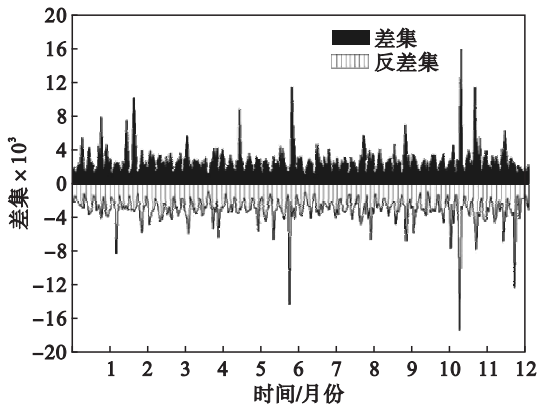

图 4　2014 年路由表差集

Fig. 4　Difference set of routing table during 2014

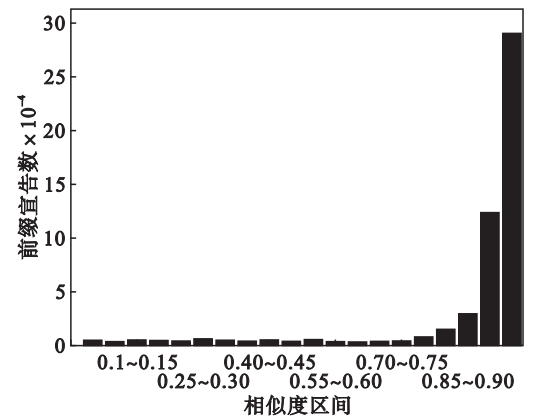

图 5　2014 年 11 月 6 日前缀相似性

Fig. 5　Prefixes self-similarity analysis during november 6th in 2014

实验表明,对于大部分 AS 宣告的一个地址块,存在它宣告另外一个地址块与当前地址块具有很高的相似性,即,同一个 AS 宣告的多个路由前缀有一定的连续性.

3　结　　论

相较于 RIR/IRR 数据,对历史 BGP 路由表快照进行分析得到的数据更为真实,可信度高;而针对短时间内新的路由前缀,利用路由前缀之间的相似性判断路由前缀宣告的可信、实时性程度高. 通过分析历史路由信息,挖掘路由前缀宣告的特征及对路由前缀宣告进行可信性分析,可构建一个高效、实时、准确的知识库,为检测路由劫持

提供信息支撑.

参考文献:

[1] Chen Y, Datta A K, Tixeuil H, et al. Stabilizing inter-domain routing in the Internet[J]. *Journal of High Speed Networks*, 2005, 14(1): 21 – 37.

[2] Internet Engineering Task Force. RFC 1195: use of OSI IS-IS for routing in TCP/IP and dual environments [S]. Los Angeles: IETF, 1990.

[3] Internet Engineering Task Force. RFC 1771: a border gateway protocol 4 (BGP-4) [S]. Los Angeles: IETF, 1995.

[4] Internet Engineering Task Force. RFC 4272: BGP security vulnerabilities analysis[S]. Los Angeles: IETF, 2006.

[5] Toonk A. A BGP leak made in Canada[EB/OL]. (2012 – 08 – 02) [2016 – 11 – 26]. http://www. bgpmon. net/a-bgp-leak-made-in-canada/.

[6] 黎松,诸葛建伟,李星. BGP 安全研究[J]. 软件学报,2013, 24(1):121 – 138.
(Li Song, Zhuge Jian-wei, Li Xing. Study on BGP security [J]. *Journal of Software*, 2013, 24(1): 121 – 138.)

[7] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP) [J]. *IEEE Journal on Selected Areas in Communications*, 2000, 18(4): 582 – 592.

[8] 李琦,吴建平,徐明伟,等. 自治系统间的安全路由协议 GesBGP[J]. 计算机学报,2009(3):506 – 515.
(Li Qi, Wu Jian-ping, Xu Ming-wei, et al. GesBGP: a good-enough-security BGP[J]. *Journal of Computer*, 2009(3): 506 – 515.)

[9] Subramanian L, Roth V, Stoica I, et al. Listen and whisper: security mechanisms for BGP[C]// Proceedings of First Symposium on Networked Systems Design and Implementation. Los Angeles: ACM Digital Library, 2004: 10 – 14.

[10] Malhotra A, Goldberg S. RPKI vs ROVER: comparing the risks of BGP security solutions[J]. *ACM Sigcomm Computer Communication Review*, 2014, 44(1): 113 – 114.

[11] Chi Y J, Oliveira R, Zhang L. Cyclops: the AS-level connectivity observatory [J]. *ACM Sigcomm Computer Communication Review*, 2008, 38(1): 5 – 16.

[12] 胡宁,邹鹏,朱培栋. 基于信誉机制的域间路由安全协同管理方法[J]. 软件学报,2010,21(3):505 – 517.
(Hu Ning, Zou Peng, Zhu Pei-dong. Reputation-based collaborative management for inter-domain routing security [J]. *Journal of Software*, 2010, 21(3): 505 – 517.

[13] Lychev R, Goldberg S, Schapira M. BGP security in partial deployment: is the juice worth the squeeze? [J]. *ACM Sigcomm Computer Communication Review*, 2013, 43(1): 171 – 182.

[14] Oregon. RouteViews routing table archive [EB/OL]. (2005 – 1 – 23) [2016 – 11 – 26]. http://www. route views. org/.

(上接第 491 页)

[5] Rauhut H, Schnass K, Vandergheynst P. Compressed sensing and redundant dictionaries [J]. *IEEE Transactions on Information Theory*, 2008, 54(5): 2210 – 2219.

[6] Yang Y, Au O C, Fang L, et al. Reweighted compressive sampling for image compression [C]// Picture Coding Symposium. Chicago: IEEE, 2009: 1 – 4.

[7] Stankovic L, Stankovic S, Amin M. Missing samples analysis in signals for applications to L-estimation and compressive sensing[J]. *Signal Processing*, 2014, 94(1): 401 – 408.

[8] Gutiérrez I M, Fuentes H A. Overlapped block-based compressive sensing imaging on mobile handset devices[J]. *Revista Facultad de Ingeniería Universidad de Antioquia*, 2014(70): 173 – 184.

[9] 李然,干宗良,朱秀昌. 基于分块压缩感知的图像全局重构模型[J]. 信号处理,2012,28(10):1416 – 1422.
(Li Ran, Gan Zong-liang, Zhu Xiu-chang. A global reconstruction model of images using block compressed sensing [J]. *Signal Processing*, 2012, 28(10): 1416 – 1422.)

[10] 罗琦,魏倩,缪昕杰. 基于压缩感知思想的图像分块压缩与重构方法[J]. 中国科学:信息科学,2014,44(8):1036 – 1047.
(Luo Qi, Wei Qian, Miao Xin-jie. Blocked image compression and reconstruction algorithm based on compressed sensing[J]. *Scientia Sinica Informationis*, 2014, 44(8): 1036 – 1047.)

[11] Kapoor A, Dhir R. Image compression using fast 2-D DCT technique[J]. *International Journal on Computer Science & Engineering*, 2011, 3(6): 2415 – 2419.