学术通信

一种基于路由扩散的大规模网络控管方法

刘刚，云晓春，方滨兴，胡铭曾

（哈尔滨工业大学 计算机科学与工程系，黑龙江 哈尔滨 150001）

摘 要：针对已有的网络控管方法的缺点，提出一种基于路由扩散的大规模网络控管的新方法。阐述了其基本网络拓扑结构、动态路由协议的选取和配置等问题，并同已有的方法进行了详细对比。该方法具有路由器负担小、控制规则容量大、智能化、可扩展以及一处配置多处生效等优点，适用于大规模网络控管。

关键词：大规模网络控管；路由扩散；路由协议；访问控制；OSPF；BGP

中图分类号：TP393.08 文献标识码：A 文章编号：1000-436X(2003)10-0159-06

A control method for large-scale network based on routing diffusion

LIU Gang, YUN Xiao-chun, FANG Bin-xing, HU Ming-zeng

(Department of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150001, China)

Abstract: To overcome the disadvantages of the existing network control methods, a new control method for large-scale network based on routing diffusion is presented. This paper studies its overall structure of network topology, the selection of dynamic routing protocols as well as configuration, and compares this method with the existing methods in detail. With the advantages of less router load, more control rules, intelligence, scalability, multiple routers becoming effective by configuring only one router, and so on, the new method is adapted to large-scale network control.

Key words: large-scale network control; routing diffusion; routing protocol; access control; OSPF; BGP

1 引言

随着计算机网络技术的迅猛发展和国民经济与社会信息化的大力推进，各行政、企事业单位都建立了网络信息系统，电子政务、电子银行、电子商务、网上证券、远程医疗、远程

收稿日期：2002-01-21；修订日期：2003-03-14

作者简介：刘刚（1975-），男，辽宁沈阳人，哈尔滨工业大学博士生，主要研究方向为网络安全；云晓春（1971-），男，黑龙江牡丹江人，博士，哈尔滨工业大学教授，主要研究方向为网络安全；方滨兴（1960-），男，江西万年人，博士，哈尔滨工业大学教授、博士生导师，主要研究方向为网络安全、并行处理；胡铭曾（1935-），男，上海人，哈尔滨工业大学教授、博士生导师，主要研究方向为体系结构，网络安全。

教育等应用越来越广泛。但是，网络信息安全的问题也随之而来，前不久泛滥的“红色代码”、“尼姆达”病毒和越来越多的黑客入侵事件，使人们充分认识到网络信息安全管理的重要性和紧迫性。为了防止各种有害信息在网络上的蔓延，必须对网络上的信息进行过滤分析，并采取有效的手段阻断有害信息的传播。这就需要通过一定的网络控管方法管理网络上的关键点，控制网络特定信息的流动。尤其在大规模网络环境中，更需要一种高效可行的网络控管方法做到实时过滤和有效控制有害信息，同时不影响正常信息的流动。

网络访问控制是保障网络信息安全的重要手段。访问控制可以分为面向主机和面向网络两种类型。面向主机的访问控制的控管对象是建立在操作系统或者应用系统上面的用户，控管目标是防止非法用户进入系统以及合法用户对系统资源的非法使用。而面向网络的访问控制是指在各级组网设备上实现对网络流量的控制，控管的对象是流经网络设备的数据包，目标是阻断有害信息（数据包）的通过。从功能上来说，可以根据网络管理员对访问控制规则的配置，对流经的数据包进行多个元素的匹配（例如源和目的 IP 地址、源和目的端口等等）并按照匹配结果选择对数据包进行接收、丢弃和转发等形式的操作。从实现要点来说，就是在实现控管功能的同时要保证不影响正常流量和系统的效率。面向网络的访问控制根据所应用的网络规模又可以分为局域网的访问控制和大规模网络的访问控制，局域网的出入口路由器一般拥有相对较低的带宽，实时过滤容易实现，在具有复杂的访问控制规则配置情况下一般仍然可以达到线速匹配，不会导致系统丢包，所以在这种规模的网络上面可以完成比较丰富的控管功能。大规模网络访问控制，我们是指在 Internet 服务提供商（ISP）所管理的大规模自治域（AS）的核心路由器上面进行访问控制，而这些路由器通常拥有几十 G 乃至上百 Gbit 的核心交换容量、数十万条路由表项以及数十乃上百 MPPS 的包吞吐率等技术指标，按照常规的方法在上面实现访问控制而且要不影响路由器的高速数据交换是很困难的。

但是在大规模网络上面进行访问控制对于实现国家级的网络信息安全管理具有重要的意义，本文正是致力于给出一个解决方法。目前，实现网络访问控制[1, 2]有几种方式，但它们都存在一定缺陷而不适应大规模网络环境下的访问控制。为了避免对路由器的交换速率和对原有网络拓扑结构造成较大影响，在现有路由器上利用路由表匹配功能，进行流量控制是很好的方式。因为路由表匹配算法成熟且效率较高，不占用处理器太多资源，对路由器的性能影响较小，而且路由表具有较大的路由信息容纳量，也即可以承受较多的访问控制规则。本文即是利用高效的路由表匹配功能，提出一种基于路由扩散技术的大规模网络控管新方法。

2 基于路由扩散的大规模网络控管方法

基于路由扩散的网络控管方法就是在大规模自治域的出入口路由器上新接入一个起控管作用的子网或者 AS 域，将要受控的网络地址配置在这个子网或者 AS 域内的路由器中，这样利用动态路由协议的网络拓扑自动识别特性，在出入口路由器上将生成受控网络地址的路由信息，将自治域内部网络对这些受控网络地址的访问转入到这个控管子网或者 AS 域的网络中，从而实现对受控网络地址的流量控制。

2.1 路由扩散网络控管的网络结构

本文主要研究在大规模网络环境下的网络控管方法，图 1 给出了在一个较大规模 ISP 中进行路由扩散网络控管所采用的网络结构。其中，ISP0 是实施了网络控管的 ISP。因为 ISP 出入口路由器是不同 ISP 之间交换数据的必经路由器，所以 ISP 出入口路由器作为控制点路由器是面向 ISP 级网络控管的有效选择。从样本路由器（sr）到各个出入口路由器（or）的路

由扩散链路可以直接连接，也可以通过一级或多级的扩散路由器（kr）到达各个 or，其中如果条件允许可以建立双链路以做备份（例如从 sr 到 or4），每个 kr 也可以接到多个 or 上（例如 kr1）。扩散链路的建立主要有两种形式：1）使用专用线路，扩散速度快，稳定性高，但成本也较高；2）在公用数据网上使用加密隧道来建立虚拟链路连接，成本小，但扩散速度和稳定性相对差一些。可根据具体情况选择不同的形式实施，在这些链路上使用何种动态路由协议将在下一节阐述。

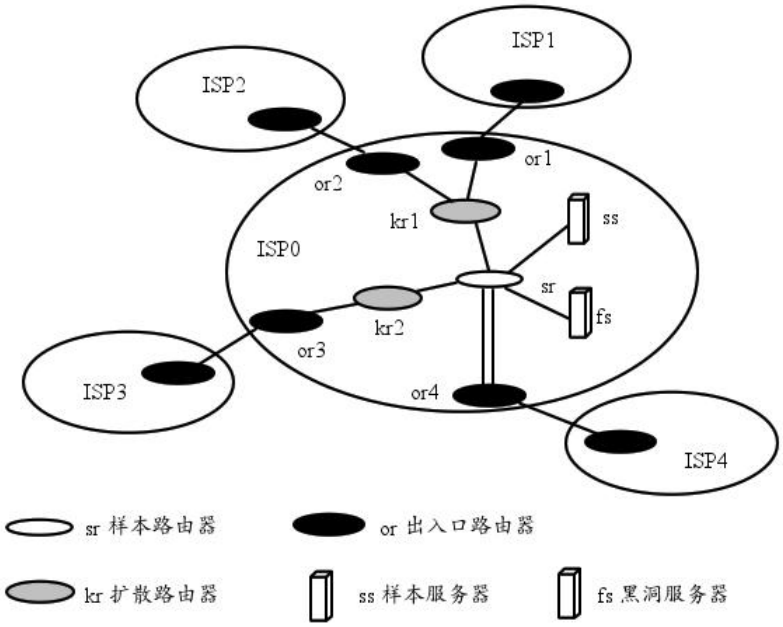

图 1　在一个 ISP 中进行路由扩散网络控管的网络结构

样本服务器（ss）连到 sr 的控制口（console），网络管理员在 ss 上录入受控网络地址 IP1，ss 上的运行程序根据受控网络地址 IP1 生成相应静态路由，该路由的目的网络地址即为受控网络地址 IP1，下一跳指向黑洞服务器（fs）的 IP 地址，并将该静态路由从控制口写入 sr 中，由 sr 经过扩散链路逐级扩散到各个 or 中，这样凡是经由各个 or 而目的网络地址为受控网络地址 IP1 的数据包都会被转发到 sr，然后由 sr 转发到黑洞服务器上。黑洞服务器可以选择直接将这些包丢弃或者做其它的处理，同时也可以据此对各种受控网络地址访问的流量进行统计和分析。这样，实现了在样本服务器上一处配置受控网络地址，即在各个出入口路由器上同时生成对这些受控地址的访问控制，具有一处配置多处生效的优点。解除控制操作的效果同样如此。

一方面，在 ISP 内的网络地址对 ISP 外的受控网络地址的访问都将被转路到黑洞服务器；另一方面，在 ISP 外的受控网络地址对 ISP 内的用户进行访问时，虽然从受控网络地址发出的请求包可以到达用户，但用户的应答包在经过 ISP 的出入口路由器时同样被转路到黑洞服务器而导致连接建立的失败。大部分的网络攻击和网络病毒都是基于面向连接协议的，只要在单方向上能对其进行流量控制，就可以破坏掉连接从而阻止该网络攻击和病毒扩散。综合以上两方面可以看出，该方法可以在网络层利用路由功能实现对受控地址的流量控制。

2.2　动态路由协议的选取和配置

动态路由协议的选取和配置是实现本文所提出的网络控管方法的一个关键。无论样本路

由器和扩散路由器是通过专用线路，还是通过虚拟线路接入到各个出入口路由器上，对 ISP 来说都相当于增加了一个或多个网络分支。根据实际的接入情况，本文提出两种动态路由协议的选取方案：

1) 将从样本路由器到各个出入口路由器的每条扩散链路看成是 AS 域内的一个网络分支，如图 2 所示，所以应考虑使用域内的动态路由协议。目前，常用的域内动态路由协议主要有 RIP、OSPF[3]和 IS-IS[4]等。RIP 是基于距离向量的路由协议，而 OSPF 是基于链路状态的路由协议。在实际的应用中链路状态协议总是比距离向量协议收敛更快，对网络控管系统来说较快的响应速度是很重要的，而且 OSPF 在对 IP 服务类型、流量平衡和超子网等方面的支持均占有优势。而 IS-IS 目前获支持程度没有 OSPF 高。基于如上的情况，该方案选用 OSPF 动态路由协议。

2) 将样本路由器和所有的扩散路由器组成的网络看成一个独立的 AS 域，各个出入口路由器在其它的 AS 域中，则样本路由器或扩散路由器同出入口路由器的路由信息交换便成为域间的路由信息交换，如图 3 所示。在域边界上应该使用域间路由协议，现在多数 ISP 出入口路由器的域间路由协议都使用 BGP 协议[5,6]。因此该方案是在样本路由器和扩散路由器组成的 AS 域内使用 OSPF 协议，在域间使用 BGP 协议。

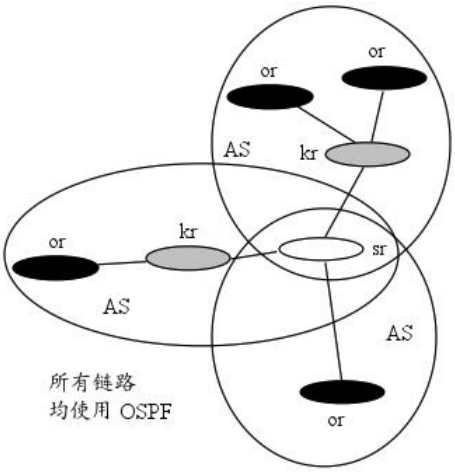

图 2 每个扩散分支属于不同 AS 域

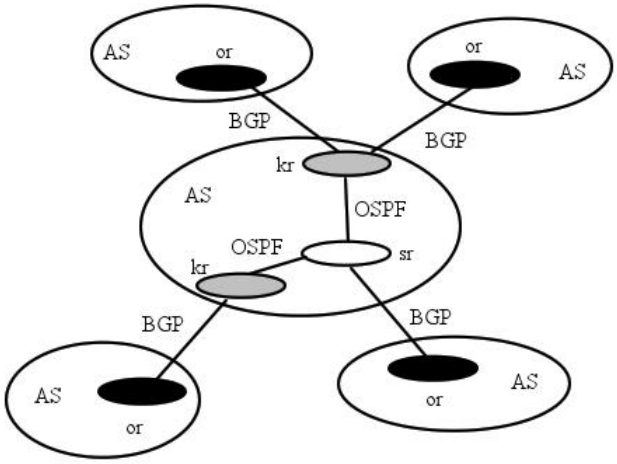

图 3 样本和扩散路由器组成一个独立的域

不管最终采用那种动态路由协议的选取方案，在配置协议时都要注意以下几个方面：

1) 在样本路由器上配置动态路由协议时，一定要将由样本服务器写入的静态路由表项，在同扩散路由器或者出入口路由器相连的接口上利用该动态路由协议重分发（redistribute）出去。如果采用第二种动态路由协议选取方案，也必须要在扩散路由器的配置有 BGP 协议的接口上利用 BGP 协议将 OSPF 的路由表项重分发出去。这是因为不管是静态路由，还是各种动态路由协议，它们都只维护自己的路由表项，如果没有主动设置重分发，它们不能获取其它协议的路由表项。

2) 在出入口路由器上禁止向扩散路由器或样本路由器发送路由信息宣告，即路由信息学习是单方向的。原因有两个：a. 出入口路由器的路由表项既多又复杂，扩散路由器和样本路由器学到这些表项没有什么用，反而会影响它们的扩散效率；b. 如果放开双向路由信息学习，各个出入口路由器会通过扩散链路在它们自己之间相互扩散路由信息，将导致主干网上的路由信息混乱。

3) 在出入口路由器上要提高扩散上来的受控路由信息的优先级，使它们能够优先匹配，从而有效实现网络控管。

2.3 同已有控管方法的对比

现在实现网络访问控制的主要方法是使用路由器访问控制列表和防火墙技术。较传统方式是使用访问控制列表[7, 8](access control list)，但由于路由器对访问控制列表的实现在很大程度上依赖于软件系统，这会占用较多的处理器资源，而在大规模网络环境下实现访问控制势必生成过长的 ACL，导致处理器负载过重，使得系统的包转发率大大降低，影响正常的流量和系统的稳定。另一种方式是使用专业防火墙[9]对特殊流量进行屏蔽，但防火墙并不适用于网络结构紧密、数据流量很大的网络出口。即使是硬件实现的，在大流量情况下也很难保证线速匹配，例如还没有出现 2.5Gbit/s 带宽下线速匹配的防火墙产品。表 1 给出了基于路由扩散的访问控制方法和这两种常规方法的比较。

表 1　　三种网络访问控制方法的对比

对比方面	访问控制列表	防火墙	路由扩散方式
效率(大规模应用)	一般	一般	高
稳定性	较好	较好	好
控制规则丰富性	较丰富	丰富	一般
控制规则实际容量	一般	一般	大
智能性	没有	没有	有
操作简单性	复杂	复杂	简单
对原有结构影响	无	大	小
可扩展性	差	差	好

在大规模网络上面实现访问控制最关键的一点就是不能影响出入口路由器的高速数据交换，在这一点上访问控制列表和防火墙方法都很难做到，而基于路由扩散的访问控制方法可以胜任，因为它是利用路由表匹配功能，进行流量控制。路由表匹配算法成熟且效率较高，一般由专用芯片完成，不占用处理器太多资源，对路由器的性能影响小。这是路由扩散方式的关键优势所在。

在其他方面，路由扩散方式的优点还体现在：1)可以实际承受很大的控制规则容量，因为控制规则的增加对路由器的影响不大，而对于另外两种方法来说，控制规则的增加对性能会造成一定的影响，这也导致了它们在实际的应用中不可能配置很多的规则；2)通过对黑洞服务器获取的数据进行统计和分析，按照一定的原则将结果反馈给样本服务器，帮助样本服务器决定对网络地址的施控或者解控，具有智能性的优点；3)操作简单，只需要管理员录入或删除受控网络地址，不必配置复杂的访问控制规则；4)对原有的网络结构影响比较小，而防火墙需要设置在出入口路由器的外围，对原有的网络结构有一定影响；5)具有可扩展性，因为每个扩散分支负责到一个出入口路由器的扩散工作，所以如果新增出入口路由器，相应增加扩散分支即可。路由扩散方式的缺点是访问控制规则不够丰富，防火墙和访问控制列表都拥有比较丰富的访问控制规则，可以对数据包进行多种元素的匹配，而路由扩散方式只能匹配数据包的目的地址，但是目前的实际情况并不适合在大规模网络上面设置复杂的访问控制规则。

网络管理员也可以直接在出入口路由器上写入静态路由，来完成控管任务，这种控管方

式可以称为直接控管。直接控管的好处在于控管生效速度最快，而且静态路由本身就有很高的匹配优先级。但是，一个大的 ISP 可能有多个出入口路由器，较多次的手工输入势必导致输入环节出错概率增大，同时效率低下，而路由扩散方式则具有一处配置，多处生效的优点。同时因为大部分的出入口路由器主要靠动态路由协议来了解网络拓扑信息，所以一般用来存放配置信息和永久静态路由的快速存储器（flash memory）容量都较小，写不了太多静态路由。如果静态路由只写到内存中，则路由器重启后，将会丢失写入的静态路由。因此，直接控管并不适合在大规模网络环境中应用。

3 结论

本文提出了利用动态路由协议，通过将受控路由信息扩散到大规模网络的出入口路由器上来实现大规模网络控管的方法。这个方法具有路由器负担小、控制规则容量大、智能化、可扩展以及一处配置多处生效等优点。本文所提出的方法在多个 ISP 的实践中表明，基于路由扩散的访问控制方法可以在大规模网络上实现控管，能配置高达上万条的访问控制规则，不影响核心路由器的高速数据交换，整个系统工作稳定。

参考文献：

[1] SAMPEMANE G, NALDURG P, CAMPBELL R. H. Access control for active spaces[A]. 18th Annual Computer Security Applications Conference (ACSAC2002)[C]. Las Vegas, Nevada, 2002. 343-352.

[2] DUAN H X, WU J P, LI X. Policy based access control framework for large networks[A]. 8th International Conference on Networks (ICON 2000)[C]. Singapore, 2000. 267-272.

[3] RASTOGI R, BREITBART Y, GAROFALAKIS M, *et al*. Optimal configuration of OSPF aggregates[J]. IEEE/ACM Trans on Networking, 2003, 11(2):181-194.

[4] FORTZ B, THORUP M. Optimizing OSPF/IS-IS weights in a changing world[J]. IEEE Journal on Selected Areas in Communications, 2002, 20(4):756-767.

[5] TIMOTHY G., GORDON WILFONG. An analysis of BGP convergence properties[A]. Proceedings of ACM SIGCOMM' 99[C]. Boston, 1999. 277-288.

[6] XU K,WANG A P, WU J P, *et al*. Research on routing policy and routing information propagation of boarder gateway protocol version 4 (BGP-4)[A]. IEEE TENCOM'02[C]. Beijing, 2002. 850-854.

[7] GAO J, STEENKISTE P. An access control architecture for programmable routers[A]. 2001 IEEE Open Architectures and Network Programming Proceedings[C]. Alaska, 2001. 15-24.

[8] SLATTERY T 著，苏金树译. Cisco 网络高级 IP 路由技术[M]. 北京：机械工业出版社, 1999.

[9] VERWOERD T, HUNT R. Policy and implementation of an adaptive firewall[A]. 10th International Conference on Networks (ICON 2002)[C]. Singapore, 2002. 434-439.