一种基于切割映射的规则冲突消除算法

李 林, 卢显良
(电子科技大学计算机科学与工程学院, 四川成都 610054)

摘 要: 防火墙规则冲突不仅使规则集变得难于管理, 而且会影响报文分类的效率. 现有的规则冲突消除算法不能完全消除冲突. 针对这一情况, 从计算几何角度对规则冲突进行了分析, 提出了一种基于切割映射的冲突消除算法. 该算法对规则冲突进行了详细的分类, 并根据不同的类型消除冲突. 算法以两条冲突规则为基本处理对象, 在其冲突消除过程中, 顺序切割优先级较低的规则的每一维分量. 理论分析和测试表明, 算法达到了只需增加少量规则即能彻底消除冲突的目的.

关键词: 规则冲突; 冲突消除; 切割映射; 计算几何; 冲突分类
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2008) 02-0408-05

A Filter Conflicts Resolving Algorithm Based on Cutting Mapping

LI Lin, LU Xiao-liang
(*Department of Computer Science, University of Electronic Science and Technology of China, Chengdu, Sichuan 610054, China*)

Abstract: Filter conflicts resolving is an important issue for packet classification and network management. On the one hand, to reduce the time spent on packet classification, a certain algorithm for resolving filter conflicts should be applied to eliminate all filter conflicts during the preprocessing phase. On the other hand, because of the complexity of firewall filters, when firewall administrators add a filter, the newly added filter may conflict with existing ones. This not only makes filter databases difficult to manage, but also may lead to security vulnerabilities. Thus a certain algorithm for resolving filter conflicts should also be applied to eliminate all filter conflicts. Several algorithms for resolving filter conflicts have already been proposed but most of them cannot eliminate filter conflicts completely and set restrictions on filters. This paper analyses filter conflicts from the perspective of computational geometry and presents a filter conflicts resolving algorithm based on cutting mapping. The algorithm resolves filter conflicts according to the classification of conflicts. It treats two filters as the basic processed object and sequentially cuts every dimension of the filters that have lower priority. This paper proves the algorithm and experiments verify its good performance.

Key words: filter conflicts; resolving conflicts; cutting mapping; computational geometry; classification of conflicts

1 引言

在报文分类过程中, 可能出现规则冲突, 通常的处理方式是给每条规则赋予不同的优先级. 随着防火墙规则数目不断增多, 规则冲突通常会带来诸多问题. 下面简要说明其中两个常见的问题.

(1) 规则冲突通常会影响报文分类的速度[1~3]. 许多分类算法为了加快分类速度, 采用了一些复杂的数据结构. 在这种情况下, 分类算法找到的第一条匹配规则, 并不一定是在相冲突的规则中优先级最高的规则. 所以需要进行搜索, 以找到在与数据包相匹配的规则中优先级最高的规则. 显然, 这会影响报文分类的速度.

(2) 规则冲突使得规则集难于管理[1~3]. 下面举例对此说明. 假设规则集中包含有一条规则: 允许 IP 地址在 192.168.*.* 中的节点访问 ftp 服务器. 仅凭这条规则管理员并不能确认, IP 地址在 192.168.*.* 中的节点就一定能访问 ftp 服务器. 因为该规则可能会与其他规则相冲突. 由此可见, 规则冲突加大了规则管理难度.

从以上讨论可知, 若规则集不含有冲突规则, 将有助于提高报文分类的速度, 及降低规则集的管理难度. 由此可见, 有必要对规则冲突消除进行研究.

目前有关规则冲突的研究, 大多集中在规则冲突分类和规则冲突检测等方面, 只有少量的研究是针对规则冲突消除. 在这些研究工作中, 文献[1]讨论了主机型防火墙规则冲突的几种形式, 对冲突进行了详细的分类, 并采用了一种十分简单的冲突检测算法, 即线性冲突检测算法. 该算法类似于报文分类的线性查找算法, 即顺序地检测每条规则.

文献[2, 3]研究了在分布式防火墙环境下规则冲突的情况, 并对冲突进行了分类.

文献[4]对规则冲突进行了分析, 指出仅依靠优先级, 不能使规则集正确表达管理员规则配置意图. 文献[4]又提出了一种冲突消除算法. 该算法通过添加重叠规则来消除冲突. 然而这种处理方式只是使得规则集

收稿日期: 2007-01-23; 修回日期: 2007-10-15
基金项目: 信息产业部生产发展基金(No. 2002[546])

能正确表达管理员意图, 并没有彻底消除冲突. 因为重叠规则本身就是一种规则冲突形式.

文献[5] 采用了文献[4]提出的冲突消除算法, 并对其做了改进, 即减少了重叠规则的引入个数. 然而文献[5] 同文献[4] 一样, 都使用重叠规则消除冲突, 因此它们均不能完全消除冲突. 文献[6] 提出了一种报文分类算法, 并对规则冲突进行了形式化地分析.

从以上讨论可知, 以文献[4, 5] 算法为代表的现有冲突消除算法, 不能彻底消除冲突. 由此可见, 有必要研究能够完全消除冲突的算法. 本文提出了一种适用于多维的基于切割映射的规则冲突消除算法 RCBCM (Resolving Conflicts Based on Cutting Mapping). RCBCM 算法以两条冲突规则为基本处理对象, 在其冲突消除过程中, 顺序切割优先级较低的规则的每一维分量. 另外在算法执行过程中, RCBCM 算法还消除了冗余规则. 理论分析与测试表明, RCBCM 算法达到了只需增加少量规则即能彻底消除冲突和冗余规则的目的.

与文献[4, 5] 算法相比, RCBCM 算法的主要优点是, 能够彻底消除冲突, 而文献[4, 5] 算法只能消除部分类型的冲突. 因此, RCBCM 算法适用于对规则冲突消除有严格要求的应用. 另一方面, 由于 RCBCM 算法的时间复杂度较高, 导致其不适用于那些要求冲突消除在线运行的应用. 而文献[4, 5] 算法的时间复杂度同样较高, 也不适合于这样的应用. 而实际上, 大多数应用都不会要求冲突消除在线运行, 因此, RCBCM 算法适用于大部分冲突消除场合.

2　冲突的定义

本文约定: 所讨论的规则集, 是一个包含有 n 条规则的 m 维规则集, 记为 I.

定义 **1**　规则 R_i 定义为: $R_i = \{T_{i1}, T_{i2}, \cdots, T_{ik}, \cdots, T_{im}\}$, $1 \leqslant k \leqslant m$. 其中 $T_{ik} = [T_{ik}^S, T_{ik}^E]$, 即 $T_{ik} = \{x \mid T_{ik}^S \leqslant x \leqslant T_{ik}^E, T_{ik}^S, x, T_{ik}^E \in \mathrm{N}\}$. 规则优先级定义为 $pri(R_i)$, 处理动作定义为 $act(R_i)$.

定义 **2**　一个数据包 P, 其对应的 m 维分量为 $T(P) = \{t_{P1}, t_{P2}, \cdots, t_{Pk}, \cdots, t_{Pm}\}$, t_{Pk} 是一个第 k 维值域上的非负整数, $1 \leqslant k \leqslant m$. $\exists R_i$, 对于 $\forall j$, $1 \leqslant j \leqslant m$, 均使得 $t_{P_j} \in T_{ij}$, 则称数据包 P 匹配规则 R_i, 记为 $P \in R_i$, 否则称 P 不匹配规则 R_i, 记为 $P \notin R_i$. P 的处理动作记为 $A(P)$.

定义 **3**　数据包 P 和规则 R_i、R_j, 若 $P \in R_i$, $P \in R_j$, 且 $act(R_i) \neq act(R_j)$, 则称 R_i 和 R_j 冲突, 记为 $R_i \int R_j$.

定义 **4**　$\exists$ 数据包 P 和规则集合 $Match(P)$, $\forall R_p \in Match(P)$, 均有 $P \in R_p$, 而 $\forall R_q \notin Match(P)$, $R_q \in I$, 均有 $P \notin R_q$, 则称 $Match(P)$ 是 P 的匹配集合. $A(P) = act(R_r)$, $R_r \in Match(P)$ 且 R_r 是 $Match(P)$ 中优先级最高的规则.

从定义 1 可知, 规则分量 T_{ik} 在数轴上相当于一条线段, 规则 R_i 在 m 维空间中相当于一个超长方形[8]. 下面从计算几何角度分析规则冲突.

定义 **5**　数轴上两条线段 T_{ik} 和 T_{jk}.

若 T_{ik} 和 T_{jk} 不相交, 即 $T_{ik}^E < T_{jk}^S$ 或者 $T_{jk}^E < T_{ik}^S$, 则称 T_{ik} 和 T_{jk} 无关, 记为 $T_{ik} \propto T_{jk}$.

若 $T_{ik}^S < T_{jk}^S \leqslant T_{ik}^E$、$T_{jk}^S \leqslant T_{ik}^E < T_{jk}^E$, 或者 $T_{jk}^S < T_{ik}^S \leqslant T_{jk}^E$、$T_{ik}^S \leqslant T_{jk}^E < T_{ik}^E$, 则称 T_{ik} 和 T_{jk} 交叉, 记为 $T_{ik} \sigma T_{jk}$.

若 $T_{ik}^S \leqslant T_{jk}^S \leqslant T_{jk}^E \leqslant T_{ik}^E$, 则称 T_{ik} 包含 T_{jk}, 记为 $T_{ik} \partial T_{jk}$.

若 $T_{ik} \sigma T_{jk}$ 或者 $T_{ik} \partial T_{jk}$ 或者 $T_{jk} \partial T_{ik}$, 则称 T_{ik} 和 T_{jk} 相关, 记为 $T_{ik} \infty T_{jk}$.

定义 **6**　两个超长方形 R_i 和 R_j. 若对于 $\forall k$, $1 \leqslant k \leqslant m$, 都有 $T_{ik} \infty T_{jk}$, 且 $act(R_i) \neq act(R_j)$, 则称 R_i 和 R_j 冲突, 即 $R_i \int R_j$.

3　冲突的分类

本文从规则的空间位置关系以及冲突消除的角度, 简化了对规则冲突的分类. 规则冲突分为以下三类:

定义 **7**　两个超长方形 R_i 和 R_j, $R_i \int R_j$, $pri(R_i) < pri(R_j)$. $\forall k$, $1 \leqslant k \leqslant m$, 均有 $T_{jk} \partial T_{ik}$, 则称 R_j 覆盖 R_i, 记为 $R_j \triangledown R_i$.

定义 **8**　两个超长方形 R_j 和 R_j, $R_i \int R_j$, $pri(R_i) > pri(R_j)$. $\forall k$, $1 \leqslant k \leqslant m$, 均有 $T_{jk} \partial T_{ik}$, 则称 R_i 遮挡 R_j, 记为 $R_i \mathscr{R} R_j$.

定义 **9**　两个超长方形 R_i 和 R_j, $R_i \int R_j$. $\exists k$, $1 \leqslant k \leqslant m$, 使得 $T_{ik} \sigma T_{jk}$, 则称 R_i 部分遮挡 R_j, 记为 $R_i \mathrm{I} R_j$.

下面分析冗余关系.

定义 **10**　两个超长方形 R_i 和 R_j. 对于 $\forall k$, $1 \leqslant k \leqslant m$, $T_{ik} \partial T_{jk}$, 且 $pri(R_i) > pri(R_j)$, $act(R_i) = act(R_j)$, 则称 R_j 被 R_i 冗余覆盖, 记为 $R_i \Psi R_j$.

定义 **11**　两个超长方形 R_i 和 R_j, $pri(R_i) < pri(R_j)$, $act(R_i) = act(R_j)$. 对于 $\forall k$, $1 \leqslant k \leqslant m$, $T_{ik} \partial T_{jk}$, 且不存在超长方形 R_d, $pri(R_i) < pri(R_d) < pri(R_j)$, 使得 $R_d \int R_j$, 则称 R_j 对于 R_i 是多余的, 记为 $R_i \Omega R_j$.

4　RCBCM 算法

RCBCM 算法的目的: 使得任意数据包匹配的规则数小于等于 1, 或者匹配多条规则, 但这些规则的处理动作一致. 在规则冲突消除过程中, RCBCM 算法将根据

不同的冲突类型做出不同的处理. 因此, 下面分别对这些冲突类型进行讨论.

4.1 简单冲突关系的消除

下面首先分析定义 7、10 和 11 讨论的覆盖关系、冗余覆盖关系以及多余关系的处理.

定理 1 若 $R_j \nabla R_i$、$R_j \Psi R_i$、$R_j \Omega R_i$, 则删去 R_i 后, 不影响规则语义(即 $\forall$ 数据包 p, 无论是否删去 R_i, $A(p)$ 不变).

证明: 根据定义 7、10 和 11 易证, 此处略去.

4.2 切割映射

定义 12 $\langle L, \circ_1, \circ_2, \circ_3 \rangle$, L 是数轴上所有线段组成的集合, $\circ_1$、$\circ_2$ 和 $\circ_3$ 是定义在 L 上的二元运算. $\forall l \in L$, $l = [l^S, l^E]$, 其中 l^S 表示 l 的左端点, l^E 表示 l 的右端点. $\circ_1$、$\circ_2$ 和 $\circ_3$ 定义如下:

$\forall l_1, l_2 \in L$, 不妨假设 $l_2^S \leqslant l_1^S$,

$$
\begin{cases}
l_1 \circ_1 l_2 = \tau \\
l_1 \circ_2 l_2 = \begin{cases} l_1, & l_2^E < l_1^S \\ [l_2^E + 1, l_1^E], & l_2^S \leqslant l_1^S \leqslant l_2^E < l_1^E \\ \tau, & \text{others} \end{cases} \\
l_2 \circ_1 l_1 = \begin{cases} l_2, & l_2^E < l_1^S \\ [l_2^S, l_1^S - 1], & l_2^S < l_1^S \leqslant l_2^E \\ \tau, & \text{others} \end{cases} \\
l_2 \circ_2 l_1 = \begin{cases} [l_1^E + 1, l_2^E], & l_1^E < l_2^E \\ \tau, & \text{others} \end{cases} \\
l_1 \circ_3 l_2 = l_2 \circ_3 l_1 = \begin{cases} [l_1^S, l_2^E], & l_2^S < l_1^S \leqslant l_2^E < l_1^E \\ \tau, & \text{others} \end{cases}
\end{cases}
$$

τ 是一条特殊线段, $\tau = [0, 0]$ 规定: $\forall k$, $1 \leqslant k \leqslant 3$, 均有 $\tau \circ_k l = l \circ_k \tau = \tau$.

定义 13 切割映射 $f: L \times L \to 2^L$, 2^L 是 L 的幂集. $\forall l_1, l_2 \in L$, 且 $l_1, l_2 \neq \tau$,

$$
f(\langle l_1, l_2 \rangle) = \begin{cases}
\{l_1 \circ_3 l_2\} \cup \{l_2 \circ_2 l_1\}, & l_1^S < l_2^S \leqslant l_1^E < l_2^E \\
\{l_1 \circ_3 l_2\} \cup \{l_2 \circ_1 l_1\}, & l_2^S < l_1^S \leqslant l_2^E < l_1^E \\
\{l_2 \circ_1 l_1\} \cup \{l_2 \circ_2 l_1\} \cup \{l_1\}, & l_2^S < l_1^S \leqslant l_1^E < l_2^E \\
\{l_2 \circ_2 l_1\} \cup \{l_1\}, & l_2^S = l_1^S \leqslant l_1^E < l_2^E \\
\{l_2 \circ_1 l_1\} \cup \{l_1\}, & l_2^S < l_1^S \leqslant l_1^E = l_2^E \\
\{l_1\}, & l_2^S = l_1^S \leqslant l_1^E = l_2^E \\
\{l_1 \circ_1 l_2\} \cup \{l_1 \circ_2 l_2\} \cup \{l_2\}, & l_1^S < l_2^S \leqslant l_2^E < l_1^E \\
\{l_1 \circ_2 l_2\} \cup \{l_2\}, & l_1^S = l_2^S \leqslant l_2^E < l_1^E \\
\{l_1 \circ_1 l_2\} \cup \{l_2\}, & l_1^S < l_2^S \leqslant l_2^E = l_1^E \\
\Phi, & \text{others}
\end{cases}
$$

若 l_1 或者 $l_2 = \tau$, $f(\langle l_1, l_2 \rangle) = \Phi$.

4.3 遮挡和部分遮挡冲突关系的消除

首先定义第 k 维分量的冲突切割映射.

定义 14 $\forall k$, $1 \leqslant k \leqslant m$, 均有冲突切割映射 $g_k: A \times A \to 2^A$. A 是所有规则或者超长方形组成的集合. $\forall R_i, R_j \in A$, $1 \leqslant i, j \leqslant n$, $g_k(\langle R_i, R_j \rangle) =$

$$
\begin{cases}
\bigcup_{q=p}^{p+num} \{R_q\}, & (R_i \mathrm{I} R_j \text{ 或 } R_i \mathscr{R} R_j) \text{ 且 } pri(R_i) > pri(R_j) \\
\Phi, & \text{others}
\end{cases}
$$

其中, $num = |f(\langle T_{ik}, T_{jk} \rangle)| - 1$, p 是规则集可用下标起始值, $R_q = \{T_{q1}, T_{q2}, \ldots, T_{qk}, \ldots, T_{qm}\}$, $pri(R_q) = pri(R_j)$, $act(R_q) = act(R_j)$. $\forall r$, $1 \leqslant r \leqslant m$, $r \neq k$, 均有 $T_{qr} = T_{jr}$, 而 $T_{qk} \in f(\langle T_{ik}, T_{jk} \rangle)$.

定理 2 $\forall R_i, R_j \in A$, 若 $pri(R_i) > pri(R_j)$, $R_i \mathscr{R} R_j$ 或 $R_i \mathrm{I} R_j$, 则性质

(a) $g_k(\langle R_i, R_j \rangle)$ 中只有一个元素与 R_i 冲突, 设该元素是 R_z, 则 $T_{ik} \partial T_{zk}$;

(b) $g_k\langle R_i, R_j \rangle$中的元素互不冲突;

(c)规则集合$\{R_i, R_j\}$与规则集合$\{R_i\} \cup g_k(\langle R_i, R_j \rangle)$是等价的(即 $\forall$ 数据包 B, 对两个规则集合而言, $A(B)$ 相同);

(d) $\forall R_s \in A$, 若 R_s 不与 R_j 冲突, 则 R_s 也不与 $g_k(\langle R_i, R_j \rangle)$ 中的元素冲突.

证明: 这里只讨论 $T_{jk}^S < T_{ik}^S < T_{ik}^E < T_{jk}^E$ 的情况, 其余情况类似. 根据定义 13 和定义 14 可知:

$g_k(\langle R_i, R_j \rangle) = \{R_p, R_{p+1}, R_{p+2}\}$, $f(\langle T_{ik}, T_{jk} \rangle) = \{[T_{jk}^S, T_{ik}^S - 1], [T_{ik}^S, T_{ik}^E], [T_{ik}^E + 1, T_{jk}^E]\}$. 不妨假设, $T_{pk} = [T_{jk}^S, T_{ik}^S - 1]$、$T_{(p+1)k} = [T_{ik}^S, T_{ik}^E]$ 和 $T_{(p+2)k} = [T_{ik}^E + 1, T_{jk}^E]$. 显然, $g_k(\langle R_i, R_j \rangle)$ 中不存在冲突规则, 即性质(b)成立. 根据定义 12、13 和 14, 以及性质(b), 易证性质(a)、(c)和(d)成立, 此处略去.

R_i 和 R_j 经过 m 次冲突切割映射后, 可以转换成一组等价且没有冲突的规则. 下面对此进行证明.

定理 3 $\forall R_i, R_j \in A$, 若 $pri(R_i) > pri(R_j)$, $R_i \mathscr{R} R_j$ 或 $R_i \mathrm{I} R_j$, 则$\{R_i, R_j\}$与$(\bigcup_{k=1}^{m}(g_k(\langle R_i, R^{k-1} \rangle) - R^k) \cup \{R_i\}$等价, 且后者不包含任何冲突规则. 其中 $R^0 = R_j$, R^k 是 $g_k(\langle R_i, R^{k-1} \rangle)$ 中与 R_i 相冲突的规则.

证明: 从定理 2 的性质(c)可知, $\{R_i, R_j\}$ 与 $(\bigcup_{k=1}^{m-1}(g_k(\langle R_i, R^{k-1} \rangle) - R^k) \cup g_m(\langle R_i, R^{m-1} \rangle) \cup \{R_i\}$ 等价.

所以$\{R_i, R_j\}$与$(\bigcup_{k=1}^{m}(g_k(\langle R_i, R^{k-1} \rangle) - R^k) \cup \{R_i\}$等价. 显然, 命题得证.

从上述讨论可知, 这类冲突关系的消除是以增加规则为代价的. 下面对规则增加的数量进行讨论.

定理 4 $\forall R_i, R_j \in A$, 若 $pri(R_i) > pri(R_j)$, $R_i \mathscr{R} R_j$ 或 $R_i \mathrm{I} R_j$, $|(\bigcup_{k=1}^{m}(g_k(\langle R_i, R^{k-1} \rangle) - R^k) \cup \{R_i\}| \leqslant 2m + 1$.

其中 $R^0 = R_j$, R^k 是 $g_k(\langle R_i, R^{k-1}\rangle)$ 中与 R_i 相冲突的规则.

证明: 从定义 12、13 和 14 易证, 此处略去.

4.4 RCBCM 算法分析

前面描述了两条规则的冲突消除, 本节将讨论如何消除整个规则集的冲突. RCBCM 算法使用线性冲突检测算法查找冲突规则对和冗余规则对, 然后再根据前面讨论的内容, 消除两条规则的冲突以及冗余规则, 直到规则集中不存在任何冲突规则和冗余规则为止.

由定理 2 的性质(d)可知, $\forall R_s \in I$, 若 R_s 不与 R_j 冲突, 则 R_s 也不与 $g_k(\langle R_i, R_j\rangle)$ 中的元素冲突. 但是若 R_i 和 R_j 冲突, 且 $R_s \neq R_i$, 则 R_s 有可能与 $g_k(\langle R_i, R_j\rangle)$ 中的元素冲突(将这种冲突称为继发冲突). 下面对 RCBCM 算法进行分析, 首先讨论其正确性.

定理 5　规则集 I 和 I', 其中 I' 是经过 RCBCM 算法冲突消除后得到的规则集. 证明: I 和 I' 等价, 且 I' 中不存在冲突规则和冗余规则.

证明: 从定理 1、2 和 3 易证, 此处略去.

RCBCM 算法的空间复杂度取决于消除规则集冲突而增加的规则数目. 定理 6 给出了在最坏的情况下, 规则增加的数量级.

定理 6　规则集 I 和 I', 其中 I' 是 I 经过 RCBCM 算法冲突消除后得到的规则集. 证明: 在最坏的情况下, $|I'|$ 的数量级是 n^m.

证明: 根据前面讨论的相关定义和定理 4 易证, 此处略去.

5　测试

测试环境: Intel2.4G, 512M 内存, linux2.4 内核, 使用 C++ 语言实现 RCBCM 算法. 测试使用的冲突检测算法是线性冲突检测算法. 测试所用规则集, 来自于本文统计的 24 个企业级防火墙和 95 个个人防火墙. 其中, 规则集的维数从 2 到 5 不等. 下面首先讨论这些规则集的特性.

(1) 防火墙规则数目较少. 24 个企业级防火墙中, 72% 的规则集包含有 200 至 500 条规则; 而 95 个个人防火墙中, 83% 的规则集包含有 50 到 100 条规则.

(2) 规则集包含的冲突规则对和冗余规则对的个数很少, 平均而言, 其比例为规则集大小的 10%. 在这些冲突规则对和冗余规则对中, 45% 的规则对是覆盖关系或冗余覆盖关系, 31% 的规则对是多余关系, 18% 的规则对是遮挡关系, 而只有 6% 的规则对是部分遮挡关系. 另外, 绝大多数规则只与数条规则相冲突, 在本文统计的规则集中, 其最大值为 4. 这就意味着继发冲突的规则对较少.

测试项目:

(1) RCBCM 算法和文献[4, 5] 提出的冲突消除算法的对比测试. 测试方法: 首先将上述规则集分别按照 RCBCM 算法和文献[4, 5] 算法进行处理, 然后使用线性冲突检测算法对处理后的规则集进行冲突检测. 测试结果: 文献[4, 5] 算法处理后的规则集, 仍然有冲突规则, 表 1 列出了其中部分二维规则(出于安全和隐私考虑, 表 1 使用# 号代替部分 IP 地址); RCBCM 算法处理后的规则集不含有冲突规则和冗余规则, 因此表 1 未列出其测试结果. 从表 1 可知, R_1 和 R_2 冲突, R_3 和 R_4 冲突.

表 1　文献[4, 5]算法测试结果

	R_1	R_2	R_3	R_4
源 IP 起始值	#.#.2.45	#.#.2.4	#.#.45.28	#.#.45.10
源 IP 结束值	#.#.2.45	#.#.2.50	#.#.45.35	#.#.45.253
目的 IP 起始值	#.#.10.2	#.#.10.2	#.#.3.23	#.#.3.23
目的 IP 结束值	#.#.10.2	#.#.10.2	#.#.3.34	#.#.3.34
规则处理动作	放行	丢弃	放行	丢弃

(2) RCBCM 算法的空间性能测试. 测试方法: 使用 RCBCM 算法对上述规则集进行处理, 记录规则增加的个数. 理论上最坏的情况下, 规则个数会以 n^m 的数量级增加. 而在实际应用中, 冲突消除并不会增加过多规则. 图 1 描述了测试结果, 横坐标表示规则集的大小, 纵坐标表示规则增加的个数.

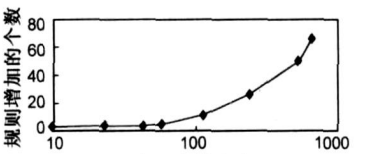

图 1　规则增加的个数

从图 1 可知, 规则增加的个数, 随着规则集的增大而缓慢增加; 平均而言, 增加的规则只占规则集的 10% 左右. 即实际规则增加情况与理论最坏情况相差很大. 造成这种情况的原因主要有以下几点: (1) 冲突规则对和冗余规则对的个数, 只相当于规则集大小的 10%, 与理论上最坏情况时所有规则均相冲突, 相去甚远. (2) 在这些冲突规则对和冗余规则对中, 45% 的规则对是覆盖关系或冗余覆盖关系, 31% 的规则对是多余关系. 根据定理 1 可知, 处理这几类关系不仅不会增加规则, 反而会减少规则. (3) 绝大多数规则只与数条规则相冲突. 这就使得继发冲突的规则对较少.

上述测试说明, RCBCM 算法只需增加少数规则即能达到消除冲突的目的.

6　结论

针对现有的冲突消除算法不能彻底消除冲突这一实际情况, 本文提出了一种基于切割映射的冲突消除算法 RCBCM. RCBCM 算法以两条冲突规则为基本处理单位, 在其冲突消除过程中, 顺序切割优先级较低的规则的每一维分量. 理论分析与测试表明, RCBCM 算法只

需增加少量规则即能完全消除冲突. 该算法适用于大多数冲突消除场合.

参考文献:

[1] Ehab Al-Shaer, Hazem Hamed. Taxonomy of conflicts in network security policies[J]. IEEE Communications Magazine, 2006, 44(3): 134-141.

[2] Ehab Al-Shaer, Hazem Hamed. Discovery of policy anomalies in distributed firewalls[A]. IEEE INFOCOM 2004[C]. San Diego: IEEE, 2004. 2605-2616.

[3] Ehab Al-Shaer, Hazem Hamed. Conflict classification and analysis of distributed firewall policies[J]. Selected Areas in Communications, 2005, 23(10): 2069-2084.

[4] Adiseshu Hari, Subhash Suri. Detecting and resolving packet filter conflicts[A]. IEEE INFOCOM 2000[C]. Tel Aviv: IEEE, 2000. 1203-1212.

[5] Haibin Lu, Sartaj Sahni. Conflict detection and resolution in two-dimensional prefix router tables[J]. IEEE/ACM Transactions on Networking, 2005, 13(6): 1353-1363.

[6] 田大新, 刘衍珩, 等. 数据包过滤规则的快速匹配算法和冲突检测[J]. 计算机研究与发展, 2005, 42(7): 1128-1135.
Tian Daxin, Liu Yanheng, et al. A fast matching algorithm and conflict detection for packet filter rules[J]. Journal of Computer Research and Development, 2005, 42(7): 1128-1135. (in Chinese)

[7] 杜德超, 姚庆栋. 多维过虑规则无冲突的高速分组分类算法[J]. 电子学报, 2002, 30(11): 1676-1680.
Du Dechao, Yao Qingdong. High speed packet classification for multidimensional conflict-free filters[J]. Acta Electronica Sinica, 2002, 30(11): 1676-1680. (in Chinese)

[8] Xuehong Sun, Sartaj K. Sahni. Packet classification consuming small amount of memory[J]. IEEE Transactions on Networking, 2005, 13(5): 1135-1144.

作者简介:

李 林 男, 1981 年生于四川成都, 博士研究生. 研究方向为网络安全.
E-mail: lilin@uestc.edu.cn

卢显良 男, 1944 年生于河北, 教授, 博士生导师. 研究方向为计算机网络、操作系统.