基于流量矩阵和Kalman滤波的DDoS攻击检测方法

颜若愚
(河南财经政法大学计算机与信息工程学院 郑州 450002)

摘 要 针对分布式拒绝服务(DDoS)攻击产生的流量往往对路由器造成难以承受的负担的问题,提出一种既能减轻路由器负荷又能快速准确检测DDoS攻击的方法。该方法首先在路由器中构造端口对之间的流量矩阵来准确描述DDoS攻击的流量汇聚特性,然后利用Kalman滤波对流量矩阵进行估计,接着使用GLR统计测试进行异常检测,进而判断路由器端口是否受到DDoS攻击。最后,基于实际数据进行了仿真实验,结果表明,所提方法相比主成分分析(PCA)方法具有更高的检测率、更低的误检率和更小的检测延迟。

关键词 分布式拒绝服务,卡尔曼滤波,异常检测,流量分析,流量矩阵
中图法分类号 TP393.08 **文献标识码** A

DDoS Attacks Detection Method Based on Traffic Matrix and Kalman Filter

YAN Ruo-yu
(College of Computer and Information Engineering, Henan University of Economics and Law, Zhengzhou 450002, China)

Abstract Distributed Denial of Service (DDoS) attack traffic often is an unbearable burden on router, so a new DDoS attack detection method was proposed to release the burden and to detect the attack fast and accurately. In this method, traffic matrix between ports on the router is first constructed to precisely describe DDoS attack traffic aggregation characteristics. Then Generalized Likelihood Ratio (GLR) statistical test is used to detect traffic anomaly after Kalman filter is applied to estimate traffic matrix. After that whether each router port is attacked by DDoS is judged. Finally, a simulation experiment with actual data was conducted to compare the method with PCA method, which shows that the proposed method has higher detection rate, lower false alarm rate and smaller detection lag time.

Keywords Distributed denial of service, Kalman filter, Anomaly detection, Traffic analysis, Traffic matrix

随着因特网规模的日益扩大,网络安全问题也越来越突出,其中分布式拒绝服务(DDoS)攻击对网络的破坏尤为严重。目前DDoS攻击检测方法大致可以分为两类,一类为专门针对DDoS攻击的检测方法,这些方法主要利用了DDoS攻击在网络流量中表现出来的特殊属性,如文献[1-6]等。另一类为异常检测方法,这些方法主要对正常网络流量行为进行建模,可以检测到各种网络异常行为,包括DDoS攻击等,如文献[7-11]等。

文献[1]提出从历史网络流量中抽取合法用户的IP地址建立数据库,以检查流经路由器的当前数据包中的源IP地址是否在合法IP地址库中作为检测DDoS攻击的手段。文献[2-4]使用不同的CUSUM (Cumulative Sum)方法来统计路由器中进出各端口的流量,并以进出流量比率作为检测DDoS攻击的统计量。文献[6]采用一种基于线性判别分析法的有监督学习系统来区分合法流量和DDoS攻击流量,依靠系统的自学习能力解决系统参数调校不准确的问题。文献[7]使用一种自回归系统来估计参数分形维数D和自相似系数H,利用基于最大似然估计的改变点检测方法来检测DDoS攻击。文献[8]提出利用主成分分析(Principal Component Analysis,PCA)对骨干网络中的OD flow和物理链路流量进行建模和特征分析,并在文献[9]中针对物理链路中的流量利用PCA检测DDoS攻击。文献[10]侧重分析了PCA方法在大规模网络流量中异常检测的灵敏性,并对3种不同粒度的流量进行检测的结果做了比较分析。文献[11]使用Kalman滤波对OD flow进行估计,介绍了4种统计假设检测方法,并对它们的优缺点进行了比较。文献[8-11]主要利用大规模网络中的OD flow流量矩阵进行很宽泛的异常检测,但都不以DDoS攻击检测作为研究目的,而且由于实时获取OD flow流量很困难,这些方法难以在实际网络环境中得到应用。

DDoS攻击为了达到阻止合法用户访问网络共享服务或资源的目的,参与攻击的主机不仅数量庞大,而且来自于网络的四面八方,因此大量的攻击流量通过路由器汇聚到被攻击节点,即攻击流量从路由器多个端口汇聚到同一个出口,基于DDoS攻击的这种流量汇聚特点,本文提出了一种检测DDoS攻击的新方法。该方法利用单个路由器中的流量建立流量矩阵,解决了流量矩阵获取困难的问题,然后为减轻路由器负荷,使用基于Kalman滤波的方法对流量矩阵进行检测,据此

到稿日期:2013-05-16 返修日期:2013-09-02 本文受国家自然科学基金项目(61101211,61202285),湖南省自然科学基金项目(11JJ9010),河南省自然科学基金项目(132300410337),河南省教育厅项目(13B520901)资助。
颜若愚(1974—),男,博士,讲师,主要研究方向为网络安全,E-mail:hn_yry@163.com。

判断路由器端口是否受到 DDoS 攻击。最后的实验结果验证了所提出的 DDoS 攻击检测方法的有效性。

1 路由器中建立流量矩阵

为叙述方便，首先给出以下 3 种流量定义：

(1)P-P flow：单位时间内从一个端口进入路由器并从另外一个端口出去的所有数据包(即 Port to Port)。

(2)Input link：单位时间内从同一端口进入路由器的所有数据包。

(3)Output link：单位时间内从同一路由器端口出去的所有数据包。

显然，input link(或 Output link)流量实际是由多个相关 P-P flow 叠加而成的，它们之间的这种关系可以精确地用一个路由矩阵 H 来描述，矩阵 H 大小为 size(# Input link)×size(# IF flow) (size (#Input link)，size (#IF flow)分别表示 Input link 和 P-P flow 的个数)，如果 P-P flow j 经过 input link i，则 H 中元素 $H_{ij}=1$，反之 $H_{ij}=0$。显然，Input link 的流量向量 y 和 P-P flow 的流量向量 x 可通过路由矩阵 H 相关联 $y=Hx$，这为后面建立流量的状态空间模型提供了可能。

直接获取路由器端口之间的流量(P-P flow)目前还没有专门的工具，通过 MIB 信息库也只能提取到通过各端口的流量信息。虽然采用分析数据包路由的方法可以得到 P-P flow，但需要获得路由器中的路由表，并监控所有流经路由器的数据包，这在时间和资源上消耗都很大，而且路由表的动态更新使得分析的难度加大。本文提出一种更简便的方法来解决这个问题。大多数高级 Cisco 路由器都具有可配置的 Netflow 功能[12]，该功能按一定时间间隔生成 Netflow 记录，该记录中包含了 input(入端口号)和 output(出端口号)属性，针对这两个属性通过 SQL 编程可以实现流量汇聚，分别得到一定时间间隔上 Input link、Output link 和 P-P flow 3 种流量的统计值。但是路由器生成 Netflow 记录会增加其 CPU 利用率，Netflow 性能分析白皮书[13]表明，根据同时存在路由器中的 Netflow 记录数多少，Netflow 功能因此增加路由器的 CPU 使用率平均为 7%～23%，为了解决 Netflow 功能的开启对重负荷路由器性能所造成的影响，在检测 DDos 攻击时本文提出了无需不间断收集 P-P flow 流量的 Kalman 滤波估计检测方法。

2 基于 Kalman 滤波的流量矩阵异常检测方法

2.1 流量状态空间模型建立

为了反映流量采集的不准确性，Input link(或 output link)流量和 P-P flow 的关系现改用如下公式来描述。

$$y_t=H_tx_t+v_t \tag{1}$$

式中，y_t 表示 Input link 流量向量(观测变量)，x_t 表示 P-P flow 流量向量(隐含变量)，H_t 表示内部路由矩阵，当 P-P flow j 通过 input link i 时，元素 $h_{ij}=1$，否则 $h_{ij}=0$。由于数据采集设备会发生测量错误，用 v_t 表示一个随机过程来捕捉这种测量误差。

对流量进行预测虽然可以使用任何结构的预测模型和噪声分布来建模，但考虑到目前线性随机预测模型和高斯噪声相结合的预测方法比较成功，本文利用基于状态空间模型的线性动力学系统构造如下线性方程，建立 x_{t+1} 和 x_t 相关联的时间模型。

$$x_{t+1}=\Phi_tx_t+w_t \tag{2}$$

式中，状态转移矩阵 Φ_t 刻画了系统的动态行为，w_t 是一个随机过程噪声，描述流量的随机性和不可预测部分。式(1)、式(2)即为该动力系统的完整描述。

$$\begin{cases}x_{t+1}=\Phi_tx_t+w_t\\ y_t=H_tx_t+v_t\end{cases} \tag{3}$$

式(3)是线性动力学系统的经典形式，在该模型中假设状态噪声 w_t 和量测噪声 v_t 是不相关的零均值高斯白噪声过程，其协方差分别为 Q_t 和 R_t。在已知以上模型系统的情况下，只要给出过去一系列的观察值$\{y_1,\cdots,y_{t+1}\}$，问题就转化为寻找对真实网络状态 x_{t+1} 的优化估计，Kalman 滤波正是解决这种问题的经典方法。

2.2 离散 Kalman 滤波方程

离散时变系统下的 Kalman 滤波方程组包括了预测步骤(式(4))和更新步骤(式(5))，对其中一些重要变量的说明如表 1 所列。在初始条件$\hat{x}_0^0=E[x_0]$和协方差矩阵 $P_0^0=E[(\hat{x}_0^0-x_0)(\hat{x}_0^0-x_0)^T]$已知的情况下，利用方程组(4)和(5)即可实现对 x_t 的迭代估计计算。

表 1 Kalman 滤波方程变量说明

变量	说明
y_t	系统观测向量
x_t	系统状态向量
$\hat{x}_{t+1}^t$	使用所有到时间 t 为止的可获得信息对 x_{t+1} 的预测值
$\hat{x}_{t+1}^{t+1}$	使用所有过去值和在 t+1 时刻到达的观测值对 x_{t+1} 的估计值
P_t^t	状态向量在 t 时刻估计值的协方差矩阵
P_{t+1}^t	状态向量在 t 时刻预测值的协方差矩阵
K_{t+1}	在 t+1 时刻的 Kalman 增益矩阵

$$\begin{cases}\hat{x}_{t+1}^t=\Phi_t\hat{x}_t^t\\ P_{t+1}^t=\Phi_tP_t^t(\Phi_t)^T+Q_t\end{cases} \tag{4}$$

$$\begin{cases}\hat{x}_{t+1}^{t+1}=\hat{x}_{t+1}^t+K_{t+1}[y_{t+1}-H_{t+1}\hat{x}_{t+1}^t]\\ P_{t+1}^{t+1}=(I-K_{t+1}H_{t+1})P_{t+1}^t\\ K_{t+1}=P_{t+1}^t(H_{t+1})^T[H_tP_{t+1}^t(H_{t+1})^T+R_{t+1}]^{-1}\end{cases} \tag{5}$$

2.3 EM 算法对{Φ,Q,R}进行估计

在非平稳状态下 Kalman 滤波方程中的参数{Φ,Q,R}是变化的，但实际上较长一段时间(如一个星期)内不校准{Φ,Q,R}对检测结果所造成的影响很小。为了在实际应用中提高检测速度和减少数据采集开销，假定{Φ,Q,R}为常值，不随时间变化，即这些参数在方程中的时间下标可以去掉。

为了使用 Kalman 滤波器对流量矩阵进行估计，需要知道{H,Φ,Q,R}，根据路由器中内部流量关系，矩阵 H 是常值并可知的，其它参数 $\theta=\{\Phi,Q,R\}$ 则需要计算。本文使用 EM (Expectation Maximum)算法求取参数 θ，即以迭代的方式计算系统参数 θ 的最大似然估计。

假定式(3)中的系统状态可观察，$Y=[y_0\,y_1\cdots y_n]$和 $X=[x_0\,x_1\cdots x_n]$已知，即可使用最大似然估计求出系统参数 θ，其最大化方程如下。

$$\ln L(X,Y,\theta)=-\frac{n}{2}\log|Q|-\frac{1}{2}\sum_{k=1}^{n}(x_k-\Phi x_{k-1})^{\mathrm{T}}Q^{-1}(x_k-\Phi x_{k-1})-\frac{n}{2}\log|R|-\frac{1}{2}\sum_{k=1}^{n}(y_k-Hx_k)^{\mathrm{T}}R^{-1}(y_k-Hx_k)+CONSTANT$$

一般地，假定 w_k 和 v_k 为不相关高斯白噪声过程，推导可得以下系统参数值。

$$\hat{\Phi}=BA^{-1}$$

$$\hat{Q}=n^{-1}(C-B\Phi^{\mathrm{T}}-\Phi B^{\mathrm{T}}+\Phi A\Phi^{\mathrm{T}})$$

$$\hat{R}=n^{-1}\sum_{t=1}^{n}[(y_t-Hx_t^n)(y_t-Hx_t^n)^{\mathrm{T}}+HP_t^nH^{\mathrm{T}}]$$

式中，A、B、C 定义如下。

$$A=\sum_{t=1}^{n}[P_{t-1}^n+x_{t-1}^n(x_{t-1}^n)^{\mathrm{T}}]$$

$$B=\sum_{t=1}^{n}[P_{t,t-1}^n+x_t^n(x_{t-1}^n)^{\mathrm{T}}]$$

$$C=\sum_{t=1}^{n}[P_t^n+x_t^n(x_t^n)^{\mathrm{T}}]$$

$\{A,B,C\}$ 中的变量可用固定区间平滑形式的 Kalman 滤波来计算，该滤波过程包括标准的 Kalman 滤波前向迭代(Forward Recursion)和后向迭代(Backward Recursions)过程。前向迭代过程就是式(4)和式(5)，只是参数值 $\{H,\Phi,Q,R\}$ 在这里与时间无关。Kalman 平滑后向迭代包括以下公式。

对于 $t=n,n-1,\cdots,1$

$$x_{t-1}^n=x_{t-1}^{t-1}+J_t(x_t^n-x_t^{t-1})$$

式中，$J_t=P_{t-1}^{t-1}\Phi^{\mathrm{T}}(P_t^{t-1})^{-1}$

$$P_{t-1}^n=P_{t-1}^{t-1}+J_t(P_t^n-P_t^{t-1})J_t^{\mathrm{T}}$$

对于 $t=n,n-1,\cdots,2$

$$P_{t-1,t-2}^n=P_{t-1}^{t-1}J_{t-1}^{\mathrm{T}}+J_t(P_{t,t-1}^n-\Phi P_{t-1}^{t-1})J_{t-1}^{\mathrm{T}}$$

式中，$P_{n,n-1}^n=(I-K_nH)\Phi P_{n-1}^{n-1}$。

应该注意的是后向迭代中的一些初始值如 x_n^n、P_n^n、P_n^{n-1} 和 P_{n-1}^{n-1} 由前向迭代计算所得终值进行初始化。综上所述，图1给出了利用 EM 算法估计 θ 的流程。Φ、Q、R 可以初始化为单位阵，迭代次数越多其估计精度越高，但耗时也越多，收敛速度也变慢，因此往往以迭代的次数作为结束条件。

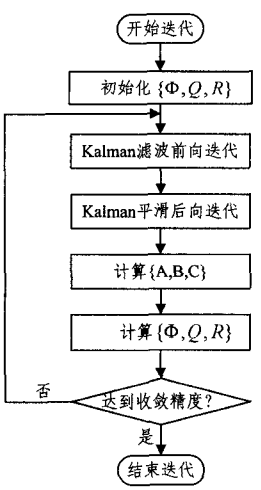

图1 EM 估计 $\{\Phi,Q,R\}$ 的流程图

2.4 GLR 统计检测流量矩阵

由于 Kalman 滤波公式给出了 P-P flow 流量的预测值和估计值，P-P flow 的新息 δ_{t+1} 和残差 η_{t+1}(residual)可方便求得：

$$\delta_{t+1}=x_{t+1}-\hat{x}_{t+1}^{t}$$

$$\eta_{t+1}=\hat{x}_{t+1}^{t+1}-\hat{x}_{t+1}^{t}$$

因此可用 δ_{t+1} 对 P-P flow 流量进行异常检测，但是在 x_{t+1} 不可知时近似计算 δ_{t+1} 非常复杂。为了减少计算量，本文使用残差 η_{t+1} 代替 δ_{t+1}，然后使用文献[14]中的 GLR(Generalized Likelihood Ratio)方法对每个 P-P flow 的残差进行统计检测，该方法能在时间序列的均值和方差都未知的情况下求得最好估计。

3 检测路由器端口是否受到 DDoS 攻击

根据对 P-P flow 流量矩阵的检测结果，实时对路由器中每个端口进行 DDoS 攻击度评估。评估方法充分利用了 DDoS 攻击流量的汇聚结构特点，着重考虑了影响评估指数的两个因素。因素一为到达同一端口的异常 P-P flow 个数，异常个数越多，该端口遭到的攻击也就越严重。因素二为到达同一端口的异常 P-P flow 的流量大小，异常流量所占该端口的出去流量比重越大，该端口遭到的攻击也就越严重。具体评估公式如下：

$$E_i(t)=\begin{cases}\alpha\times\dfrac{\sum_{i=1}^{n}F_{ji}(t)}{n-1}+\beta\times\sum_{j=1}^{n}W_{ji}(t)F_{ji}(t), & n\leqslant 5 \text{ 或 } \sum_{j=1}^{n}F_{ji}(t)=0\\ \alpha\times\dfrac{1}{1+\exp(\lceil n/2\rceil-\sum_{j=1}^{n}F_{ji}(t))}+\beta\times\sum_{j=1}^{n}W_{ji}(t)F_{ji}(t) & \\ n>5 \text{ 且 } \sum_{j=1}^{n}F_{ji}(t)>0 & \end{cases}$$

式中，$\alpha+\beta=1$，实验中取 $\alpha=0.6$，表示到达同一端口的 P-P flow 异常数在该评估指数中所占权重较大，而异常 P-P flow 的流量大小所占权重较小。n 表示路由器的活动端口数目，i、j 都为端口号，$E_i(t)$ 为端口 i 在 t 时刻被 DDoS 攻击的程度值即评估指数。当 $j\neq i$ 时，$F_{ji}(t)$ 为 P-P flow $j-i$ 在 t 时刻的异常值，即如果检测到该流量异常则 $F_{ji}(t)=1$，否则 $F_{ji}(t)=0$，$W_{ji}(t)$ 为 t 时刻 P-P flow $j-i$ 所占 Output link $\sharp i$ 流量的比重值。当 $j=i$ 时，根据 P-P flow 定义，入出为同一端口的流量不被考虑，因此有 $F_{ji}(t)=0$，$W_{ji}(t)=0$。应该注意的是这里使用两个条件公式来计算评估指数，原因是相同的异常 P-P flow 数目对具有较多活动端口的路由器影响较小，而对具有较少活动端口的路由器却影响较大。实际应用中，对于具有较少活动端口的路由器，一般认为到达某个端口的异常 P-P flow 数和 DDoS 攻击对该端口的影响程度呈线性递增关系。因此如果一个路由器的活动端口数不超过 5 个，使用具有较大斜率的线性函数来表示异常 P-P flow 数对评估指数的贡献，否则使用 Sigmoid 函数。Sigmoid 函数是一种很好的阈值函数，其形态特点是前后两部分的斜率较小，而中间部分是函数的阈值部分，斜率陡峭。Sigmoid 函数的形态很好地模拟了异常 P-P flow 数目对端口的影响程度：异常数目很小时对端口的影响也小，当异常数目大到一定程度时，对端口的影响迅速增加，但进一步增加异常 P-P flow 数目后，新增的异常对端口的影响已相对有限。

当检测路由器的某个端口是否受到 DDoS 攻击时，本文针对该端口的评估指数设置一个阈值 0.6 来判断其是否受到 DDoS 攻击。

4 实验与结果比较分析

4.1 实验数据

为了验证检测方法的有效性，一种方式是利用实际流量统计值，但必须事先检索实际流量，标定可能的异常。在大规模流量中要准确标定异常是一项困难的工作，可能会存在疏漏和误标，同时实际流量包含的异常有限，强度不一，不能按需要来检验方法的性能，因此有必要生成人工异常流量作为检验数据集，本文中所有比较实验都以人工流量作为测试样本。

人工异常流量的生成在文献[11]中有很详细的描述，以该方法和一个5端口路由器连续一周的P-P flow真实流量为基础，本文使用表2中的参数来生成实验仿真数据，具体步骤可以参考文献[11]，在此不再赘述。

DDoS攻击的持续时间一般为5～30分钟[15]，短则少于1分钟，长则超过一天，本文选取常见的持续时间即1～30分钟。表2中，δ为攻击强度，取值为0.1的倍数，表示P-P flow中DDoS攻击流量和正常流量的百分比。本文针对不同的δ值分别生成了具有随机起始时间和持续时间的40次DDoS攻击，每次攻击平均影响到2.5个P-P flow。(Src, Dst)表示DDoS攻击从Src个入端口进入，从Dst个出端口流出，这里$Dst=1$表示DDoS攻击只聚集到一个出端口。斜坡函数(Ramp)和指数函数(Exponential)是模拟DDoS攻击流量变化的趋势函数。

表2 DDoS攻击描述参数取值范围

描述参数	持续时间(minute)	攻击强度	异常P-P flow数(Src,Dst)	趋势函数
取值范围	1～30	$0.1\leqslant\delta\leqslant2$	(1,1)～(4,1)	Ramp Exponential

4.2 实验结果比较分析

文献[9]中使用的基于Q-statistic统计的主成分分析(PCA)方法是检测流量矩阵异常的重要基准方法，因此将本文方法和该方法进行比较是十分合适的。该方法首先离线求得流量矩阵序列的主成分，然后计算被检测流量矩阵的均方预测误差(Squared Prediction Error, SPE)，最后设定SPE在置信水平$1-\alpha$上的检测阈值δ_α^2，当$SPE>\delta_\alpha^2$时，认为发生了异常。图2和图3是Kalman方法和PCA方法[9]在检测率、误检率、漏检率和攻击强度上的实验结果比较。检测率即是正确检测到DDoS攻击的百分比，误检率即是正常流量被错误检测为DDoS攻击的百分比，漏检率即是误判为正常的DDoS攻击所占的百分比。

由图2(a)可见，在攻击强度相同情况下PCA方法的漏检率比Kalman方法高很多，随着攻击强度的增加，其漏检率虽然呈减少趋势，但和Kalman方法的差距却在加大。图2(b)则显示，在攻击强度相同情况下Kalman方法的误检率比PCA方法低，而且基本不随攻击强度发生改变。以上情况说明，在攻击强度相同情况下Kalman方法不仅控制误检要好于PCA方法，同时检测率也高于PCA方法。究其原因，PCA方法对正常子空间维度的选择非常敏感，而且需要足够长的流量数据来构造正常子空间，否则会造成数据过拟合，从而降低Q-statistic统计算法检测异常的准确性，导致漏检率和误检率较高。而Kalman滤波方法对参数变化的敏感度低，使用EM算法所求得的参数$\theta=\{\Phi,Q,R\}$值比较稳定，对于突发的异常流量其残差值会显著突出，其次GLR改变点统计算法被普遍用于突发异常的检测，效果理想，所以本实验中随着攻击流量强度的增大，Kalman滤波方法的漏检率会大幅降低，而误检率却维持在较稳定的水平。图3是两种检测方法的ROC(Receiver Operation Characteristic)曲线，ROC曲线是以检测率和误检率作为纵横坐标描绘的检测性能曲线图。当误检率在0～14%范围内时，Kalman方法检测率平均比PCA高8%左右，而当误检率大于14%以后，PCA方法检测率略微超过Kalman方法。但当误检率很低时(0～5%左右)，Kalman方法检测率远比PCA高，而误检率很高时(19%以上)，两种方法的检测率相差无几。考虑到实际检测中误检率越低越好，同时检测率越高越好，Kalman方法在减少误报、提高检测准确性上显然比PCA方法优势明显。下面针对两种方法进行的检测延迟实验更验证了Kalman方法的检测优越性。

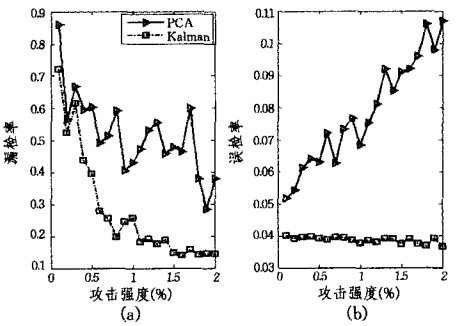

图2 漏检率和误检率分别作为攻击强度的函数

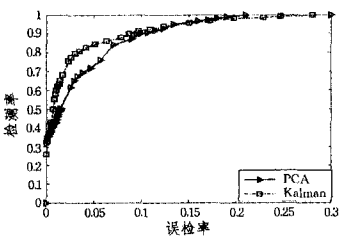

图3 两种检测方法对应的ROC曲线

检测延迟时间是指检测方法在第一时间检测到DDoS攻击时距离攻击开始时的时间长度。两种方法的检测延迟时间累积概率分布结果如图4所示。在所有检测到的攻击中，约30%能够被PCA方法毫无延迟地检测到，约60%能够被Kalman方法毫无延迟地检测到，也就是说，Kalman方法远比PCA方法更容易在攻击的一开始就检测到攻击，而随着延迟的增大，两种方法的检测效果也越来越接近，但Kalman方法始终优于PCA方法。

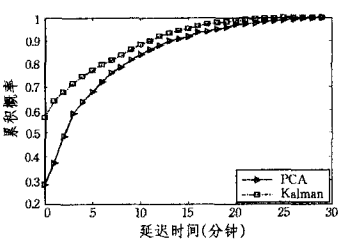

图4 检测延迟时间累积概率分布

结束语 本文根据DDoS攻击的特点，定义了一种更能凸显异常流量的流量类型P-P flow，并以此构建了路由器内部流量矩阵作为检测DDoS攻击的数据源，提出一种基于

Kalman 滤波的方法来检测流量矩阵的异常，然后检测路由器端口是否受到 DDoS 攻击。实验结果表明该方法不仅具有较高的检测率、较低的漏报率，还在检测延迟上具有较大优势。该方法易于获取流量矩阵，也减轻了路由器的流量采集负担，因此具有一定的实用价值。目前该方法仅在仿真实验数据上进行了实验，对于真实网络环境中的流量数据是否具有同样效果是今后的研究内容。由于 P-P flow 可直接从路由器中的 Netflow 记录中统计得到，而不需要考虑多个路由器之间的数据包路由，因此它比 OD flow 更易于实时采集，也易于将该方法推广到大规模网络环境，针对多个关键路由器进行分布式检测，这也是今后的研究重点。

参 考 文 献

[1] Peng T, Leckie C, Rramaohanarao K. Protection from distributed denial of service attacks using history-based IP filtering[C]// Proceedings of the International Conference on Communication (ICC). Anchorage: IEEE, 2003: 482-486

[2] Pu S. Choosing parameters for detecting DDoS attack[C]// Proceedings of the International Conference on Wavelet Active Media Technology and Information Processing. Chengdu: IEEE Computer Society, 2012: 239-242

[3] Chen Y H, Wang K, Ku W S. Collaborative detection of DDoS attacks over multiple network domains[J]. IEEE transactions on parallel and distributed systems, 2007, 18(12): 1649-1662

[4] 莫家庆，胡忠望，林瑜华. 非参数 PCUSUM 算法 DDoS 攻击检测[J]. 计算机工程与应用，2011，47(22)：96-98

[5] 任勋益，王汝传，王海艳. 基于自相似检测 DDoS 攻击的小波分析方法[J]. 通信学报，2006，27(5)：6-11

[6] Thapngam T, Yu S, Zhou W L. DDoS discrimination by linear discriminant analysis (LDA)[C]// Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC). Maui: IEEE Computer Society, 2012: 532-536

[7] Xia Z M, Lu S N, Li J H. DDoS flood attack detection based on fractal parameters[C]// Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing. Shanghai, IEEE, 2012: 1-5

[8] Lakhina A, Papagiannaki K, Crovella M, et al. Structural analysis of network traffic flow[C]// Proceedings of the SIGMETRICS/Performance. New York: ACM, 2004: 61-72

[9] Lakhina A, Crovella M, Diot C. Diagnosing network-wide traffic anomalies[C]// Proceedings of the SIGCOMM'04. Portland: ACM, 2004: 219-230

[10] Ringberg H, Soule A, Rexford J P, et al. Sensitivity of PCA for traffic anomaly detection[C]// Proceedings of the SIGMETRICS'07. San Diego: ACM, 2007: 109-120

[11] Soule A, Salamatian K, Taft N. Combining filtering and statistical methods for anomaly detection[C]// Proceedings of the USENIX Internet Measurement Conference. Philadelphia: ACM, 2005: 331-344

[12] Cisco IOS NetFlow White Papers [EB/OL]. http://www.cisco.com/en/US/products/ps6601/prod_white_papers_list.html, 2006-08-21

[13] Cisco NetFlow Performance Analysis White Papers [EB/OL]. http://www.cisco.com/en/US/technologies/tk543/tk812/tech-nologies_white_paper0900aecd802a0eb9_ps6601_Products_White_Paper.html, 2007-06-15

[14] Hawkinds D M, Qin P H, Kang C W. The changepoint model for statistical process control [J]. Journal of Quality Technology, 2003, 35(4): 355-366

[15] Moore D, Voelker G M, Savge S. Inferring internet Denial-of-Service activity [J]. ACM Transactions on Computer Systems, 2006, 24(2): 115-139

(上接第 171 页)

力进行了重新评估。改正了文献[4]中给出的基于等价结构的错误 5 轮区分器，并综合利用 SNAKE(2)算法原结构与等价结构，构造了一个新的 6 轮 Square 区分器，基于该区分器对 7、8、9 轮的 SNAKE(2)算法应用了 Square 攻击。文献[4]中的 5 轮 Square 区分器采用一种等价结构，本文通过混合采用两种等价结构获得了新的更好的 6 轮 Square 区分器，基于新的 6 轮区分器的攻击结果好于改正后文献[4]中基于 5 轮区分器的攻击结果。在构造 Square 区分器的过程中灵活应用等价结构可期望得到更好的 Square 等价结构区分器以及更好的分析结果。

参 考 文 献

[1] Lee C, Cha Y. The Block Cipher: SNAKE with Provable Resistance against DC and LC attacks 1997[C]// Proceedings of 1997 Korea-Japan Joint Workshop on Information Security and Cryptology (JWISC'97). 1997: 3-17

[2] Moriai S, Shimoyama T, Kaneko T. Interpolation attacks of the block cipher: SNAKE 1999[J]. Lecture Notes in Computer Science, Fast Software Encryption, 1999, 1636: 275-289

[3] Sun B, Qu L, Li C. Impossible Differential Cryptanalysis of SNAKE-2 2009[C]// International Conference on IEEE Networks Security, Wireless Communications and Trusted Computing, 2009. 2009, 2: 63-66

[4] 张鹏，孙兵，李超. 对特殊类型 Feistel 密码的 Square 攻击[J]. 国防科技大学学报，2010，32(4)：137-140

[5] 魏悦川，孙兵，李超. 对简化轮数的 SNAKE(2)算法的中间相遇攻击[J]. 计算机工程与科学，2012，34(6)：28-31

[6] Daemen J, Knudsen L R, Rijmen V. The block cipher SQUARE [J]// Lecture Notes in Computer Science, Fast Software Encryption, 1997, 1267: 149-165

[7] Lei D, Chao L, Feng K. New observation on Camellia [J]. Lecture Notes in Computer Science, Selected Areas in Cryptography, 2006, 3897: 51-64

[8] 唐学海，李超，谢端强. CLEFIA 密码的 Square 攻击[J]. 电子与信息学报，2009，31(9)：2260-2263

[9] 王美一，唐学海，李超，等. 3D 密码的 Square 攻击[J]. 电子与信息学报，2010，32(1)：157-161

[10] Zhang P, Sun B, Li C. Saturation attack on the block cipher HIGHT[C]// Proceeding of the 8th International Conference on Crytology and Network Security. 2009: 76-86

[11] 张鹏，李瑞林，李超. Zodiac 算法新的 Square 攻击[J]. 电子与信息学报，2010，32(11)：2790-2794

[12] 陈华，吴文玲，冯登国. 提高 S 盒非线性度的有效算法[J]. 计算机科学，2005，32(10)：68-70