doi:10.3969/j.issn.1000-436x.2012.z1.035

基于流角色检测 P2P botnet

宋元章[1]，何俊婷[2]，张波[1]，王俊杰[1]，王安邦[1]
(1.中国科学院 长春光学精密机械与物理研究所，吉林 长春 130033；
2.中国第一汽车股份有限公司 技术中心汽车电子部电控产品设计室，吉林 长春 130011)

摘 要：提出了一种基于流角色的实时检测 P2P botnet 的模型，该模型从流本身的特性出发，使其在检测 P2P botnet 时处于不同的角色，以发现 P2P botnet 的本质异常和攻击异常，同时考虑到了网络应用程序对检测的影响。为进一步提高检测精度，提出了一种基于滑动窗口的实时估算 Hurst 指数的方法，并采用 Kaufman 算法来动态调整阈值。实验表明，该模型能有效检测新型 P2P botnet。

关键词：P2P botnet；自相似性；multi-chart CUSUM；Kaufman
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0262-08

Detecting P2P botnet based on the role of flows

SONG Yuan-zhang[1], HE Jun-ting[2], ZHANG Bo[1], WANG Jun-jie[1], WANG An-bang[1]
(1. Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China;
2. Electronic Control Automotive Electronics Department, Ltd R&D Center, China FAW Co., Changchun 130011,China)

Abstract: Towards the weaknesses of the existing detection methods of P2P botnet, a novel real-time detection model based on the role of flows was proposed, which was named as RF. According to the characteristics of flows, the model made the flows play the different roles in the detection of the P2P botnet to detect the essential abnormality and the attacking abnormality. And the model considered the influence on the detection of the P2P botnet which the Web applications generated, especially the applications based on the P2P protocols. To minimize the false positive rate and false negative rate, a real-time method based on the sliding window to estimate the Hurst parameter was proposed, and the Kaufman algorithm was applied to adjust the threshold dynamically. The experiments showed that the model was able to detect the new P2P botnet with a relatively high precision.

Key words: P2P botnet; self-similarity; multi-chart CUSUM; Kaufman

1 引言

僵尸网络（botnet）是攻击者(botmaster)通过 bot 程序控制的恶意计算机群。它是从传统恶意代码形态进化而来的目前对 Internet 最有效的攻击方式。攻击者可以通过改变 botnet 的负载方便地发起 DDoS 攻击、发送垃圾邮件(spamming)等。非集中控制的分散式网络结构将是 botnet 未来的发展趋势。2007 年出现的 Storm botnet 是新型 P2P botnet 的代表，它使用基于 P2P 的 Overnet/eDonkey 网络维持 C&C(command and control)[1]。

新型分散式 botnet 将 P2P 网络的分散式拓扑结构引入到 botnet 的 C&C 机制中，在整个 botnet 中没有控制中心，即使一部分 bot 节点被剔除，剩余

收稿日期：2012-06-20
基金项目：国家自然科学基金资助项目（90204014）；激光与物质相互作用国家重点实验室研究基金资助项目（SKLLIM0902-01）
Foundation Items: The National Natural Science Foundation of China (90204014); The State Key Laboratory Laser Interaction with Material Research Fund (SKLLIM0902-01)

的 bot 节点仍能构成有效的攻击网络，因此针对传统的集中式 botnet 的单个控制中心的检测和防御方法已经失效。新型 P2P botnet 的检测已成为当前网络安全研究的重大问题。

在详细分析 Storm botnet 行为与特征的基础上，本文提出了一种新型的基于流角色的实时检测 P2P botnet 模型—RF。流角色是指基于网络流自身的特性所决定的其在检测 P2P botnet 时所起的作用，假设 P2P botnet 发动攻击时会导致某种网络流的异常，那么就可通过检测该网络流的特征来检测 P2P botnet 导致的“攻击异常”，这就可以看作是该网络流在检测 P2P botnet 时的角色。本文提出的 RF 模型从流本身的特性出发，使其在检测 P2P botnet 时处于不同的角色，以发现 P2P botnet 的本质异常和攻击异常：通过对 UDP 流和 ICMP 流的处理发现 botnet 的固有特征导致的“本质异常”，因为 UDP 流和 ICMP 流与 botnet 的 C&C 机制直接相关；通过对 SMTP 流的处理发现是 botnet 的攻击流导致的异常，因为 P2P botnet 经常用来发动垃圾邮件攻击，从而导致 SMTP 流的异常；考虑到网络应用程序对检测的影响，利用 TCP 流的特征来区分流量异常是由网络应用程序引起的还是因为爆发 P2P botnet 引起的。为了进一步降低检测的误报率和漏报率，本文提出了一种基于滑动窗口的实时估算 Hurst 指数的方法，并且采用 Kaufman 算法来动态调整阈值。实验表明，该模型能够有效检测新型 P2P botnet，适应更复杂的网络环境。

2　相关研究

目前，对新型分散式 P2P botnet 的分析和检测研究刚刚展开。

Grizzard J B 等人[2]对 P2P botnet 的特征进行了详细分析，以 Storm botnet 为例对其感染、传播和通信机制进行了深入研究和阐述，对以后的研究工作有很大的启发意义。

Sarat S 等人[3]和 Holz T 等人[4]使用类似的方法分析 Storm botnet。前者的研究结果表明 Storm 的 Peer ID 非常不规律，有很多不可达的 IP 地址，为检测和防御提供了一定的基础。后者通过发布伪造的 key 来混淆 bot 主机间的通信以抑制 botnet 规模。

STEGGINK M 等人[5]通过对比 Storm 与其他软件的流量情况，提出了基于网络特征（例如 Storm 分组特定长度）的检测方法。

Phillip Porras 等人[6]通过分析 Storm 会话特征，提出通过使用 BotHunter 对会话和交互过程进行模式匹配以检测 P2P botnet 的方法。

王海龙等人[7]提出了一种 botnet 检测层次协同模型，它能够在信息、特性以及决策 3 个级别上进行协同。

王劲松等人[8]提出了一种基于组特征过滤器的检测 botnet 的方法，使用多个成员特征对内网主机数据分组进行过滤，可以在不需要开发新的模式匹配算法的前提下实现对 bot 主机间的通信数据的识别以检测 bot 主机。

考虑到僵尸网络的迁移问题，臧天宁[9]等人关注的是不同的僵尸群之间的关系，利用云模型对僵尸群的通信特征进行分析，从而判断它们是否属于同一个僵尸网络。

诸葛建伟等人[10,11]分析和总结了 botnet 的演化过程，国内外目前跟踪、检测和防御 botnet 的方法，并对 botnet 的发展趋势和进一步的研究方向进行了探讨。

综上所述，当前 P2P botnet 分析和检测研究仍处于初期阶段，主要存在以下问题。

1) 对于网络流采取类似的处理方法，忽视了网络流本身的特性，使得它们在 P2P botnet 检测中的充当相同的角色：UDP 流异常是 botnet 的 C&C 过程导致的，这是 botnet 本质的流量异常；ICMP 流异常是 bot 主机固有的 bootstrap 过程导致的，这也是 botnet 本质的流量异常；SMTP 流异常是攻击者利用 botnet 发送大量垃圾邮件导致的，这是 botnet 的攻击流导致的异常，所以不同种类的流在检测 P2P botnet 时应处于不同的角色。

2) 没有考虑到网络应用程序，尤其是 P2P 应用对 P2P botnet 检测的影响。从本质上看，P2P botnet 是一个可以发动网络攻击的 P2P 网络，所以两者有较强的相似性，因此正常 P2P 应用对 P2P botnet 的检测会产生很大的误差影响。

3　Storm botnet 分析

Storm botnet 是 P2P botnet 的典型代表，其生命周期如下。

1) 侵染受害主机。

① 通过传播 bot 程序侵染网络中易感主机。

② bootstrap 过程：主机感染 bot 程序后，会周期性通过连接相应 bot 节点尝试加入 P2P botnet。

③ 二次注入过程：bot 主机通过 P2P 网络查询

事先约定的 key 以下载攻击负载、更新自身代码和更新 P2P 节点列表等。

④ keep alive：bot 主机通过定期与其他 bot 主机通信来保证其一直处于 P2P botnet 中。

2) 攻击者发送攻击命令，以催动 botnet 中的 bot 主机执行攻击负载向攻击目标发动攻击。

这些过程中有几个流量方面的特征。

1) UDP 流主要用来 C&C：在 botnet 中 keep alive、发现其他 bot 节点等，这会导致 UDP 流大量增加，由于 botnet 固有的特性 C&C 过程导致的 UDP 流异常是 botnet 的本质异常。

2) 在 bootstrap 过程中，bot 主机会随机连接某些 bot 节点，这时会发生较多的连接失败，导致 ICMP 流异常，这是 botnet 固有的特性（bot 主机的 bootstrap 过程）导致的本质异常。

3) bot 主机发送大量垃圾邮件会大量使用 SMTP 协议[5]进而导致 SMTP 流异常，这是 botnet 发动的攻击流导致的异常。

因此，对于网络流应从流本身的特性出发，使其在检测 P2P botnet 时处于不同的角色，不应不做区分就做相似的处理。在第 4 章将从流本身的特性出发，使其在检测 P2P botnet 时处于不同的角色，分别检测 P2P botnet 的本质异常和攻击异常，并用一定的手段消除正常 P2P 应用对 P2P botnet 的检测产生的误差影响。

4 RF 模型

4.1 发现 P2P botnet 的本质异常

4.1.1 C&C 机制导致的异常

由第 3 节知，C&C 过程是 botnet 的根本，而 UDP 流是 botnet 进行 C&C 过程的主要手段，尽管实现 C&C 过程的 P2P 协议和 botnet 发动的攻击多种多样，但是从 UDP 流的角度来看是类似的，所以 UDP 流异常是最能反映 botnet 流量特征的本质异常。在 RF 模型中，通过检测 UDP 流的异常来发现 botnet 的本质异常，首先采用反映网络自相似性的 Hurst 指数来获取 UDP 流的情况以发现其异常，再将处理后的数据输入到 Multi-chart CUSUM 中以提高检测的灵敏度。

4.1.1.1 网络自相似性

近年来，许多研究发现，相比于传统短时相关模型，网络流量自相似性过程能更好地描述网络流量的特征[12,13]。特别地，KIM J S 等人[14]研究发现 UDP 流有明显的自相似性，这是 UDP 流自身所固有的特征。

自相似性指的是总体结构和局部结构在某种程度上有一致性。网络流量可以看作是在时间维度上具有自相似性的时间序列。

若对所有的 $a>0$，一个连续时间随机过程 $X(t)$ 都有

$$X(t)=a^{-H}X(at) \tag{1}$$

式(1)中的等号代表统计意义上的相等，则 $X(t)$ 具有自相似性。式(1)中的参数 $H(0.5\leqslant H<1)$称为 Hurst 指数，反映自相似的程度。自相似程度越低，H 值越接近 0.5。

假设当前时刻为 k，定义

$$HP_k=1-Hurst_k \tag{2}$$

由第 3 节知，Storm 会导致 UDP 分组增多，而且 bot 主机在 bootstrap、keep alive 时，会周期性地与某些 bot 节点联系，这会导致 UDP 流自相似性的减弱，进而引起 Hurst 值减小，HP_k 增大，故可通过检测参数 HP_k 来发现这些异常：首先对 UDP 流量采样，然后计算其 Hurst 值，再计算参数 HP_k，当 HP_k 增大时表示 UDP 流发生了异常。计算 Hurst 指数的方法详见 4.1.1.2 节。为了提高检测的灵敏度，将 HP_k 输入到 Multi-chart CUSUM 中以放大异常，详见 4.1.2 节。

4.1.1.2 一种基于滑动窗口的实时估算 Hurst 指数的方法

Karagiannis 等人[15,16]对估算 Hurst 指数的方法研究发现，相比于小波分析法(abry-veitch method)和周期图法(periodogram method), R/S 法(rescaled range method)受噪声等因素的影响更小，具有更好的稳定性，因此本文使用 R/S 法。为了进一步提高估算的精度，保证实时性，本文对 R/S 方法进行了改进，提出了一种基于滑动窗口的实时估算 Hurst 指数的方法，如图 1 所示。

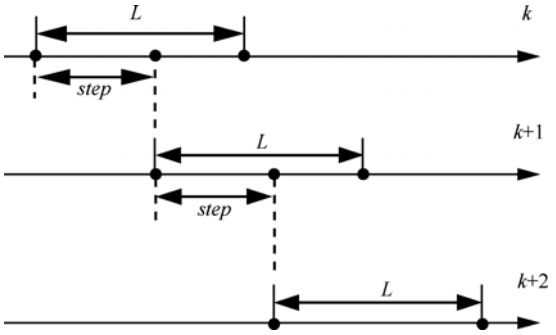


图 1 滑动窗口示意

假设滑动窗口的长度为 L，每使用 R/S 法估算一次 Hurst 指数需要一个滑动窗口大小的时间序列，每估算完一次 Hurst 指数后向前滑动步长 *step*, 即：使用原先的 *L-step* 长度的数据和新采样的 *step* 长度的数据计算下一个 Hurst 指数。

假设长度 L 的时间序列为$\{X_1,\cdots,X_L\}$，利用 R/S 法估算 Hurst 值的过程具体如下：将该时间序列划分成长度为 n 的子序列，那么得到子序列的个数 $d=L/n$。对于每一个子序列 $m=1,\cdots,d$。

1) 求其期望 E_m：

$$E_m=\frac{1}{n}\sum_{i=(m-1)n+1}^{mn}X_i \tag{3}$$

2) 求其标准差 S_m：

$$S_m=\sqrt{\frac{1}{n}\sum_{i=(m-1)n+1}^{mn}(X_i-E_m)^2} \tag{4}$$

3) 求其极差 R_m：

$$R_m=\max_{1\leqslant i\leqslant n}\{Z_{i,m}\}-\min_{1\leqslant i\leqslant n}\{Z_{i,m}\} \tag{5}$$

$$Z_{i,m}=\sum_{j=1}^{i}(Y_{j,m}-E_m)=\sum_{j=1}^{i}Y_{j,m}-iE_m \tag{6}$$

$Y_{j,m}$ 代表第 m 个子序列第 j 个元素的值。$Z_{i,m}$ 代表第 m 个子序列前 i 个元素与 E_m 偏差的累计。

4) 求各子序列的 $R_m/S_m(m=1,\cdots,d)$ 的期望

$$(R/S)_n=\frac{1}{d}*\sum_{m=1}^{d}(R_m/S_m) \tag{7}$$

研究表明，$(R/S)_n$ 与子序列长度 n 的关系可表示为

$$(R/S)_n=Cn^H \tag{8}$$

C 为常数，H 为 Hurst 值(式(8)中的等号代表统计意义上的相等)。

式(8)两边取对数得

$$\log(R/S)_n=\log C+H\log n \tag{9}$$

对于一个给定的 n 值，可得一个 $(R/S)_n$。对于不同的 n 值，若以 $\log n$ 为横坐标，$\log(R/S)_n$ 为纵坐标，则在直角坐标系中可得到许多点，那么 Hurst 指数的估算值就是进行直线拟合后所得直线的斜率。

4.1.2 Bootstrap 过程导致的异常

在 bootstrap 过程中，bot 主机会随机连接某些 bot 节点，这时会发生较多的连接失败，导致 ICMP 流异常，这是 botnet 固有的特性导致的本质异常。

在 RF 模型中，通过利用 Multi-chart CUSUM 来检测 ICMP 流的异常以检测该 botnet 本质异常。

一维非参数 CUSUM 算法已经在异常检测和改变点检测方面有广泛的应用，本文将其扩展为 Multi-chart CUSUM[17]，它可以同时考虑网络流量多种特征，放大流量异常，以提高检测的灵敏度。

对于随机序列 $\{X_1,\cdots,X_n\}$，令 P_k^i 代表第 $i(i=1,\cdots,n)$个观测序列在 k 时刻检测到异常，P_∞ 代表未检测到异常。$\sum_{s=k}^{n}g_{i,s}(X_i(1),\cdots,X_i(s))$ 代表 P_k^i 的累计评价，第 i 个观测序列的累计评价和 $S_n(i)$为

$$S_n(i)=\left\{\max_{1\leqslant k\leqslant n}\sum_{s=k}^{n}g_{i,s}(X_i(1),\cdots,X_i(s))\right\}^+ \tag{10}$$

其中，$x^+=\begin{cases}x, & x>0\\ 0, & x\leqslant 0\end{cases}$。

为使用 CUSUM 算法，需要对 $g_{i,s}(X_i(n))$ 做如下变换，使得正常情况下观测序列的均值为负数，在变化发生后其均值为正数：

$$g_{i,s}(X_i(n))=X_i(n)-\mu_i-\eta_i \tag{11}$$

式(11)中，$\mu_i=E_\infty X_i(n)$ 代表在正常情况下观测序列的均值。可将式（10）递归表示如下：

$$\begin{aligned}&S_n(i)=\{S_{n-1}(i)+X_i(n)-\mu_i-\eta_i\}^+\\&S_0(i)=0\end{aligned} \tag{12}$$

定义判定函数

$$d_M(S_n(i))=\begin{cases}1, & S_n(i)>M\\ 0, & S_n(i)\leqslant M\end{cases} \tag{13}$$

当 $S_n(i)$ 大于阈值时，表示发生异常。为了提高检测精度，使用 Kaufman 算法[18]动态调整 M。

当上述的随机序列$\{X_1,\cdots,X_n\}$是 ICMP 流的比例值 C_{ICMP} 和 UDP 流在第一阶段处理后的结果 HP_k 时，Multi-chart CUSUM 可以及时检测到 ICMP 流和 UDP 流的异常。

4.2 发现攻击流导致的异常

Bot 主机在发送大量垃圾邮件时会大量使用 SMTP 协议进而导致 SMTP 流异常，这是 botnet 发动的攻击流导致的异常。在 RF 模型中，通过检测 SMTP 流的异常来发现 botnet 的攻击异常，对于 SMTP 流采用与 ICMP 流相同的处理方式，详见 4.1.2 节。

4.3 区分异常产生的原因

从本质上看，P2P botnet 是一个可以发动网络

攻击的 P2P 网络，所以 P2P botnet 和 P2P 应用程序有较强的相似性，应采用一定的手段消除正常 P2P 应用对 P2P botnet 的检测产生的误差影响。

正常 P2P 应用大多用来进行文件的传输和共享，通常利用超过 1 300byte 的 TCP 长分组传输数据。而 botnet 大多数的数据传输是二次注入时下载负载利用 HTTP 协议进行的，数据量不大。因此，可利用时间 Δt 内剔除与正常网络应用程序相关的 TCP 分组后的 TCP 长分组的比例 P_{TCP} 来区分导致第 3 节中流量异常出现的原因，TCP 长分组的比例越小，异常是 P2P botnet 爆发引起的概率越大。

假设当前要处理的 TCP 分组记为 P_i，TCP 分组的数目为 N，TCP 长分组的数目为 N_{TCP}，具体处理过程如图 2 所示。

定义判定函数

$$f_{\mathrm{TCP}}=\begin{cases}1, & P_{\mathrm{TCP}}<M_{\mathrm{TCP}}\\ 0, & P_{\mathrm{TCP}}\geqslant M_{\mathrm{TCP}}\end{cases} \tag{14}$$

f_{TCP} 值为 1，说明第 3 节中流量异常是 P2P botnet 爆发引起的概率较大。阈值 M_{TCP} 可通过 Kaufman 算法[18]进行动态修改。

4.4　RF 模型的流程

假设当前时刻为 k，RF 模型处理流程如图 3 所示。

1) 获取 ICMP 流的比例值 C_{ICMP}、SMTP 流的比例值 C_{SMTP} 和 UDP 流的比例值 C_{UDP}，同时计算得出 TCP 流的 f_{TCP} 值，以消除网络应用对 P2P botnet 检测产生的误差影响。

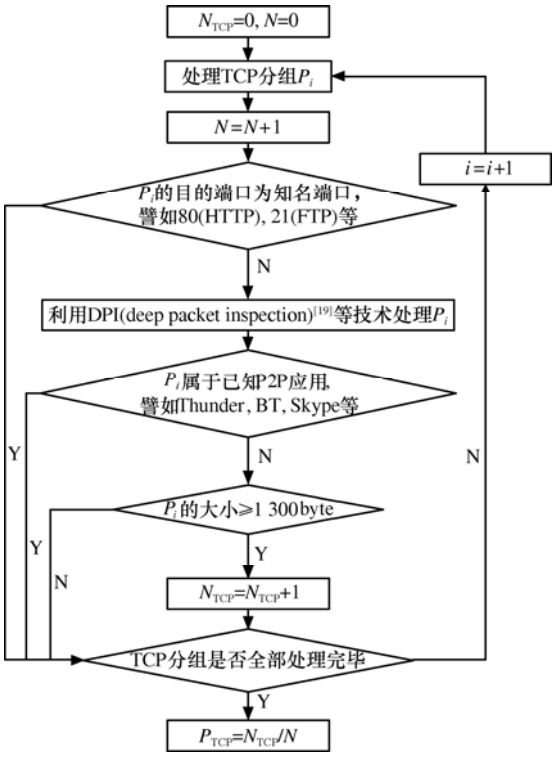


图 2　处理 TCP 流的流程

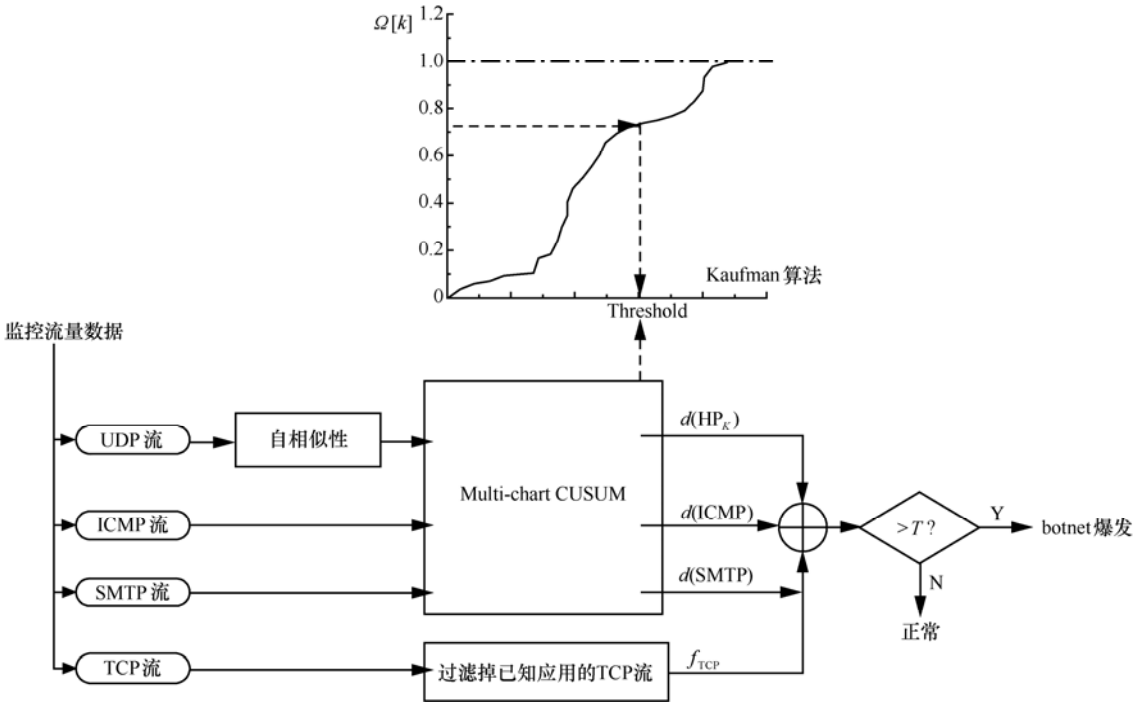


图 3　RF 模型示意

2) 从流本身的特性出发，使其在检测 P2P botnet 时处于不同的角色，发现 botnet 导致不同的流量异常。

① 利用基于滑动窗口的实时估算 Hurst 指数的方法得到 HP_k；

② 将 C_{ICMP}、C_{SMTP} 和 HP_k 输入到 Multi-chart CUSUM 中计算出 $d(S_i(ICMP))$、$d(S_i(SMTP))$ 和 $d(S_i(HP_k))$。

3) 最终判定：

$$\begin{aligned} D_k &= \alpha_k d(S_n(ICMP)) + \beta_k d(S_n(SMTP)) + \\ &\quad \gamma_k d(S_n(HP_k) + \theta_k f_{\mathrm{TCP}} \\ \alpha_k &+ \beta_k + \gamma_k + \theta_k = 1 \end{aligned} \tag{15}$$

T 是判定 P2P botnet 是否存在的阈值，当 $D \leqslant T$ 时表示网络状态正常，否则表示 P2P botnet 存在。

5　实验

5.1　网络流量实验

该实验主要是监测网络流量：每 10s 采集一次网络数据分组，在一段时间后注入 Storm bot 程序。

分析图 4 可得，当 bot 主机开始通信时，UDP 分组数目比一般情况下增多了 20 倍左右，主要因为 botnet 的 C&C 机制通过 UDP 流进行。ICMP 分组数目从 100 增加到 900，主要因为 bot 主机在 bootstrap 过程连接某些 bot 节点时发生了较多的连接失败。因为 botnet 在 Spamming 时发送垃圾邮件的延迟，该实验几乎未发现 SMTP 流，所以接下来的实验暂不考虑 SMTP 流。

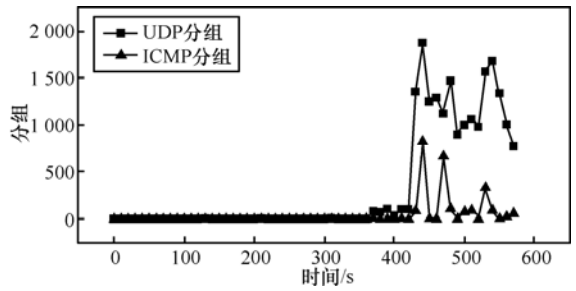


图 4　网络流量数据

5.2　参数 *HP* 实验

该实验主要观测 UDP 流自相似性程度的变化。一般情况下 UDP 流自相似性程度非常明显，Hurst 指数保持在[0.65, 0.85]，参数 *HP* 保持在[0.15, 0.35]，同时会有一定的波动。

分析图 5 可得，在一段时间注入 Storm bot 程序后，参数 *HP* 在 420s 增大到了 0.45，在 460s 甚至增大到了最高点 0.59，这充分说明 UDP 流已经丧失了自相似性，出现了异常。因为 bot 主机数目的逐步增大，P2P botnet 规模的逐步扩大，原先 UDP 流表现出的与一般情况不同的异常特征却变成了它的一种新的自相似性行为，进而导致参数 *HP* 下降。

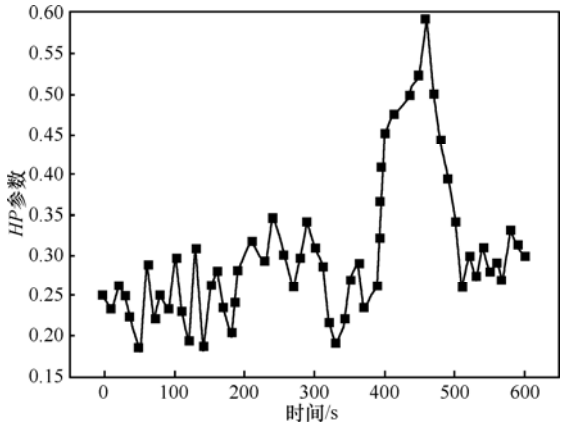


图 5　UDP 流的 *HP* 参数

5.3　RF 模型实时性实验

将实验 1 中 UDP 流、ICMP 流输入到 RF 模型中的处理结果如图 6 所示。与实验 1 相比，图 6 中检测到 UDP 分组和 ICMP 分组增加的时刻均有一定的延迟，基本在[25s,50s]区间内。因此，RF 模型具有较小的检测延迟，可以满足实时检测 P2P botnet 的要求。

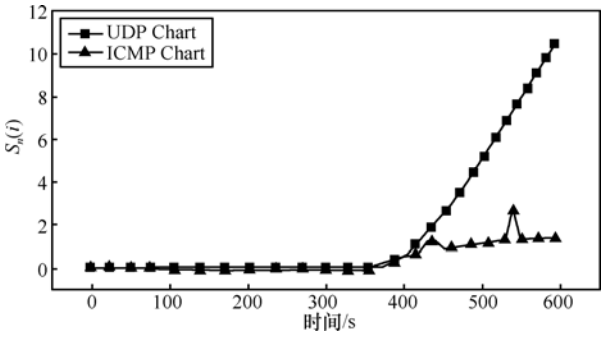


图 6　基于 UDP 流和 ICMP 流的 RF 的输出

5.4　漏报率和误报率实验

为检验本文提出的 RF 模型在不同情况下的检测能力，该实验选择了 4 组数据，分别使用不同的检测方法检测 botnet：前 2 组未注入 bot 程序，仅仅改变了各种数据分组的流量比，其中第 2 组数据中有大量网络应用程序和 P2P 应用程序的数据分组；后 2 组注入了 bot 程序，其中第 4 组数据有大

量网络应用程序和 P2P 应用程序的数据分组。实验结果如表 1 所示。

表 1　　漏报率和误报率对比

检测方案	No.1	No.2	No.3	No.4
真实情况	0	0	100	100
UDP	11	42	79	143:69
ICMP	16	20	61	135:57
SMTP	11	14	68	105:63
RF	5	3	92	113:77

在第 1 组和第 3 组数据中 RF 模型的检测结果非常理想，接近真实情况。第 2 组数据和第 4 组数据分别是在正常和存在 bot 程序的网络环境中注入了大量网络应用程序和 P2P 应用程序的数据分组，此时所有的检测方法都出现了一定的漏报和误报，但是 RF 模型的漏报率和误报率较低，因为 RF 模型充分考虑到了网络中正在运行的应用程序对 P2P botnet 检测的影响。特别地，表中的“113:77”表示 RF 模型在第 4 组数据中检测到了 113 次攻击，但是其中有 77 次是真正的攻击。

综上所述，利用 RF 模型检测 P2P botnet，其表现出较低的漏报率和误报率，具有较小的检测延迟。

6　结束语

本文在详细分析 Storm botnet 行为与特征的基础上，提出了一种新型的基于流角色的实时检测 P2P botnet 模型—RF，该模型从流本身的特性出发，使其在检测 P2P botnet 时处于不同的角色，同时考虑到了网络应用程序对检测的影响。为了进一步减小检测的漏报率和误报率，本文提出了一种基于滑动窗口的实时估算 Hurst 指数的方法，并且采用 Kaufman 算法来动态调整阈值。实验表明，该模型能够有效检测新型 P2P botnet，检测的误报率和漏报率较低，适应更复杂的网络环境。

下一步的研究重点，更详细地研究 P2P 应用与 P2P botnet 流量特征的差异，进一步提高检测的精度和实时性。

参考文献：

[1] JOE STEWART. Storm Worm DDOS Attack[R]. SecureWorks, Inc, Atlanta GA, 2007.

[2] GRIZZARD J B, SHARMA V, NUNNERY C. Peer-to-peer botnets: overview and case study[A]. HotBots ’07 conference[C]. 2007.

[3] SARAT S, TERZIS A. Measuring the Storm Worm Network[R]. Technical Report 01-10-2007, HiNRG Johns Hopkins University, 2007.

[4] HOLZ T, STEINER M, DAHL F. Measurements and mitigation of peer-to-peer-based botnets: a case study on storm worm[A]. 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats[C]. San Francisco, 2008.

[5] STEGGINK M, IDZIEJCZAK I. Detection of Peer-to-Peer Botnets[R]. University of Amsterdam, Netherlands, 2007.

[6] PORRAS P, SAIDI H, YEGNESWARAN V. A multi-perspective analysis of the storm (peacomm)worm[A]. Computer Science Laboratory, SRI International[C]. CA, 2007.

[7] 王海龙, 胡宁, 龚正虎. Bot_CODA:僵尸网络协同检测体系结构[J]. 通信学报, 2009, 30(10A): 15-22.
WANG H L, HU N, GONG Z H. Bot_CODA: botnet collaborative detection architecture[J]. Journal on Communications, 2009, 30(10A): 15-22.

[8] 王劲松，刘帆，张健. 基于组特征过滤器的僵尸主机检测方法的研究[J]. 通信学报, 2010, 31(2): 29-35.
WANG J S, LIU F, ZHANG J. Botnet detecting method based on group-signature filter[J]. Journal on Communications, 2010, 31(2): 29-35.

[9] 臧天宁, 云晓春, 张永铮. 僵尸网络关系云模型分析算法[J]. 武汉大学学报(信息科学版), 2012, 37(2): 247-251.
ZANG T N, WANG X CCC, ZHANG Y Z. A botnet relationship analyzer based on cloud model[J]. Geomatics and Information Science of Wuhan University, 2012, 37(2): 247-251.

[10] 诸葛建伟, 韩心慧, 周勇林. 僵尸网络研究[J]. 软件学报, 2008, 19(3): 702-715.
ZHUGE J W, HAN X H, ZHOU Y L. Research and development of botnets[J]. Journal of Software, 2008, 19(3): 702-715.

[11] 江健, 诸葛建伟, 段海新. 僵尸网络机理与防御技术[J].软件学报, 2012, 23(1): 82-96.
JIANG J, ZHUGE J W, DUAN H X. Research on botnet mechanisms and defenses[J]. Journal of Software, 2012, 23(1): 82-96.

[12] LELAND W E, TAQQU M S, WILLINGER W. On the self-similar nature of Ethernet traffic(extended version)[J]. IEEE/ACM Trans on Networking, 1994, 2(1): 1-15.

[13] BERAN J, SHERMAN R, TRAQQU M S. Long range dependence in

variable bit rate video traffic[A]. IEEE Trans on Communication[C]. 1995, 43(234): 1566-1579.

[14] KIM J S, KAHNG B, KIM D. Self-similarity in fractal and non-fractal networks[J]. Journal of the Korean Physical Society, 2008, 52: 350-356.

[15] KARAGIANNIS T, MOLLE M, FALOUTSOS M. Understanding the Limitations of Estimation Methods for Long-range Dependence[R]. University of Califomia,Tech ReP:TRUCR-CS-2006-10245,2006.

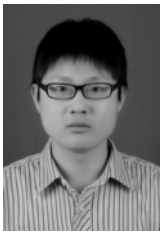
[16] KARAGIANNIS T, MOLLE M, FALOUTSOS M. Long-range dependence: Ten years of Internet traffic modeling[J]. IEEE Intenet Computing, 2004,8(5):57-64.

[17] TARTAKOVSKY A G, ROZOVSKII B, SHAH K. A Nonparametric Multichart CUSUM test for rapid intrusion detection[A]. Proceedings of Joint Statistical Meetings[C]. 2005.

[18] KASERA S, PINHEIRO J, LOADER C. Fast and robust signaling overload control[A]. Proceedings of Ninth International Conference on Network Protocols[C]. 2001. 323-331.

[19] SEN S, SPATSCHECK O, WANG D M. Accurate, scalable in-network identification of P2P traffic using application signatures[A]. Proceedings of the 13th international conference on World Wide Web[C]. New York, 2004.512-521.

作者简介：



宋元章（1986-），男，山东潍坊人，硕士，中国科学院长春光学精密机械与物理研究所实习员，主要研究方向为分布式计算、网络安全等。

何俊婷（1985-），女，黑龙江牡丹江人，硕士，中国第一汽车股份有限公司技术工程师，主要研究方向为车载网络、网络安全等。

张波（1974-），女，吉林长春人，博士，中国科学院长春光学精密机械与物理研究所副研究员，主要研究方向为软件测试及系统检测。

王俊杰（1979-），男，吉林长春人，博士，中国科学院长春光学精密机械与物理研究所副研究员，主要研究方向为软件测试及测试环境。

王安邦（1987-），男，山东临沂人，硕士，中国科学院长春光学精密机械与物理研究所实习员，主要研究方向为软件测试等。