DOI：10.7652/xjtuxb201302003

入侵检测系统利用信息熵检测网络攻击的方法

夏秦，王志文，卢柯
（西安交通大学电子与信息工程学院，710049，西安）

摘要：针对传统入侵检测系统报警事件数量多、误报率高的问题，提出了一种基于信息熵的网络攻击检测方法。该方法利用雷尼熵对报警事件源IP地址、目标IP地址、源威胁度、目标威胁度以及数据报大小这5个属性香农熵的融合结果来表示网络状态，通过与正常网络状态的对比识别网络异常。真实攻击和人工合成攻击环境中的实验结果表明，该方法能在保持误报率低于1%的情况下命中率高于90%；与基于特征香农熵的攻击检测方法相比，该方法对攻击更敏感，最易检测出DoS攻击和主机入侵，其次是主机扫描和端口扫描，对蠕虫攻击的检测敏感度稍差。对比测试结果表明，该方法在提高命中率的同时，还能有效降低误报率。

关键词：网络攻击；入侵检测系统；香农熵；雷尼熵
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2013)02-0014-06

A Method to Detect Network Attacks Using Entropy in the Intrusion Detection System

XIA Qin, WANG Zhiwen, LU Ke
(School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, China)

Abstract: A method to detect network attacks using entropy is proposed to solve the problem that the existing intrusion detection system (IDS) typically generates large amounts of alerts with high false rate. Rainey cross entropy is employed to fuse the Shannon entropy vector for five properties of alerts. These five properties are source IP address, destination IP address, source threat, target threat and datagram length. Then the fusing result is used to describe the network state, and is compared with the normal network state to identify the anomalies. The experimental results on actual network attacks data and synthetic attacks show that the proposed approach can detect network attacks with a hit rate more than 90% whereas the false rate is less 1%. Comparisons with the attack detection method based on the characteristics of the Shannon entropy show that the proposed method is more sensitive to attacks, and is easier to detect in the order Denial of Service (DoS) and hosts intrude attacks, and then the hosts scan and port scan attacks, however, is relatively difficult to worm attacks. The test results also show that the proposed method is better than the compared systems with higher hit rate and lower false positives.

Keywords: network attack; intrusion detection system; Shannon entropy; Rainey entropy

入侵检测系统(IDS)是用于监测网络和/或系统行为中是否存在恶意或违反策略行为，并向控制台产生检测报告的设备或软件[1]。虽然目前的IDS具有强大的攻击监测能力，但多数IDS仍然存在报

收稿日期：2012-04-09。 作者简介：夏秦(1973—)，女，博士，讲师。 基金项目：国家自然科学基金资助项目(60970121)。
网络出版时间：2012-10-31 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20121031.1103.008.html

警事件数量较大和误报率较高的问题。Gina 等人通过 Snort 对 1999 DARPA 数据集的测试,得出 69%的报警事件都是误报[2]。解决这个问题的方法主要分为 2 类:一类是合理配置入侵检测系统的规则[3];另一类是以事后处理的方式加强报警管理或者挖掘报警关联[4-7]。与前一类方法相比,后一类方法人工参与较少,适用面更广。

熵理论目前被广泛应用于信息安全领域的数据分析和异常检测。与传统信息熵相比,相对熵和互雷尼信息熵对异常检测往往具有更好的检测效果[8]。本文从事后处理的角度出发,针对 Snort 产生的报警事件集,利用互雷尼信息熵对 5 个报警事件的特征香农熵进行融合,并以该结果反映网络状态,并通过与正常网络状态的比较,能够较准确地判断是否存在网络异常。测试实验分别在真实和合成攻击环境中进行,通过改变 5 种不同合成攻击的强度,比较了本文方法与基于特征香农熵检测方法以及与文献[6]中系统的检测效果。

1　报警事件特征

1.1　报警事件特征选取

传统的基于流量分析的网络攻击检测方法大都采用 IP 地址、端口和网络流大小分布作为网络流量特征[1]。本文的数据对象是 Snort 产生的报警事件,每条报警事件都有表示事件严重程度的优先级属性,其值从 1 到 4,威胁程度依次减弱(high,medium,low,info)。因此,本文选取的报警事件特征包括每个源和目的 IP 地址对应的报警事件数、报警事件的威胁度以及能够反映网络流大小并触发报警规则的数据报字节数。由于报警事件相对于原始流量较为精简,相关端口变化较小,随机性较强,统计特征较差,因此没有选取端口作为报警事件特征。

1.2　报警事件特征分析

假设在时间窗口 δ 内产生了 n 条报警事件,则该报警事件集合表示为

$$A=\{a_1,a_2,\cdots,a_n\} \tag{1}$$

若所有报警事件的源和目标 IP 地址的数量分别为 m 和 k,则源和目标 IP 地址的集合表示为

$$P_S=\{p_{S,1},p_{S,2},\cdots,p_{S,m}\} \tag{2}$$

$$P_D=\{p_{D,1},p_{D,2},\cdots,p_{D,k}\} \tag{3}$$

若来自 $p_{S,i}$ 的报警事件数为 $n_{S,i}$,发向 $p_{D,i}$ 的报警事件数为 $n_{D,i}$,则每个源和目标 IP 地址对应的报警事件数分别为

$$N_S=\{n_{S,1},n_{S,2},\cdots,n_{S,m}\} \tag{4}$$

$$N_D=\{n_{D,1},n_{D,2},\cdots,n_{D,k}\} \tag{5}$$

为了突出报警事件威胁程度对异常检测的影响,使用 $t_i=5^{(4-q_i)}$ 表示 a_i 的威胁度,其中 q_i 表示 a_i 的报警程度优先级的属性值。若所有来自 $p_{S,i}$ 的报警事件威胁度之和为 $t_{S,i}$,所有发向 $p_{D,i}$ 的报警事件威胁度之和为 $t_{D,i}$,则源和目标 IP 地址的威胁度表示为

$$T_S=\{t_{S,1},t_{S,2},\cdots,t_{S,m}\} \tag{6}$$

$$T_D=\{t_{D,1},t_{D,2},\cdots,t_{D,k}\} \tag{7}$$

若 x 是不同长度数据报的个数,则报警事件集合 A 对应的数据报长度集合表示为

$$L=\{l_1,l_2,\cdots,l_x\} \tag{8}$$

若数据报长度为 l_i 的报警事件数为 m_i,则不同数据报长度对应的报警事件数为

$$M=\{m_1,m_2,\cdots,m_x\} \tag{9}$$

在时间窗口 δ 中,源和目标 IP 地址的香农熵表示为

$$H(P_S(\delta))=-\sum_{i=1}^{m}(n_{S,i}/n)\lg(n_{S,i}/n) \tag{10}$$

$$H(P_D(\delta))=-\sum_{i=1}^{k}(n_{D,i}/n)\lg(n_{D,i}/n) \tag{11}$$

源和目标 IP 地址威胁度的香农熵表示为

$$H(T_S(\delta))=-\sum_{j=1}^{m}\left(t_{S,j}/\sum_{i=1}^{n}t_i\right)\lg\left(t_{S,j}/\sum_{i=1}^{n}t_i\right) \tag{12}$$

$$H(T_D(\delta))=-\sum_{j=1}^{k}\left(t_{D,j}/\sum_{i=1}^{n}t_i\right)\lg\left(t_{D,j}/\sum_{i=1}^{n}t_i\right) \tag{13}$$

数据报长度的香农熵表示为

$$H(L(\delta))=-\sum_{i=1}^{x}(m_i/n)\lg(m_i/n) \tag{14}$$

由式(10)~式(14)可得到时间窗口 δ 关于报警事件特征的香农熵值向量 $\boldsymbol{V}(\delta)=[H(P_S(\delta)),H(P_D(\delta)),H(T_S(\delta)),H(T_D(\delta)),H(L(\delta))]$,该向量反映了时间窗口 δ 的网络状态,熵值向量的时间序列 $\boldsymbol{V}(1),\boldsymbol{V}(2),\cdots,\boldsymbol{V}(\delta)$ 能够反映一段时间的网络状态。

香农熵向量 $\boldsymbol{V}(\delta)$ 单位化的结果表示为

$$\overline{\boldsymbol{V}}(\delta)=[\overline{H}(P_S(\delta)),\overline{H}(P_D(\delta)),\overline{H}(T_S(\delta)),\overline{H}(T_D(\delta)),\overline{H}(L(\delta))] \tag{15}$$

式中:$\overline{H}(P_S(\delta))=H(P_S(\delta))/H_{sum}$;$\overline{H}(P_D(\delta))=H(P_D(\delta))/H_{sum}$;$\overline{H}(T_S(\delta))=H(T_S(\delta))/H_{sum}$;$\overline{H}(T_D(\delta))=H(T_D(\delta))/H_{sum}$;$\overline{H}(L(\delta))=H(L(\delta))/H_{sum}$;$H_{sum}=H(P_S(\delta))+H(P_D(\delta))+$

$H(T_S(\delta))+H(T_D(\delta))+H(L(\delta))$。

2 检测算法

本文提出的检测算法，能够避免网络终端用户数和攻击程度对报警事件特征香农熵的影响，该方法将 5 维检测指标的香农熵融合于 1 维。当网络处于正常状态时，互雷尼信息熵总是接近于 0，与终端用户数无关；当网络遭受攻击时，其值将发生突变，此时对检测指标采用固定阈值，可以取得较好的检测效果，具体步骤如下。

(1)采用手工选取最初 n 个正常时间窗口的香农熵值的均值作为初始正常时间集合 T，其香农熵向量为

$$\boldsymbol{V}(T)=\frac{1}{n}\sum_{i=1}^{n}\boldsymbol{V}_N(i) \tag{16}$$

式中：$\boldsymbol{V}_N(i)$是正常时间窗口的香农熵向量；n 取固定值，由实验方法确定。

(2)利用式(17)计算 $\bar{\boldsymbol{V}}(\delta)$和 $\bar{\boldsymbol{V}}(T)$的互雷尼信息熵，其中 $\bar{\boldsymbol{V}}(T)$是 $\boldsymbol{V}(T)$单位化后的熵值，$p(T)$和 $p(\delta)$分别是 $\bar{\boldsymbol{V}}(T)$和 $\bar{\boldsymbol{V}}(\delta)$的概率分布函数。

$$I_{0.5}(\bar{\boldsymbol{V}}(T),\bar{\boldsymbol{V}}(\delta))=2\mathrm{lb}\sum_{r}(p(T)p(\delta))^{1/2} \tag{17}$$

式中：r 表示报警事件特征维数。

(3)利用式(18)对时间窗口 δ 的网络状态变化进行合法性判定，当计算结果大于检测阈值 η_{detect} 时，则认为发生了网络攻击(η_{detect}与网络相关，由管理员根据基础阈值 η_{base}和经验设置)

$$I_{0.5}(\bar{\boldsymbol{V}}(T),\bar{\boldsymbol{V}}(\delta))\begin{matrix}\overset{\text{change}}{>}\\ \underset{\text{nochange}}{<}\end{matrix}\eta_{\mathrm{detect}} \tag{18}$$

(4)当最新时间窗口与正常时间集合的互雷尼信息熵小于基础阈值 η_{base}(η_{base}由实验方法确定)时，则认为该时间窗口正常，并对 T 进行更新。

3 攻击测试

3.1 实验环境

实验利用 Snort 对西安交通大学学生宿舍区 32 个 C 网，约 3 000 台主机进行了为期 4 周的监测，取 2010 年 12 月 6 日的 862 284 条报警事件作为实验数据，这些报警事件共包含 65 种报警事件签名，来自42 473个源 IP 地址，发向11 790个目标 IP 地址。训练数据的采集时间从 10:00 到 14:00，共包含 170 516条报警事件，来自13 148个源 IP 地址，发向 7 570个目标 IP 地址；测试数据的采集时间从 14:00 到 23:30，共包含578 389条报警事件，来自29 327个源 IP 地址，发向10 590个目标 IP 地址。

3.2 关键参数

本文使用 ROC(receiver operating characteristic)曲线描述检测结果，其横坐标表示命中率(hit rate，HR)，即命中次数(hit time，HT)占总攻击次数的比率；纵坐标表示误报率(false positive rate，FPR)，即误报次数(false positive time，FPT)占全部正常时间窗口数的比率。当检测结果具有较高的 HR 和较低的 FPR 时，ROC 曲线接近于左上角，此时 ROC 曲线下方的面积(area under ROC curve，AUC，用符号 S_{AUC}表示)将增大，据此进一步确定正常时间集合大小 n 和基础阈值 η_{base}的最佳值。

基于文献[9]的假设，本文采用一种半自动化网络流标定方法剔除真实报警事件。首先通过分析报警事件统计值、香农熵值及互雷尼信息熵值，确定异常时间窗口；然后查看异常时间窗口中贡献最大的源 IP 与目标 IP 地址，剔除与其相关的可疑报警事件；最后重新计算报警事件统计值、香农熵值及互雷尼信息熵值，查看异常是否消失。在训练数据中采用本文方法可以剔除真实报警事件，得到常规训练数据。

在常规训练数据中，由于不存在网络攻击，相邻时刻 δ 和 $\delta-1$ 的网络状态变化相对较小，时刻 δ 和 $\delta-1$ 的互雷尼信息熵接近于 0，所有熵值都处于正常范围内。利用式(19)可以计算出时间窗口 δ 和时间窗口 $\delta-1$ 的互雷尼信息熵，其中 $\bar{\boldsymbol{V}}(\delta-1)$和 $\bar{\boldsymbol{V}}(\delta)$是分别单位化的互雷尼信息熵值，$p(\delta-1)$和 $p(\delta)$分别是 $\bar{\boldsymbol{V}}(\delta-1)$和 $\bar{\boldsymbol{V}}(\delta)$的概率分布函数。图 1 表示了每个时间窗口 δ 和其之前的时间窗口 $\delta-1$ 的互雷尼信息熵，时间窗口为 5 s。

$$I_{0.5}(\bar{\boldsymbol{V}}(\delta-1),\bar{\boldsymbol{V}}(\delta))=2\mathrm{lb}\sum_{r}(p(\delta-1)p(\delta))^{1/2} \tag{19}$$

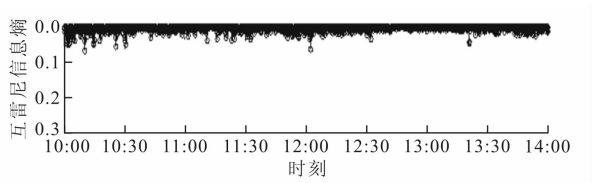

图 1 常规训练数据互雷尼信息熵

互雷尼信息熵值大小的分布如图 2 所示，可以看出：互熵值分布范围在 −0.07 到 0 之间，几乎所有的互熵值都大于 −0.04，因此设置基础阈值 η_{base}

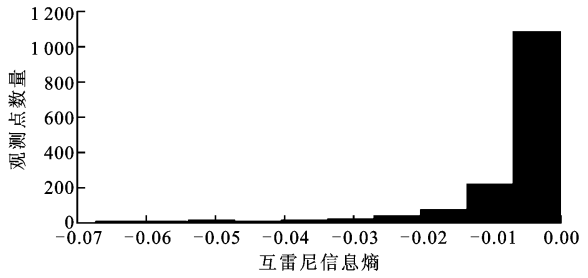

图 2　互雷尼信息熵分布

的取值范围为{−0.001，−0.002，−0.003，…，−0.04}，n 的取值范围为{5，10，15，…，200}，即将正常时间集合的长短从 25 s 到 1 000 s 逐渐增大。由 η_{base} 和 n 的每种组合计算 S_{AUC} 值，图 3 中最深色区域是出现最大 S_{AUC} 值的地方。当 $n=95$，$\eta_{base}=-0.022$ 时，S_{AUC} 取最大值 0.996 2，此时全部训练数据和常规训练数据的互雷尼信息熵如图 4 所示。

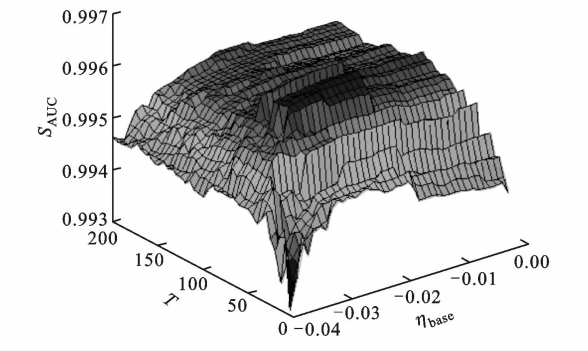

图 3　AUC 曲面

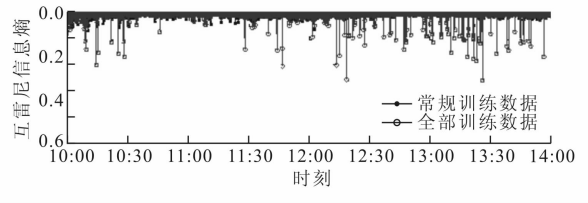

图 4　常规训练数据和全部训练数据互雷尼信息熵

3.3　合成攻击

由于真实数据中攻击事件数量较少且各类攻击分布不均，采用人工合成攻击可以进一步验证参数选择的合理性及该方法的有效性，合成攻击检测的实验数据是在剔除真实报警事件后的背景数据中，加入人工合成的攻击报警事件。

发动合成攻击时，利用工具 SuperScan 按照表 1 描述的攻击方式对被测网络进行扫描，人工产生 5 种攻击各 100 个，并将报警事件随机分布在常规测试数据中。在表 1 中，报警事件数、源 IP 数、目标 IP 数和数据报长度均为一个时间窗口内的统计值，报警事件数随机分布在各个源 IP、目标 IP 和数据报长度上。由于水平扫描和块扫描和主机扫描相似，本文只考虑垂直扫描，即对特定目的主机的多个端口进行扫描。

表 1　合成攻击分类

攻击类型	报警事件数	源 IP 数	目标 IP 数	威胁等级	数据报长度
主机扫描	70～150	1～3	报警事件数/2	3	固定
端口扫描	50～100	1	1	3	随机（共 10～30 种）
DoS 攻击	100～300	5～20	1	1 或 2	固定
蠕虫攻击	100～250	2～5	2～5	1 或 2	随机（共 20～40 种）
主机入侵	50～150	1	1	1 或 2	随机（共 15～40 种）

4　测试效果

4.1　攻击测试

当 $n=95$，$\eta_{detect}=-0.016$ 时，对于真实的测试数据，220 次攻击中共检测出 211 次，误报 8 次，检测命中率为 95.9%，误报率为 0.12%。203 次主机扫描命中 197 次，7 次端口扫描命中 4 次，6 次 DoS、3 次主机入侵和 1 次蠕虫攻击全部命中。

该检测方法对合成攻击的总体误报率为 0.45%，其中对主机扫描、DoS、蠕虫及主机入侵的检测率在 95%以上，对端口扫描命中数相对较小，这与该类攻击触发的报警事件数较少且威胁度低有关，13 次漏报中 6 次都发生在 22：30 到 23：30 之间，该段时间活动用户较多，报警事件数量较大，当端口扫描报警事件较少时，容易被常规报警淹没。

真实攻击和合成攻击环境中的实验结果表明该方法利用 5 个报警特征表现出较好的检测效果，命中率大于 90%，误报率小于 1%。

4.2　敏感度测试

文献[8]提出的传统特征分析法主要是基于各特征香农熵的。测试时，针对 5 种特定类型攻击，重新合成攻击报警事件，通过调整合成攻击报警数占当前窗口内总报警数的比例 R，设置不同的报警事件数量级，每个数量级各包含 100 次合成攻击。

图 5～图 9 显示了各种攻击情况下 5 个特征的香农熵值以及互雷尼信息熵值随合成报警事件数量变化而发生的改变。由图 5 可以看出：由少数几台主机对大量主机发起的主机扫描会导致源 IP 香农熵值逐渐减小，目标 IP 香农熵值逐渐增大，扫描过程中产生的大量长度相同的数据报将导致数据报长度的香农熵值有所下降。图 6 的结果说明，来自同一源 IP、发向同一目标 IP 的大量端口扫描报警事件会同时导致源 IP 和目标 IP 香农熵值逐渐减小，扫描过程中产生的多种长度数据报会使数据报长度的香农熵值增大。由于 DoS 攻击触发的入侵报警事件类型单一，因此图 7 中目标 IP、目标 IP 威胁度和数据报长度的香农熵会逐渐减小。由图 8 可以看出：在蠕虫传播初期，由于报警事件主要集中在少量几台主机之间，虽然报警威胁度较高，但源和目标 IP、源 IP 威胁度和目标 IP 威胁度的香农熵减小幅度并不大，蠕虫继续传播过程中所产生的不同长度的数据报将导致数据报长度的香农熵逐渐增大。攻击报警数量占总报警数 70％时，互雷尼信息熵值为 －0.016 2，能够检测出蠕虫攻击。图 9 的结果表明：主机入侵时，虽然报警事件较少，但报警事件威胁度高，源 IP、目标 IP、源 IP 威胁度和目标 IP 威胁度的香农熵值会随着合成报警事件数的增加呈下降趋势，这是因为大量单一源和目标 IP 的报警事件使得整个报警事件集合更加“规整”；相反，由于攻击中存在较多不同长度的数据报，将导致数据报长度香农熵逐渐递增。与香农熵相比，互雷尼信息熵随着合成报警事件数量的增加变化幅度更加明显，本文检测方法的敏感度优于传统香农熵的检测方法。当检测阈值 $\eta_{\text{detect}}=-0.016$，攻击报警事件数占报警总数的 50％以上时，基本上能够检测出全部 5 类攻击，在同一报警事件数量级下，最易检测出 DoS 攻击和主机入侵，其次是主机扫描和端口扫描，对蠕虫

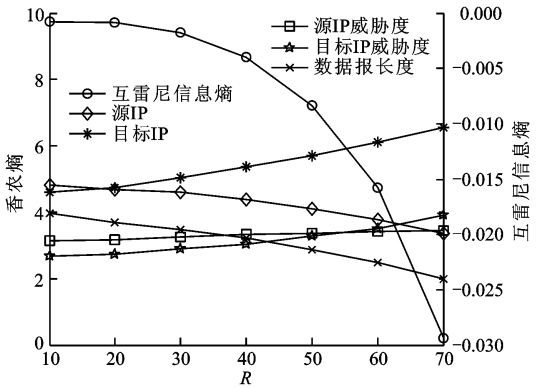

图 5 主机扫描攻击的香农熵和互雷尼信息熵

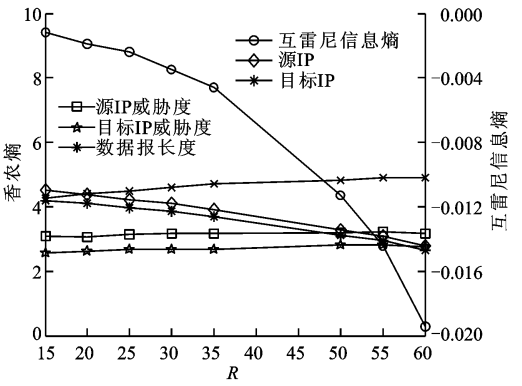

图 6 端口扫描攻击的香农熵和互雷尼信息熵

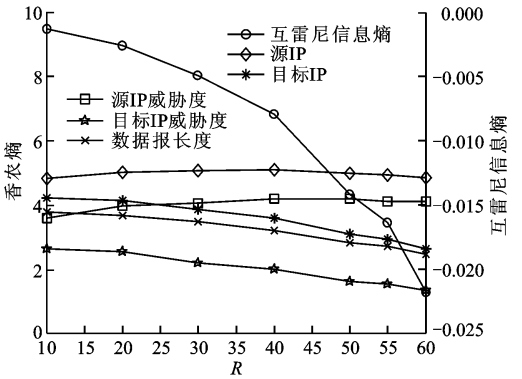

图 7 DoS 攻击的香农熵和互雷尼信息熵

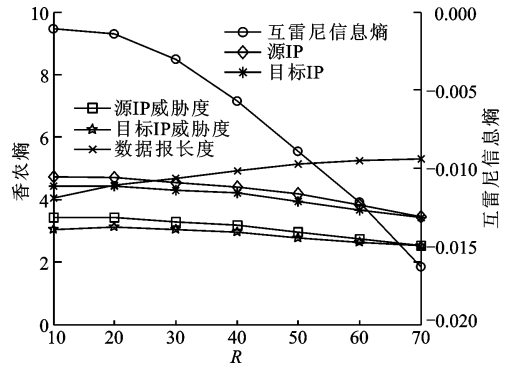

图 8 蠕虫攻击的香农熵和互雷尼信息熵

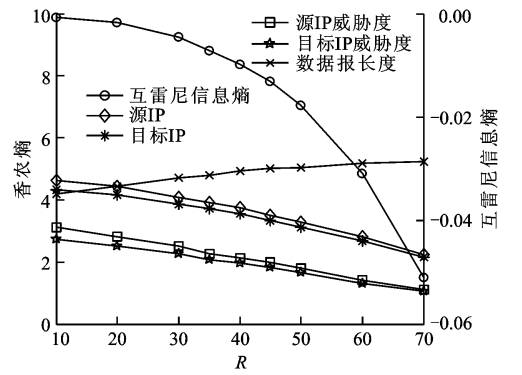

图 9 主机入侵的香农熵和互雷尼信息熵

攻击的检测敏感度稍差。

4.3 对比测试

文献[6]面向报警事件集构造的过滤器基于以下 3 个观察结果：真实报警通常会产生大量源或者目的 IP 地址相同的报警，攻击会增加相同特征真实报警出现的频率，无攻击时段的报警特征可用于分辨真实和误报警，据此设计了相邻报警(NRA)、高报警频率(HAF)和一般误报(UFP)这 3 个检测部件，并融合各检测部件的输出以提高攻击检测命中率。

对比实验仍然在真实攻击和合成攻击环境中进行，由于文献[6]是通过不断试探确定关键参数和阈值的，因此本文实验将按照其对 DARPA 1999 数据集设置的参数执行，合成函数取 3 个算法结果的最大值，判断攻击的阈值 b_{th} 为 1。

2 种方法的实验对比结果如表 2 所示，可以看出：文献[6]除了对端口扫描合成攻击的命中率略高于本文的检测方法外，其对真实攻击和其他几种合成攻击的命中率均不如本文算法。同时，文献[6]的误报率也明显偏高，其原因主要在于：NRA 是基于相似的 IP 地址识别攻击的，当数据中出现大量相似 IP 地址时，一方面对攻击的识别效果越好，另一方面误报率也越高。文献[6]在设计 NRA 时，分别为 IP 或端口扫描攻击设计了 2 种算法，使用不同的参数，这在实际应用中很难确定。HAF 依赖报警频率识别真实报警的方式适用于攻击相对密集的情况，只有对相同特征频繁出现的攻击命中率才会较高；由于在实际应用中很难收集完整无攻击状态的特征信息，因此 UFP 依据历史特征频率和瞬时特征频率识别真实报警的做法并不完全可行。

表 2　攻击对比结果

实验环境	命中次数		命中率/%		误报次数		误报率/%	
	本文算法	文献[6]	本文算法	文献[6]	本文算法	文献[6]	本文算法	文献[6]
真实环境	211	178	95.9	80.9	8	21	0.15	0.32
主机扫描	96	93	96	96	6	15	0.09	0.24
端口扫描	87	90	87	90	6	13	0.09	0.21
DoS 攻击	99	99	99	99	6	11	0.09	0.17
蠕虫攻击	95	83	95	83	5	12	0.08	0.19
主机入侵	98	98	98	98	6	18	0.09	0.28

5 结束语

本文提出的网络攻击检测方法在抽取报警特征时，综合考虑了传统入侵检测系统报警事件的属性以及报警工具 Snort 自身的特点，利用雷尼信息熵对报警事件特征属性的香农熵进行融合，通过与正常网络状态的比较是能够较准确地感知网络安全态势变化的。与基于特征香农熵的攻击检测方法相比，该方法对攻击更敏感，最易检测出 DoS 攻击和主机入侵，其次是主机扫描和端口扫描，对蠕虫攻击的检测敏感度稍差。与对比系统的实验表明该方法能大量减少 Snort 的报警次数，提高命中率，降低误报率。

入侵特征的抽取一直以来都是入侵检测的难点之一，目前现有的入侵特征抽取大都是基于专家知识和实际测试的，因此本文下一步的工作将会从理论上分析该检测方法对特征信息的抽取是否合理。

参考文献：

[1] SCARFONE K, MELL P. Guide to intrusion detection and prevention systems [M]. Gaithersburg, MD, USA: NIST Special Publication, 2007: 9.

[2] TJHAI G, PAPADAKI M, FURNELL S, et al. The problem of false alarms: evaluation with snort and DARPA 1999 dataset [C]// Proceedings of 5th International Conference on Trust, Privacy and Security in Digital Business. Berlin, Germany: Springer-Verlag, 2008: 139-150.

[3] ABIMBOLA A A, MUNOZ J M, BUCHANAN W J. Investigating false positive reduction in http via procedure analysis [C]// Proceeding of the International Conference on Networking and Services. Los Alamitos, CA, USA: IEEE Computer Society, 2006: 87-93.

[4] TIAN Zhihong, ZHANG Weizhe, YE Jianwei, et al. Reduction of false positives in intrusion detection via

(下转第 46 页)