



网络入侵检测系统中的漂移检测

钱亚冠¹, 关晓惠²

(1. 浙江科技学院 杭州 310023; 2. 浙江水利水电学院 杭州 310018)

摘要: 目前基于机器学习的入侵检测系统大都建立在入侵数据始终保持统计平稳的假设之上, 无法应对攻击者有意改变数据特性或新型攻击方式的出现, 而导致的检测率下降的状况。对于上述问题, 即攻击漂移, 提出了加权 Rényi 距离的检测方法。在 KDD Cup99 数据集上的实验证明, Rényi 距离可以有效地增强检测效果; 在检测到漂移后, 通过重新训练模型可以使得对攻击的识别率显著提高。

关键词: 入侵检测; 攻击流量; 攻击漂移; 加权 Rényi 距离

doi: 10.11959/j.issn.1000-0801.2015058

Adversarial Drift Detection in Intrusion Detection System

Qian Yaguan¹, Guan Xiaohui²

(1. Zhejiang University of Science and Technology, Hangzhou 310023, China;

2. Zhejiang University of Water Resources and Electric Power, Hangzhou 310018, China)

Abstract: The recent intrusion detection systems based on machine learning generally assume that the intrusion traffic always satisfies stationary of statistics. However, this assumption is not always held when adversaries arbitrarily alter the distribution of traffic data, or develop new attack techniques, which may reduce the detection rate. To overcome this adversarial drift, a novel drift detection approach based on weighted Rényi distance was suggested. The experiment on KDD Cup99 shows that the weighted Rényi distance is able to perfectly detect the adversarial drift, and improve the intrusion detection rate by retraining the model.

Key words: intrusion detection, attack traffic, adversarial drift, weighted Rényi distance

1 引言

近些年, 网络攻击手段的多样化以及新型攻击方式的不断出现, 使得基于机器学习的网络入侵检测技术开始成为研究热点^[1-6]。基于机器学习的网络入侵检测技术主要分

为两类: 通过正常流量数据训练模型, 识别出异常流量(称异常检测); 通过异常流量数据训练分类模型, 识别出不同的异常流量(称误用检测)。尽管已发表的论文成果显示, 机器学习方法具有良好的检测率, 但这种高检测率大都建立在训练数据与测试数据均保持统计平稳的假设之上, 即

收稿日期: 2014-11-24; 修回日期: 2015-02-02

基金项目: 国家自然科学基金资助项目(No.61379118), 浙江省网络媒体云处理与分析工程技术中心开放课题基金资助项目(No.2012E10023-14), 2014年度高校国内访问学者专业发展基金资助项目(No.FX2014092)

Foundation Items: The National Natural Science Foundation of China (No.61379118), The Zhejiang Province Network Media Cloud Processing and Analysis of Engineering Technology Center Open Topic (No.2012E10023-14), 2014 Annual Professional Development Program of Domestic Universities Visiting Scholar (No.FX2014092)

论文引用格式: 钱亚冠, 关晓惠. 网络入侵检测系统中的漂移检测. 电信科学, 2015058

Qian Y G, Guan X H. Adversarial Drift Detection in Intrusion Detection System. Telecommunications Science, 2015058

训练数据与测试数据都来自同一样本总体。而事实上,由于攻击者对攻击数据特性的有意改变或新型攻击方式的出现,都将导致异常流量的统计特性发生改变。这种改变对基于机器学习的误用检测影响尤其明显,并已引起研究人员的极大关注^[7-10]。

UC Berkeley 的 Kantchelian A 等人^[9]提出攻击漂移(adversarial drift)的概念来描述网络对抗环境下的这种异常数据分布改变的情况。他们意识到攻击者通过人为地改变攻击流量的特征分布,从而绕过分类器的检测;或通过错误的训练分类器^[11],达到将来攻击时不被检测到的目的,于是提出利用分类器集成的方式来克服攻击漂移。Singh A 等人^[8]指出,恶意软件具有恒定的进化能力,这种进化会导致其流量特征的统计分布不平稳,正是这种不平稳性给基于机器学习的入侵检测系统提出了极大的挑战。Singh A 将这种流量特征分布的不平稳性归入机器学习领域中的概念漂移(concept drift)^[12,13]。无论是 Kantchelian A 提出的攻击漂移,还是 Singh A 认为的概念漂移,从统计学角度看都是数据特征分布的改变。如何在恶意网络环境下及时检测到这种漂移现象的发生,是保证入侵检测系统效率的关键^[8,9]。因此,本文在 Bayes 决策理论框架下,专门针对恶意流量的攻击漂移提出有效的检测方法,具体如下:

- 将 Rényi 距离应用到恶意流量的漂移度量中,利用其可调参数提高检测的灵敏性;
- 应用最大熵方法估计的概率模型,降低 Rényi 距离的计算复杂性;
- 提出基于信息熵的加权 Rényi 距离,解决多个特征的 Rényi 距离的表征问题。

2 问题描述及相关概念

2.1 攻击流量漂移

假设 $X \in R^m$ 是 m 维特征空间的异常流量,由 m 个统计特征组成, $X=(a_1, a_2, \dots, a_m)$, $C=(c_1, c_2, \dots, c_k)$ 是攻击类型集合。由 Bayes 决策理论可知,一个优化的分类模型 $f(X) \rightarrow c_i$ 可由先验概率 $P(c_i)$ 和条件概率密度 $p(X|c_i)$ 决定^[14]:

$$p(c_i|X)=P(c_i)p(X|c_i)/p(X) \quad (1)$$

定义 1 假设在某个测量时间段 t 内获得的 c_i 类型攻击流量为 X , 定义其概率状态为 c_i 的先验概率 $P(c_i)$ 与条件概率 $p(X|c_i)$ 的联合表示为: $S_i(c_i)=(P(c_i), p(X|c_i))$ 。

定义 2 (网络攻击流量漂移) 经过时间段 D 后, 攻击流量类 c_i 的概率状态发生显著改变的过程, 即表现为

$$S_{i+\Delta}(c_i) \neq S_i(c_i)。$$

很明显, 这种攻击流量的漂移会影响到分类检测统计模型的准确率^[15]。但是目前的机器学习分类方法往往只用于时间段 t 内获得的数据训练学习器, 对于时间段 D 后的攻击流量的概率分布状况毫无感知。这种缺乏反馈机制的方法将导致在分类准确率下降的情况下, 分类模型仍然误认为自己还具有时刻 t 的分类效率。为了能自动发现攻击流量的漂移, 提出了利用 Rényi 距离^[16]作为网络攻击流量漂移的度量。

2.2 Rényi 距离

定义 3 Rényi 熵 $R(A)$ 是 Shannon 熵 $H(A)$ 的广义形式:

$$R(A) = \frac{1}{\alpha - 1} \text{lb} \int p(x)^\alpha dx \quad (2)$$

其中, α 是一个可调参数, 当 $\alpha \rightarrow 1$ 时, $R(A) \rightarrow H(A)$ 。

定义 4 假设 P 和 Q 是可测空间 (X, F) 上的概率测度, p 和 q 分别是它们的概率密度, 则 $\alpha(\alpha \geq 0)$ 阶 Rényi 距离定义为:

$$D_\alpha(P \| Q) = \frac{1}{\alpha - 1} \text{lb} \int p(x)^\alpha q(x)^{1-\alpha} dx \quad (3)$$

当 $P=Q$ 时, $D_\alpha(P \| Q)=0$ 。

Rényi 距离用于表征概率之间的差异度, 又称 Rényi 离散度。当 $\alpha \rightarrow 1$ 时, $D_\alpha(P \| Q)$ 就退化为 K-L(Kullback-Leibler) 距离^[11]。由于 Rényi 距离具有可调参数 α , 它比 K-L 距离具有更好的一般性和灵活性。但是 Rényi 距离与 K-L 距离一样具有不对称性(具体见定理 1), 因此将其进行必要的修改, 使其成为适合作为概率分布差异的度量, 本文将对称的 Rényi 距离作为漂移的度量, 在以后内容中不再做特别说明。

定义 5 对称 Rényi 距离表示为: $\bar{D}_\alpha(P \| Q) = \frac{1}{2} (D_\alpha(P \| Q) +$

$D_\alpha(Q \| P))$, 满足 $\bar{D}_\alpha(P \| Q) = \bar{D}_\alpha(Q \| P)$ 。

定理 1 如果 $P \neq Q$, 那么 $D_\alpha(P \| Q)$ 通常不等于 $D_\alpha(Q \| P)$ 。

证明 已知 $P \neq Q$, 那么有 $\int q(x)^{1-2\alpha} dx \neq \int p(x)^{1-2\alpha} dx$,

$\int p(x)^\alpha q(x)^{1-2\alpha} dx \neq \int q(x)^\alpha p(x)^{1-2\alpha} dx$, 可推知 $\frac{1}{\alpha} \text{lb} \int p(x)^\alpha q(x)^{1-2\alpha} dx \neq \frac{1}{\alpha} \text{lb} \int q(x)^\alpha p(x)^{1-2\alpha} dx$, 即 $D_\alpha(P \| Q) \neq D_\alpha(Q \| P)$, 得证。

3 识别方法

本文利用 Rényi 距离检测攻击流量的漂移。理想情况下, 如果攻击流量没有发生漂移, 则两个时间段的攻击流量的 Rényi 距离为 0。但实际情况下, 由于获取的流量样本



有限,即使攻击流量没有发生漂移,Rényi 距离也会在一个范围内波动。因此定义如下的指示函数:

$$A(P, Q) = \begin{cases} 1, & \bar{D}_\alpha(P \| Q) > \delta \\ 0, & \bar{D}_\alpha(P \| Q) \leq \delta \end{cases} \quad (4)$$

其中, δ 是判决门限,根据经验设置。计算式(4)的关键是准确快速地估计 p, q 和解决多个特征的 Rényi 距离融合问题。以往文献计算 K-L 距离通常是直接利用样本得到的经验概率(empirical probability)^[17],利用最大熵原理估计 p, q ,可获得更精确的估计,并可避免事先假设概率模型的不足。同时,利用信息增益作为加权系数,将多个特征的 Rényi 距离统一为单一的统计量。

3.1 概率密度估计

从实际流量数据中可以事先获得样本均值 μ ,由大数定律可知,样本均值依概率收敛于总体均值。因此,希望最终估计获得的概率分布的均值与样本均值保持一致。由最大熵原理^[18]可知,上述概率密度估计问题可以等价如下有约束的优化问题:

$$\max H = - \int p(x) \ln p(x) dx \quad (5)$$

$$\text{s.t. } E\{\phi_n(x)\} = \int \phi_n(x) p(x) dx = \mu_n, \quad n = 0, 1, 2, \dots, N \quad (6)$$

其中, $\phi_0(x) = x, \mu_0 = 1$,即满足概率的归一条件。理论上, $\phi_n(x)$ 可以是定义在随机变量 x 上的任意函数。 μ_n 是常量,可通过样本数据计算获得。利用拉格朗日乘数法求解可获得如下指数形式的解:

$$p(x) = \exp \left[- \sum_{n=0}^N \lambda_n \phi_n(x) \right] \quad (7)$$

其中, $\lambda = [\lambda_0, \dots, \lambda_N]$ 为拉格朗日系数。将式(7)代入式(6)可得:

$$G_n(\lambda) = \int \phi_n(x) \exp \left[- \sum_{n=0}^N \lambda_n \phi_n(x) \right] dx = \mu_n \quad (8)$$

将 $G_n(\lambda)$ 进一步展开成泰勒级数,并丢弃二阶以上的高阶项,变为求解线性方程组的问题:

$$G_n(\lambda) \cong G_n(\lambda^0) + (\lambda - \lambda^0)^T [\text{grad} G_n(\lambda)]_{(\lambda=\lambda^0)} = \mu_n \quad (9)$$

采用牛顿法求解此非线性方程组的数值解 λ 。

令:

$$\delta = \lambda - \lambda^0 \quad (10)$$

$$v = [\mu_0 - G_0(\lambda^0), \dots, \mu_N - G_N(\lambda^0)]^T \quad (11)$$

$$G = [g_{nk}] = \left[\frac{\partial G_n(\lambda)}{\partial \lambda_k} \right]_{(\lambda=\lambda^0)}, \quad n, k = 0, \dots, N \quad (12)$$

则式(9)可表示为:

$$G\delta = v \quad (13)$$

利用式(10)不断迭代 $\lambda = \delta + \lambda^0$,用新的 λ 替代 λ^0 ,直到 δ 满足终止条件。

利用最大熵估计概率密度的关键是确定式(6)中的样本函数 $\phi_n(x)$ 。不同的样本函数代表不同的已知知识,最终得到的概率密度也会有所差异。考虑到通用性和易解性,将 $\phi_n(x)$ 定义为 n 阶原点矩:

$$\phi_n(x) = x^n, \quad n = 1, \dots, M \quad (14)$$

本文采用最高 6 阶原点矩,即 $M=6$,完全满足拟合度的要求。

3.2 检测算法

通过样本估计获得概率密度 p, q ,利用式(3)可计算得到某个特征的 Rényi 距离。但机器学习分类中的数据流通常由多个特征组成,采用信息增益作为特征的权重,并加权求和成单个变量。首先给出数据集 S 的分类信息熵定义^[19]:

$$\text{Info}(S) = - \sum_{i=1}^m p_i \ln p_i \quad (15)$$

其中, p_i 是 S 中任意实例在类 C_i 中的概率,可由 $|C_{iS}|/|S|$ 估计得到。假设特征 A 可将 S 按决策树原理划分为 v 个子集 $\{S_1, S_2, \dots, S_v\}$,定义特征 A 对 S 的分类信息熵为:

$$\text{Info}_A(S) = - \sum_{j=1}^v \frac{|S_j|}{|S|} \ln \text{Info}(S_j) \quad (16)$$

进一步定义信息增益为:

$$\text{Gain}(A) = \text{Info}(S) - \text{Info}_A(S) \quad (17)$$

显然 $\text{Gain}(A) \geq 0$,因为通过特征 A 对数据集进行划分后,实例在各子集中的分布更均匀,信息熵变小。由于各特征的信息增益不满足归一条件,特征 A_i 的权重系数 α_i 可由 $\text{Gain}(A_i)/\sum \text{Gain}(A_i)$ 确定。最后将第 k 个类的加权 Rényi 距离 WD_k 表示为:

$$WD_k = \sum_{i=1}^m \alpha_i D_{k,i} \quad (18)$$

算法: traffic_evolution_detect

输入: TS_1 是原来模型的训练数据集;

TS_2 是最近获取的数据集;

A 为攻击流量的特征集合,通常通过某种特征选择算法得到;

C 是所有可能的分类集合;

δ 为 Rényi 距离的门限值,如果超过该门限值,则判断为漂移发生;

α 为 Rényi 熵的可调参数。

输出: R , 当类 c_i 发生漂移时 R_i 输出 1, 否则输出 0。
具体步骤如下。

begin

for 每个分类 $c_i \in C$ do

for 每个特征 $a_j \in A$ do

$p_{ij} \leftarrow ME(TS_1, c_i, a_j)$; //最大熵估计数据集 S_1 中类

c_i 的特征 a_j 的概率密度

$q_{ij} \leftarrow ME(TS_2, c_i, a_j)$; //最大熵估计数据集 S_2 中类

c_i 的特征 a_j 的概率密度

$D_{ij} \leftarrow RD(p_{ij}, q_{ij}, \alpha)$; //计算 p_{ij} 与 q_{ij} 的 Rényi 距离

end for

end for

for 每个特征 $a_j \in A$ do

$a_j \leftarrow Gain(a_j) / \sum Gain(a_j)$; //计算每个特征的加权系数;

end for

for 每个分类 $c_i \in C$ do

$WD_i \leftarrow \sum_{j=1}^m \alpha_j D_{ij}$; //计算类 c_i 的加权 Rényi 距离

if $WD_i > \delta$ then

$R_i \leftarrow 1$;

else

$R_i \leftarrow 0$;

end if

end for

return R ;

end

4 实验评估

利用 KDD Cup99^[20]入侵数据集对上述方法进行实验评估。KDD Cup99 数据集源于 MIT 林肯实验室收集的网络入侵数据, 目前已被广泛应用于入侵检测方面的实验评估。该数据集包含四大类攻击, 分别标记为 DoS、PROBE、U2R、R2L。同时, 该数据集分为 D1、D2 两个部分, 采集时间分别相距 6 个月。与 D1 相比, D2 增加了多种攻击方法: DoS 攻击增加了 4 种, 从最初的 6 种攻击方法增加到 10 种 (见表 1); U2R 攻击方法增加了 4 种 (见表 2); Probe 攻击方法增加了 2 种 (见表 3), 上述变化提示网络攻击方法在随时间不断地演进变化; R2L 的攻击方法数量没有变化, 只是 guess_passwd 的攻击流量有所增加 (见表 4)。通过上述分析可知, 尽管 D2 中的攻击类型仍然只有 4 种, 但其包含数量

在增多; 直接用 D1 训练的分类模型对 D2 进行分类, 发现误分类率很高, 原因就是攻击方法的衍生导致攻击漂移的发生。因此, 通过本文提出的加权 Rényi 距离来检测 D1 与 D2 的漂移是否发生及程度。实验过程中采用 MATLAB 实现了上述算法, 并通过调用机器学习软件 Weka3.6 的接口, 实现多种分类器的性能比较, 参数设置采用系统默认值。

表 1 DoS 攻击方法的类型增加情况

DoS	数据集 D1 (flow 数)	数据集 D2 (flow 数)
apache2	/	794
Back	2 203	1 098
Land	21	9
Mailbomb	/	5 000
Neptune	107 201	58 001
Pod	264	87
Processtable	/	759
Smurf	280 790	164 091
Teardrop	979	12
Udpstorm	/	2

表 2 U2R 攻击方法的类型增加情况

U2R	数据集 D1 (flow 数)	数据集 D2 (flow 数)
Buffer_overflow	30	22
Httpunnel	/	158
Loadmodule	9	2
Perl	3	2
Ps	/	16
Rootkit	10	13
Sqlattack	/	2
Xterm	/	13

表 3 Probe 攻击方法的类型增加情况

Probe	数据集 D1 (flow 数)	数据集 D2 (flow 数)
Ipsweep	1 247	306
Mscan	/	1 053
Nmap	231	84
Portsweep	1 040	354
Saint	/	736
Satan	1 589	1 633

表 4 R2L 攻击方法的类型构成情况

R2L	数据集 D1 (flow 数)	数据集 D2 (flow 数)
ftp_write	8	3
Guess_passwd	53	4 367
Imap	12	1

4.1 KDD Cup99 数据的密度估计

准确地估计数据的概率密度是获得合理 Rényi 距离



的关键。图1~图3给出了利用最大熵方法估计出的U2R类的3种特征的概率密度。由于篇幅有限,仅给出3种特征的概率密度估计。图1~图3中的虚线为估计出的概率密度,直方图为数据的频率统计。通过拟合优度检验, R -square值均达到0.98以上。可以发现,利用最大熵方法估计出的概率密度可以很好地拟合实际数据,包括数据尖峰部分。

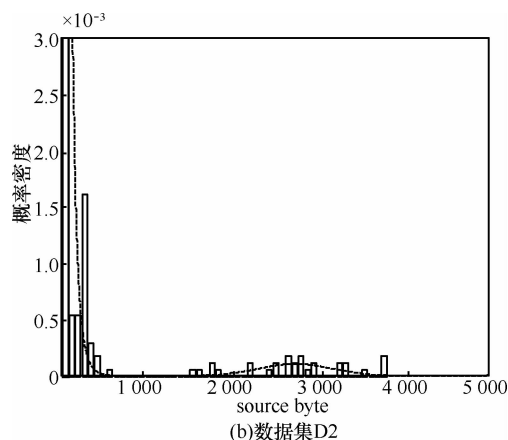
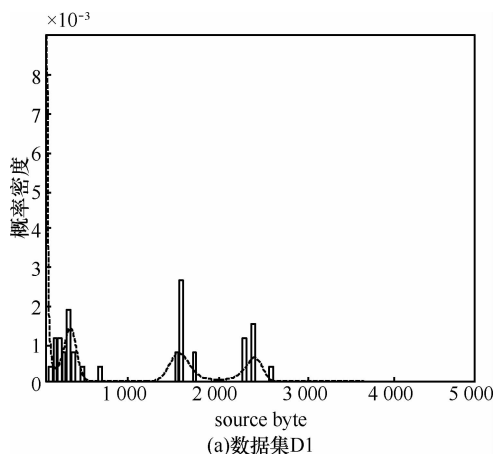


图1 U2R 的 source byte 特征的概率密度

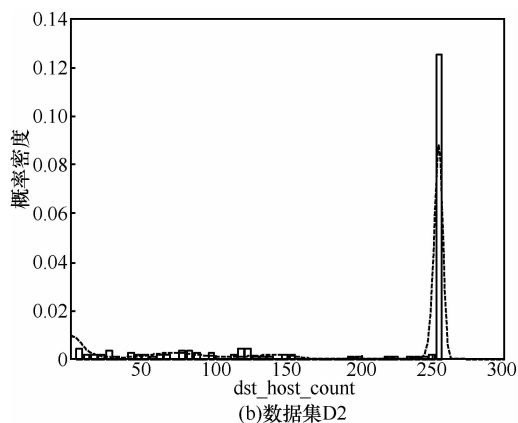
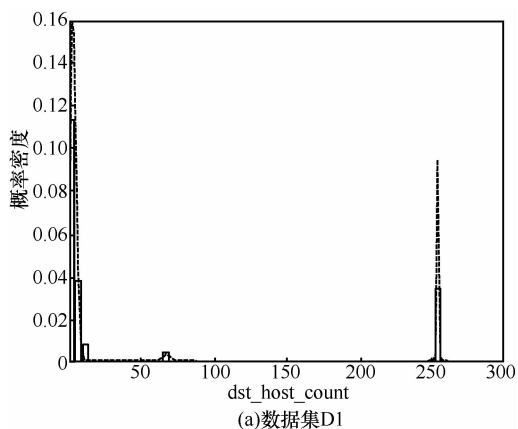


图2 U2R 的 dst_host_count 特征的概率密度

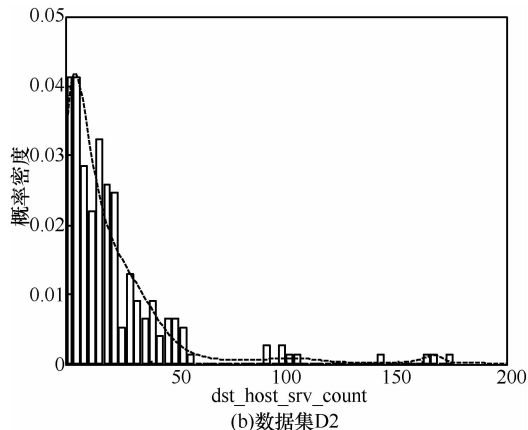
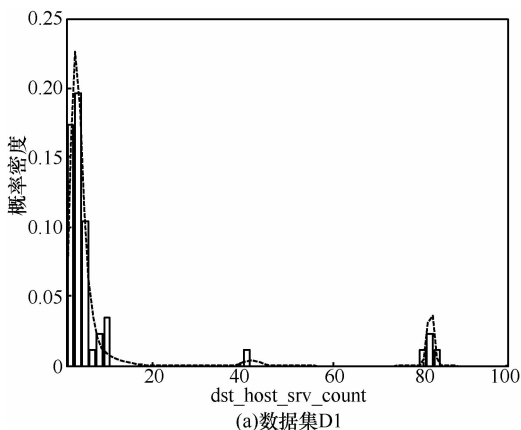


图3 U2R 的 dst_host_srv_count 特征的概率密度

4.2 加权 Rényi 距离

Rényi 距离与 K-L 距离都可表征概率之间的差异度。当 $\alpha \rightarrow 1$ 时, Rényi 距离就退化为 K-L 距离。在 KDD Cup99 的两个数据集 D1、D2 上分别计算 K-L 距离与不同参数的 Rényi 距离,并比较它们检测攻击漂移的效果。4 种攻击类型的加权 K-L 距离分别为 0.39(Probe)、0.54(DoS)、0.85(U2R)

和 0.13(R2L);参数的加权 Rényi 距离分别为 0.48(Probe)、0.80(DoS)、1.52(U2R)和 0.14(R2L);参数 $\alpha=1.8$ 的加权 Rényi 距离分别为 0.62(Probe)、1.78(DoS)、3.14(U2R)和 0.16(R2L)。图 4 显示了 4 种攻击类型的上述距离值。可以发现,U2R 攻击的距离值最大,漂移最显著;而 R2L 攻击的距离值最小,漂移最不显著;同时发现 R2L 攻击的 K-L 距离与 Rényi 距离非常接近;而在 U2R 攻击上,Rényi 距离明显大于 K-L 距离,且 α 值越大,距离值越大。与 K-L 距离相比,Rényi 距离对于漂移检测具有放大作用,且大的 α 值比小的 α 值的放大效果更明显,即对漂移具有更高的敏感性。利用 Rényi 距离的漂移敏感性,比 K-L 距离更容易设置检测算法的阈值。在本文中,根据经验值设置检测算法的阈值 $\delta=1.5$ 。

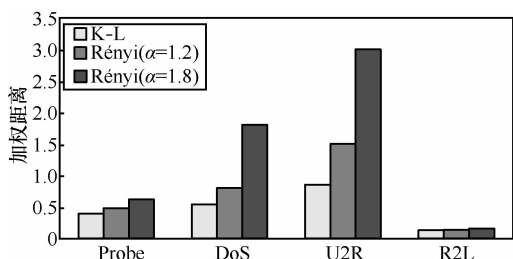


图 4 Rényi 距离与传统的 K-L 距离的漂移检测效果比较

4.3 重训练后的分类性能评估

在检测到攻击漂移后,采用模型重训练机制来更新分类模型。分别选取核估计 Naïve Bayes (NB+kernel)、Bayes 网络 (BN)、决策树 (C4.5)、支持向量机 (SVM)、 k 近邻 (k -NN)、神经网络 (NN)、随机森林 (RF) 与分类器组合方法 (Bagging) 进行实验对比。图 5~图 8 给出了在检测到概念漂移后,采用新的样本数据重新训练模型后的分类准确率与重新训练前的模型进行比较的结果。

可以看出,各种方法在模型重训练后,其准确率得到了很大程度的提高,而这些方法又以决策树算法 C4.5 的分类性能最好。对于每种攻击类型的识别率,又以漂移最明显的 U2R 的提升最显著。由此可见,在攻击漂移发生后,用新的样本数据进行模型的重新训练,可以有效地改善攻击流量分类的准确率。

5 结束语

机器学习方法目前被广泛地应用到互联网流量分类、异常流量检测等领域,取得了不少成果。但由于目前网络攻击手段不断变化更新,传统上基于静态批量学习的方法

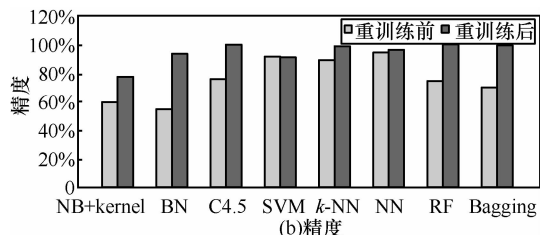
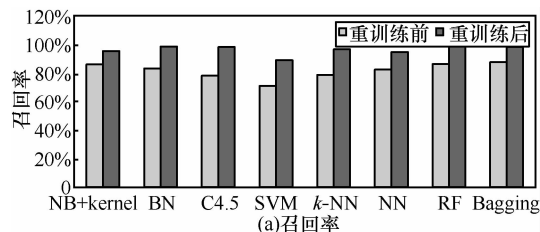


图 5 分类模型进行重训练后,Probe 攻击的召回率与精度的比较

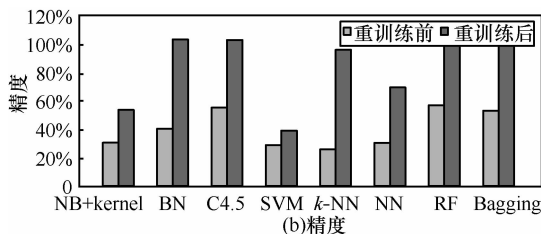
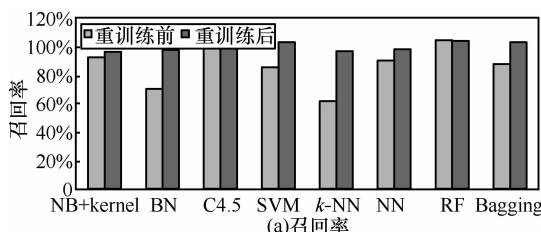


图 6 分类模型进行重训练后,DoS 攻击的召回率与精度的比较

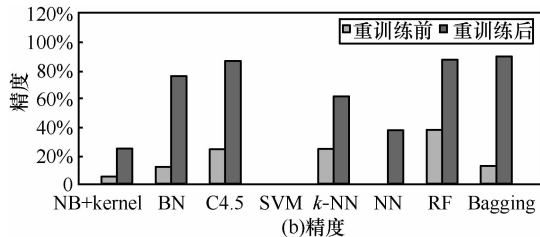
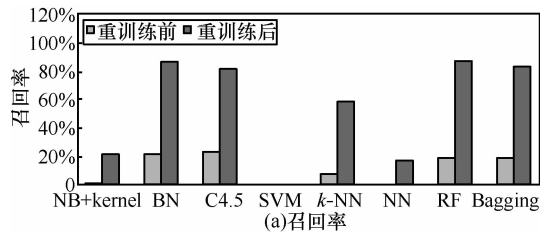


图 7 分类模型进行重训练后,U2R 攻击的召回率与精度的比较

不能很好地适应这种攻击动态演进的环境。因此,需要能及时检测到攻击漂移的发生,并及时重新训练模型,使其保持较高的识别率。本文提出的漂移检测方法从攻击流量

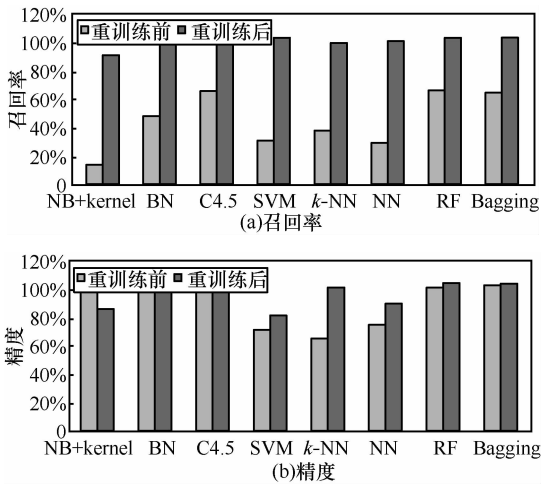


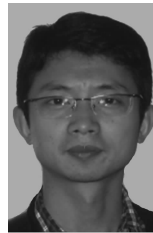
图8 分类模型进行重训练后,R2L攻击的召回率与精度的比较

的特征概率密度出发,通过 Rényi 距离对漂移的放大作用检测其是否发生,具有比 K-L 距离对漂移更敏感的优点。

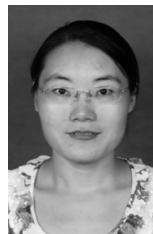
参考文献

- 陆悠, 李伟, 罗军舟等. 一种基于选择性协同学习的网络用户异常行为检测方法. 计算机学报, 2014, 37(1): 28~40
Lu Y, Li W, Luo J Z, *et al.* A network user's abnormal behavior detection approach based on selective collaborative learning. Chinese Journal of Computers, 2014, 37(1): 28~40
- 张晓惠, 林柏钢. 基于特征选择和多分类支持向量机的异常检测. 通信学报, 2009, 30(10A): 68~73
Zhang X H, Lin B G. Anomaly detection based on feature selection and multi-class support vector machines. Journal on Communications, 2009, 30(10A): 68~73
- 李洋, 方滨兴, 郭莉等. 基于主动学习和 TCM-KNN 方法的有指导入侵检测技术. 计算机学报, 2007, 30(8): 1464~1473
Li Y, Fang B X, Guo L, *et al.* Supervised intrusion detection based on active learning and TCM-KNN algorithm. Chinese Journal of Computers, 2007, 30(8): 1464~1473
- Li Y, Li W, Wu G. An intrusion detection approach using SVM and multiple kernel method. International Journal of Advancements in Computing Technology, 2012, 4(1): 463~469
- Biggio B, Corona I, Nelson B, *et al.* Security Evaluation of Support Vector Machines in Adversarial Environments. Berlin: Springer International Publishing, 2014
- Damopoulos D, Menesidou S A, Kambourakis G, *et al.* Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers. Security and Communication Networks, 2012, 5(1): 3~14
- Laskov P, Lippmann R. Machine learning in adversarial environments. Machine Learning, 2010, 81(2): 115~119
- Singh A, Walenstein A, Lakhota A. Tracking concept drift in malware families. Proceedings of the 5th ACM Workshop on Security and Artificial Intelligence, Raleigh, USA, 2012: 81~92
- Kantchelian A, Afroz S, Huang L, *et al.* Approaches to adversarial drift. Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security, 2013: 99~110
- Barreno M, Nelson B, Joseph A D, *et al.* The security of machine learning. Machine Learning, 2010, 81(2): 121~148
- Newsome J, Karp B, Song D. Paragraph: Thwarting Signature Learning by Training Maliciously. Berlin: Springer Berlin Heidelberg, 2006
- Tsymbal A. The problem of concept drift: definitions and related work. Computer Science Department, Trinity College Dublin, 2004
- Widmer G, Kubat M. Learning in the presence of concept drift and hidden contexts. Machine Learning, 1996, 23(1): 69~101
- Zliobaite I. Learning Under Concept Drift: an Overview. Technical Report, Vilnius University, 2009
- Kelly M G, Hand D J, Adams N M. The impact of changing populations on classifier performance. Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Diego, 1999: 367~371
- Van Erven T, Harremoës P. Rényi divergence and majorization. Proceedings of 2010 IEEE International Symposium on Information Theory (ISIT), Austin, Texas, USA, 2010: 1335~1339
- Yu S, Zhou W, Doss R. Information theory based detection against network behavior mimicking DDoS attacks. Communications Letters, 2008, 12(4): 318~321
- Jaynes E T. Information theory and statistical mechanics. Physical Review, 1957, 106(4)
- Shannon C E. A mathematical theory of communication. The Bell System Technical Journal, 1948(27): 379~423, 623~656
- Hettich S, Bay S D. KDD cup 1999. <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>, 2007

[作者简介]



钱亚冠,男,博士,浙江科技学院副教授,主要研究方向为互联网流量分类、下一代互联网、机器学习与数据挖掘。



关晓惠,女,浙江水利水电学院副教授,主要研究方向为机器学习与数据挖掘。