

基于核密度估计的轻量级物联网异常流量检测方法

张 叶 李志华 王长杰

江南大学人工智能与计算机学院 江苏 无锡 214122

(wxjncs_zy@aliyun.com)



摘 要 为了有效应对僵尸网络对家庭和个人物联网的安全威胁,尤其针对家用环境中用于异常检测的资源不足的客观问题,提出了一种基于核密度估计的轻量级物联网异常流量检测(Kernel Density Estimation-based Lightweight IoT Anomaly Traffic Detection,KDE-LIATD)方法。首先,KDE-LIATD 方法使用高斯核密度估计方法估计了训练集中正常样本每一维特征的特征值概率密度函数以及对应的概率密度;然后,提出了基于核密度估计的特征选择算法(Kernel Density Estimation-based Feature Selection Algorithm,KDE-FS),获得了对异常检测贡献突出的特征,从而在提升异常检测准确率的同时降低了特征维度;最后,通过三次样条插值方法计算测试样本的异常评估值并进行异常检测,这一策略极大地减少了使用核密度估计方法计算测试样本异常评估值时所需要的计算开销与存储开销。仿真实验结果表明,提出的 KDE-LIATD 方法在面向异构的物联网设备的异常流量检测方面具有比较强的鲁棒性和兼容性,能够有效地对家庭和个人物联网僵尸网络的异常流量进行检测。

关键词: 物联网;核密度估计;异常检测;僵尸网络;特征选择

中图法分类号 TP309

Kernel Density Estimation-based Lightweight IoT Anomaly Traffic Detection Method

ZHANG Ye,LI Zhi-hua and WANG Chang-jie

School of Artificial Intelligence and Computer,Jiangnan University,Wuxi,Jiangsu 214122,China

Abstract In order to effectively deal with the security threats of home and personal Internet of Things(IoT) bot nets,especially for the objective problem of insufficient resources for anomaly detection in the home environment,a kernel density estimation-based lightweight IoT anomaly traffic detection (KDE-LIATD) method is proposed. Firstly, the KDE-LIATD method uses a Gaussian kernel density estimation method to estimate the probability density function and corresponding probability density of each dimension feature value of thenormal samples in the training set. Then,a kernel density estimation-based feature selection algorithm (KDE-FS) is proposed to obtain features that contribute significantly to anomaly detection,thereby reducing the feature dimension while improving the accuracy of anomaly detection. Finally,the cubic spline interpolation method is used to calculate the anomaly evaluation value of the test sample and perform anomaly detection. This strategy greatly reduces the computational overhead and storage overhead required to calculate the anomaly evaluation value of the test sample using the kernel density estimation method. Simulation experiment results show that the KDE-LIATD method has strong robustness and strong compatibility for anomaly traffic detection of heterogeneous IoT devices,and can effectively detect abnormal traffic in home and personal IoT bot nets.

Keywords IoT,Kernel density estimation,Anomaly detection,Bot net,Feature selection

1 引言

文献[1]调查显示,到 2020 年,全球物联网设备总数将达到 500 亿。遗憾的是,在过去的十年中,物联网设备厂商没有对安全需求和未来所涉及的安全挑战进行深入的考量,导致

IoT 环境一直以来都是各类漏洞攻击的重灾区^[2]。

由于物联网设备种类繁多、结构简单,并且计算能力有限,存储容量也相当小,因此无法将计算机网络领域传统的入侵检测系统直接移植到物联网终端,这就导致物联网终端设备更容易遭受恶意软件的攻击^[3]。Mirai 作为一款臭名昭著

到稿日期:2020-06-17 返修日期:2020-08-28 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:工业和信息化部智能制造项目(ZH-XZ-180004);中央高校基本科研业务费专项资金(JUSRP211A41);中央高校基本科研业务费专项资金(JUSRP42003);111 基地建设项目(B2018)

This work was supported by the Intelligent Manufacturing Project of Ministry of Industry and Information Technology(ZH-XZ-180004),Fundamental Research Funds for the Central Universities of Ministry of Education of China(JUSRP211A41),Fundamental Research Funds for the Central Universities of Ministry of Education of China (JUSRP42003) and 111 Base Construction Project(B2018).

通信作者:李志华(jswxzhli@aliyun.com)

的物联网僵尸网络恶意软件,于2016年10月控制了100 000个物联网设备^[4],并对Dyn公司的DNS基础设施进行了分布式拒绝服务攻击(Distributed denial of service attack, DDoS)。2019年7月24日,网络安全公司Imperva报告该公司服务的一个娱乐行业的CDN客户在2019年4—5月期间受到了大规模DDoS攻击^[5]。由于物联网基础架构的松散性、协议的多样性、终端设备的低计算能力等,造成了物联网关键安全功能的缺失,给物联网信息安全带来了新的挑战。特别是随着物联网应用的普及,应用规模的不断增加,面向物联网僵尸网络入侵检测研究的紧迫性日益凸显。而当前基于异常流量的检测方法大多是针对资源充足的服务器或者个人电脑所设计的,面向物联网特性的异常流量检测模型、方法、技术相对还比较少。

文献[6-10]从不同角度对物联网异常流量检测模型与检测部署点进行了研究。文献[6-7]将异常流量检测模型部署于网络中心,通过对数据包进行捕获并解析,可以实现对已被识别的攻击进行有效的检测,但是网络中心通常远离攻击源,导致响应时间存在无意义的延迟,因此很难最小化攻击造成的影响。文献[8-10]提出对直接依赖物联网设备的计算和存储能力进行异常流量检测的策略。文献[10]在物联网设备上,使用支持向量机、逻辑回归等简单的异常检测方法进行异常流量检测,取得了较好的实验效果。尽管直接依赖物联网设备进行异常检测可以直接定位并隔离僵尸网络,但是物联网设备存在先天性的资源限制,限制了算法的复杂性和高效性,并且有些设备还面临着固件更新等约束,因此无法有效应对不断变化的恶意软件攻击。文献[11-18]将诸如随机森林、神经网络等异常流量检测模型部署于家庭或者企业的物联网网关之上,这样有利于将所发现的异常流量拦截于网关之外,从而起到防止更大范围的网络危害和防止网络遭受更多攻击的作用。文献[11]在网关上针对不同型号的物联网设备使用不同的BP神经网络异常检测模型进行异常流量检测,在实验中获得较好的异常检测效果,但是该策略增加了网关的计算开销与存储开销,不适用于家庭物联网应用环境;文献[12]通过研究僵尸网络控制协议的细节,提出了一种基于软件定义网络的异常检测算法,该算法能够有效扫描出物联网环境中受僵尸网络感染的物联网设备,但是由于僵尸网络控制协议的天日趋多变以及愈发复杂,现在学术界更多地关注及时发现被远程控制的物联网设备所发起的DDoS攻击,以及发现僵尸设备对周围物联网设备进行扫描时所产生的流量特征;文献[13]提出了一种基于双向长记忆递归神经网络的Mirai僵尸网络攻击检测方法,仿真实验显示其取得了比较好的实验效果,但是模型过于复杂,不适用于计算和存储资源均不足的物联网应用环境;文献[14]在家庭物联网环境中,通过在无线路由器上对流量进行提取,并进行特征降维,从而进行异常检测,同时其指出由于物联网协议的多样性以及无线路由器计算资源的有限性,所提取的特征必须是轻量级的,如只能是与时间有关的统计特征而不是深度包检测特征,因此其仅对Mirai僵尸网络恶意软件的DDoS攻击方式进行了模拟,并从流量中提取有限的特征,这种做法缺乏一般性;文献[15]通过在无线路由器上安装定义了流量隔离规则的物联网僵尸网

络检测模型,有效降低了物联网设备受到僵尸网络软件攻击的风险,这一方案的意义在于证明了在无线路由器或者其他网络中间件上安装简单的异常检测模型是可行的,同时也启发了学术界的同仁们,在使用异常检测模型的思路进行物联网异常检测研究时,并且在考虑到检测设备资源有限性的大前提下,不仅要关注检测的效果,还应该关注用于检测的特征数量和检测方法对设备资源所造成的计算与存储负载的消耗。

本文针对上述研究工作中存在的异常检测部署点远离攻击源、异常检测模型过于复杂等不足,面向家庭物联网环境异常流量检测的实际需求,提出了一种基于核密度估计的轻量级物联网异常流量检测(KDE-LIATD)方法。首先,KDE-LIATD方法通过使用高斯核密度估计方法训练得到训练集中正常样本每一维特征的特征值概率密度函数及其对应的概率密度;然后,考虑到家庭物联网环境异常检测设备资源不足的现实问题,提出了一种基于核密度估计的特征选择算法(KDE-FS),KDE-FS通过先前训练得到的概率密度函数计算训练集中异常样本每一维特征的特征值概率密度,对其异常检测效果进行评价,挑选出对异常检测贡献突出的特征,降低了样本特征的维度;最后,使用三次样条插值方法计算测试样本的异常评估值并进行异常检测。这种处理策略极大地减少了使用核密度估计方法获取测试样本异常评估值所需要的计算量和存储空间。本文分别在标准样本集上对上述算法和方法进行了实验验证和比较。实验结果表明所提出的KDE-FS算法及KDE-LIATD方法均具有比较好的效果。

2 特征选择

2.1 样本特征的概率密度估计

本文从UCI的物联网僵尸网络数据集^[17]中随机抽取部分样本作为训练样本。为了得到训练集中正常样本每一维特征的特征值概率密度函数及其对应的概率密度,本文提出了一种基于高斯核密度估计的样本特征值概率密度估算(Gaussian Kernel Density Estimation-based Probability Density Estimation of Sample Eigenvalues, GKDE-PDESE)算法。核密度估计作为统计学中一种非参数估计方法,非常适用于估计未知样本集的概率密度函数。与参数估计方法相比,核密度估计方法的优势在于无须预先假设数据样本的分布模型,在不依据任何先验条件的情况下,可根据已知的数据样本或样本集,对所捕获的测试样本集进行未知概率密度的估计。

假设有数据样本集 $\{X|x_1, x_2, \dots, x_i, \dots, x_n\}$ 的 n 个样本独立分布,样本 $x_i \in X$ 的概率密度函数为 $f(x_i)$,则其核密度函数估计公式如式(1)所示:

$$\hat{f}_h(x_i) = \frac{1}{n} \sum_{j=1}^n K_h(x_i - x_j) = \frac{1}{nh} \sum_{j=1}^n K\left(\frac{x_i - x_j}{h}\right) \quad (1)$$

其中, $K(\cdot)$ 为核函数,通常具有对称性,并且满足 $\int K(x_i)dx=1$;参数 h 为核函数带宽,用于平衡核密度估计的偏差以及方差。本文使用文献[19]所提出的核参数估算方法对 h 进行估计。另外,核函数有多种选择,理论上所有平滑的峰值函数均可作为核密度估计的核函数,本文使用高斯函数作为核函数。

假定训练集中正常样本集为 $R^{n_1 \times m}$, n_1 是样本数量, m 是样本维度, 样本 $x_i \in R^{n_1 \times m}$ 代表 $R^{n_1 \times m}$ 第 i 个样本, 令 $x_i = \{x_i^1, x_i^2, \dots, x_i^d, \dots, x_i^m\}$, 则 x_i^d 代表 x_i 的第 d 维特征的特征值; 进一步, 假设 $R^{n_1 \times m}$ 中所有样本的第 d 维特征的特征值用 $a^d = \{x_1^d, x_2^d, \dots, x_{n_1}^d\}$ 表示, 则所有特征特征值集合可以用 A 表示成 $A = \{a^1, a^2, \dots, a^d, \dots, a^m\}^T$ 。当 $a^d \in A$ 时, 使用高斯核密度估计方法对 a^d 进行训练, 即可获得 $R^{n_1 \times m}$ 中所有样本第 d 维特征的特征值对应的概率密度函数 $\hat{f}^d$, 样本 $x_i \in R^{n_1 \times m}$ 的第 d 维特征的特征值概率密度为 $\hat{f}^d(x_i^d)$ 。 $\hat{f}^d(x_i^d)$ 越大, 说明 x_i^d 越符合正常样本中第 d 维特征的特征值分布。基于上述研究, 本文提出如下基于高斯核密度估计的样本特征值概率密度估算 (GKDE-PDESE) 算法, 其伪代码描述如算法 1 所示。

算法 1 GKDE-PDESE

Input: $R^{n_1 \times m}$ //input the normal sample set in training set
 Output: $F, F(A)$ //output the set of feature probability density function, the set of feature probability density

1. $A \leftarrow (R^{n_1 \times m})^T$
2. for each a^d in A do // calculate the probability density function
3. use equation (1) to calculate $\hat{f}^d$
4. $F \leftarrow \hat{f}^d$
5. end for
6. for each a^d in A do //calculate the probability density
7. for each x_i^d in a^d do
8. $\hat{f}^d(a^d) \leftarrow \hat{f}^d(x_i^d)$
9. end for
10. $F(A) \leftarrow \hat{f}^d(a^d)$
11. end for
12. return $F, F(A)$

GKDE-PDESE 算法的计算开销在于第 8—13 行, 即计算 $R^{n_1 \times m}$ 中所有样本每一维特征的特征值概率密度。由于 $R^{n_1 \times m}$ 有 n_1 个样本, 根据式(1)计算一个样本某一维特征的特征值概率密度需要执行 n_1 次计算, 因为 $R^{n_1 \times m}$ 有 n_1 个样本和 m 维特征, 因此 GKDE-PDESE 算法的时间复杂度为 $O(n^2 \cdot m)$ 。

2.2 特征选择算法

通过 GKDE-PDESE 算法可获得训练集中正常样本每一维特征的特征值概率密度函数以及对应的概率密度。当样本特征的维数很大时, 若将样本中所有特征的特征值概率密度用于异常检测, 将面临如下两个问题: 1) 样本的特征越多, 需要的计算量越大, 将增加资源有限的物联网设备异常检测的计算负载; 2) 并非所有的特征都有利于异常检测, 因此为了实现特征降维的同时进一步提高异常检测方法的效率, 本文提出了一种基于核密度估计的特征选择算法 (KDE-FS)。首先, 算法 KDE-FS 通过算法 1 获得概率密度集合 $F(A)$, 对所有 $\hat{f}^d(a^d) \in F(A)$ 按照升序进行排序, 排序结果记为 $sort(\hat{f}^d(a^d))$; 然后, 从 $sort(\hat{f}^d(a^d))$ 中选取百分比为 τ 的位置之处的值 t^d 作为第 d 维特征的异常检测阈值, 其中 τ 是一个经验参数, 通常取 $\tau = 0.1\%$ 。当某个样本 x_j 的第 d 维特征的特征值概率密度 $\hat{f}^d(x_j^d) < t^d$ 时, 说明 x_j 的第 d 维特征值是异常的。这样, 所有特征的异常检测阈值集合记为 T , 表示成 $T = \{t^1,$

$t^2, \dots, t^m\}$ 形式; 最后, 对训练集中异常样本集 $R'^{n_2 \times m}$ 的所有样本每一维特征的特征值进行异常检测, 得到 m 个异常检测结果, 记为 $Z = \{z^1, z^2, \dots, z^d, \dots, z^m\}$, 其中 z^d 表示训练集中所有异常样本第 d 维特征的特征值被检测出是异常的异常样本数量。假设训练集中异常样本数量为 n_2 , 设定阈值 α , 当 $\frac{z^d}{n_2} \geq \alpha$ 时, 则选取第 d 维特征 $feature_d$, 将其加入降维后的特征子集中, 以此类推, 直到样本中的所有特征被遍历结束。概括上述处理过程, 提出基于核密度估计的特征选择算法 (KDE-FS), 其伪代码描述如算法 2 所示。

算法 2 KDE-FS

Input: $F, F(A), R'^{n_2 \times m}$ //input the set of feature probability density function, the set of feature probability density, the abnormal sample set in training set
 Output: S //output the feature subset

1. $A' \leftarrow (R'^{n_2 \times m})^T$
2. for each $\hat{f}^d(a^d)$ in $F(A)$ do //calculate the anomaly detection threshold
3. $t^d \leftarrow \tau \times \text{sort}(\hat{f}^d(a^d))$
4. end for
5. initialize Z as N -dimensional feature anomaly detection result set
6. for each a'^d in A' do //calculate anomaly detection results
7. for each $x_i'^d$ in a'^d do
8. if $\hat{f}^d(x_i'^d) < t^d$ then
9. $z^d = z^d + 1$
10. end if
11. end for
12. end for
13. for each z^d in Z do //select feature
14. if $\frac{z^d}{n} \geq \alpha$ then
15. $S \leftarrow feature_d$
16. end if
17. end for
18. return S

KDE-FS 算法的计算开销在于第 8—14 行, 即对训练集中异常样本集 $R'^{n_2 \times m}$ 的所有样本每一维特征的特征值进行异常检测。根据式(1)计算一个样本某一维特征的特征值概率密度需要执行 n_1 次计算, 并且 $R'^{n_2 \times m}$ 一共有 n_2 个样本和 m 维特征, 因此算法 KDE-FS 的时间复杂度为 $O(n^2 \cdot m)$ 。

3 轻量级物联网异常流量检测方法

3.1 异常检测阈值计算

通过算法 1 训练得到训练集中正常样本的每一维特征的特征值概率密度函数 F 及其对应的概率密度 $F(A)$; 通过算法 2 对训练集进行特征选择, 得到特征选择后的特征子集 S 。使用特征子集 S 中的特征基于核密度估计进行异常检测。首先, 根据样本每一维特征的特征值概率密度计算生成样本的联合概率密度, 即样本的异常评估值; 然后, 从训练集中所有正常样本的异常评估值中确定异常检测阈值; 最后, 根据异常检测阈值对测试样本进行异常检测。详细过程如下。

假设经过特征抽取后的样本 $s = \{s^1, s^2, \dots, s^d, \dots, s^{m'}\}$, 则

样本 s 的异常评估值 $p(s)$ 的计算公式如式(2)所示:

$$p(s) = \sum_{d=1}^{m'} \log(\hat{f}^d(s^d)) \quad (2)$$

其中,使用自然对数的目的是“放大”样本特征的概率密度,避免在检测过程中大多数吃小数现象的发生。在此, $p(s)$ 值越大,说明样本 s 越符合正常样本的分布;反之, $p(s)$ 值越小,说明样本 s 越有可能是异常样本。

基于此,计算出训练集中所有正常样本的异常评估值 $p(R^{n_1 \times m'})$ 后,将异常评估值按照升序进行排序,排序结果记为 $\text{sort}(p(R^{n_1 \times m'}))$,从 $\text{sort}(p(R^{n_1 \times m'}))$ 中选取百分比为 τ 的位置之处的值 t 作为异常检测的阈值。当一个样本 s 的异常评估值 $p(s) < t$,说明 s 是异常样本。

虽然核密度估计方法在计算机网络异常检测领域有比较好的优势和应用价值,但是对于类似资源受限的物联网应用环境而言,依然存在着不足。例如,假设训练集有 n_1 个正常样本,进行特征选择后特征子集为 m' 维,这样,在对测试集的每一个样本进行异常检测时,由式(1)、式(2)可知,使用核密度估计方法获得测试样本的异常评估值所需的时间复杂度为 $O(n^2 \cdot m')$ 。另外,由于 n_1 的数目较大,上述方法显然不适用于物联网应用环境。因此,本文使用三次样条插值方法获得测试样本的异常评估值 $p(s)$ 的近似值。具体方法描述如下。

假设训练集中正常样本子集 $R^{n_1 \times m'}$ 的所有样本第 d 维特征的特征值集合 a^d 的最大值为 $\max(a^d)$,最小值为 $\min(a^d)$,把区间 $[\min(a^d), \max(a^d)]$ 等分成 k 个子区间,这样共有 $k+1$ 个区间值,记为 $\{v_0^d = \min(a^d) < v_1^d < \dots < v_{k-1}^d < v_k^d = \max(a^d)\}$;又假设测试集为 $R^{n_3 \times m'}$,其中 n_3 是样本数量, m' 是特征子集 S 中特征维数,当测试集样本 $x_p \in R^{n_3 \times m'}$ 的第 d 维特征 x_p^d 位于区间 $[\min(a^d), \max(a^d)]$ 时,则选取 $k+1$ 个区间值 $\{v_0^d, v_1^d, \dots, v_k^d\}$ 以及与其对应的概率密度的自然对数 $\{\log(\hat{f}^d(v_0^d)), \log(\hat{f}^d(v_1^d)), \dots, \log(\hat{f}^d(v_k^d))\}$ 作为参数,通过三次样条插值方法获得 $\log(\hat{f}^d(x_p^d))$ 的近似值 $S_d(x_p^d)$,即 $S_d(x_p^d) \approx \log(\hat{f}^d(x_p^d))$;当 x_p^d 不在区间 $[\min(a^d), \max(a^d)]$ 中时,其近似值 $S_d(x_p^d)$ 的计算公式如式(3)所示:

$$S_d(x_p^d) = -\frac{(x_p^d - x_{\text{border}}^d)^2}{2 h_d^2} + \log(\hat{f}^d(x_{\text{border}}^d)) \quad (3)$$

其中, h_d 是第 d 维特征的特征值概率密度函数 $\hat{f}^d$ 的核函数带宽, x_{border}^d 是区间内与 x_p^d 间隔最近的值。进一步,测试样本 x_p 的异常评估的近似值为 $\sum_{d=1}^{m'} S_d(x_p^d)$ 。当 $\sum_{d=1}^{m'} S_d(x_p^d) < t$ 时,说明 x_p 为异常样本;否则, x_p 为正常样本。

3.2 KDE-LIATD 方法

基于上述研究,综合算法 1、算法 2,本文进一步提出面向轻量级物联网异常流量检测模型与基于核密度估计的轻量级物联网异常流量检测(KDE-LIATD)方法。面向轻量级物联网的异常流量检测模型如图 1 所示,其中 F 为训练集中正常样本的每维特征的特征值概率密度函数集合, $F(A)$ 为训练集中正常样本的每维特征的特征值概率密度集合。

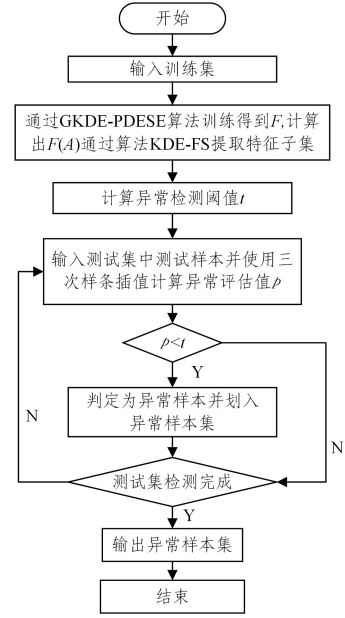


图 1 面向轻量级物联网的异常流量检测模型

Fig. 1 Model for lightweight IoT abnormal traffic detection

KDE-LIATD 方法的伪代码描述如算法 3 所示。

算法 3 KDE-LIATD

Input: $R^{n_1 \times m}, R^{n_2 \times m}, R^{n_3 \times m}$ //input the normal sample set in training set, the abnormal sample set in training set, the test set

Output: O // * output the abnormal sample set

1. $F, F(A) \leftarrow \text{GKDE-PDESE}(R^{n_1 \times m})$ //call GKDE-PDESE
2. $S \leftarrow \text{KDE-FS}(F, F(A), R^{n_2 \times m})$ //call KDE-FS
3. $R^{n_1 \times m'} \xleftarrow{S} R^{n_1 \times m}$ //extract subset from S
4. $R^{n_3 \times m'} \xleftarrow{S} R^{n_3 \times m}$ //extract subset from S
5. use equation (2) to calculate $p(R^{n_1 \times m'})$
6. $t \leftarrow \tau \times \text{Sort}(p(R^{n_1 \times m'}))$ //calculate the anomaly detection threshold
7. for each x_p in $R^{n_3 \times m'}$ do //anomaly detection process
8. initialize $\text{Score} = 0$ as anomaly evaluation value
9. for each x_p^d in x_p do //calculate the abnormal evaluation value
10. if x_p^d in interval_d then
11. use cubic spline to calculate $S_d(x_p^d)$
12. $\text{Score} = \text{Score} + S_d(x_p^d)$
13. else
14. use equation (3) to calculate $S_d(x_p^d)$
15. $\text{Score} = \text{Score} + S_d(x_p^d)$
16. end if
17. end for
18. if $\text{Score} < t$ then
19. $O \leftarrow x_p$
20. end if
21. end for
22. return O

KDE-LIATD 方法整个流程的计算开销主要由第 3 行的 GKDE-PDESE 算法与第 4 行 KDE-FS 算法产生,时间复杂度为 $O(n^2 \cdot m)$ 。

由于 KDE-LIATD 方法中所使用的 GKDE-PDESE 算法与 KDE-FS 算法的时间复杂度偏高且收集训练样本集需要时间,因此为了在家用物联网网关上实现实时轻量级异常流量检测功能,首先,在开始的一段时间内物联网网关把从流量中提取的训练样本传送到存储设备,根据专家经验标注样本是否异常;然后,存储设备通过 GKDE-PDESE 算法对训练集进行训练获得概率密度函数集合 F 及其概率密度 $F(A)$,通过 KDE-FS 算法进行特征抽取获得特征子集 S ,并根据第 3.1 节的检测阈值确定策略计算出异常检测阈值 t ,例如 $p(R^{n_1 \times m'})$ 按升序排序后,排在 $\tau \times n_1$ 位置的值即异常检测阈值 t ;最后,只需将 $R^{n_1 \times m'}$ 的 m' 维特征的 $m' \times (k+1)$ 个区间值以及对应的概率密度的自然对数、特征子集 S 、异常检测阈值 t 导入物联网网关,物联网网关计算测试样本异常评估值并据此进行异常检测。整个 KDE-LIATD 方法流程的计算开销主要由 GKDE-PDESE 算法与 KDE-FS 算法产生,时间复杂度为 $O(n^2 \cdot m)$,其中物联网网关主要执行 KDE-LIATD 方法中第 9 行之后的所有步骤,即对物联网流量中提取的测试集 $R^{n_3 \times m'}$ 进行异常检测。物联网网关通过三次样条插值方法计算测试样本的异常评估值,一个样本有 m' 维特征,因此使用三次样条插值方法计算一个样本的异常评估值需要 m' 次计算,并且测试集 $R^{n_3 \times m'}$ 共有 n_3 个测试样本,因此物联网网关执行异常检测步骤的时间复杂度为 $O(n \cdot m')$,而使用核密度估计方法获得测试样本的异常评估值所需的时间复杂度为 $O(n^2 \cdot m')$ 。可见,算法实现了轻量级物联网异常流量检测的功能。

4 实验与结果分析

4.1 实验设计

KDE-LIATD 方法的异常检测实验环境如下:操作系统为 Windows10,内存为 8 GB,处理器为 Intel Core i7-8550U CPU@1.80 GHz,所用的软件环境为 Jupyter Notebook。

实验中选取 UCI 公开的物联网僵尸网络数据集^[17],使用其中感染 Mirai 僵尸网络病毒的 7 种物联网设备的数据集进行实验。在每一种设备的数据集中,除了正常流量数据集外,依次还有 Ack, Syn, Scan, UDP, UDPplain 5 种攻击流量数据样本。该数据集将原始流量按照 Host-IP, Host-MAC&IP, Channel, Network Jitter 和 Socket 5 种类型进行了流量聚合,并使用 100 ms, 500 ms, 1.5 s, 10 s, 1 min 5 类时间窗口分别从聚合的流量中提取了 23 种特征,从而该数据集的特征一共为 115 维。数据集的特征描述如表 1 所列。

表1 数据集特征

Table 1 Data set features

Aggregation type	Features
Host-IP	Outbound packets' count, mean, variance
Host-MAC&IP	Outbound packets' count, mean, variance
Channel	Outbound packets' count, mean, variance, inbound and outbound packets' magnitude, radius, covariance, correlation coefficient
Network Jitter	Outbound packets' count, mean, variance
Socket	Outbound packets' count, mean, variance, inbound and outbound packets' magnitude, radius, covariance, correlation coefficient

由于数据样本量较多,本文针对不同设备的数据集分别

随机抽取一定数量的样本用于实验,所抽取的不同设备的样本数量如表 2 所列;对于每种设备的 5 种攻击类型的流量样本,分别随机选取 6000 条样本。实验样本集中异常样本与正常样本的比例为 3:1;最后,从实验样本集中随机抽取 70% 的样本作为训练样本,其余的 30% 作为测试集,并且训练集和测试集没有交集。

表2 实验数据集

Table 2 Experimental data set

Device type	Malicious samples	Benign samples
Doorbell(Danmini)	30 000	10 000
Thermostat(Ecobe)	30 000	10 000
Baby_Monito(B120Na0)	30 000	10 000
Security_Camera(XCS7_1002_WHT)	30 000	10 000
Security_Camera(XCS7_1003_WHT)	30 000	10 000
Security_Camera(PT_737E)	30 000	10 000
Security_Camera(PT_838)	30 000	10 000

4.2 实验与结果分析

4.2.1 评价指标

本文实验效果的评价指标使用混淆矩阵进行表示,混淆矩阵参数如表 3 所列。

表3 混淆矩阵

Table 3 Confusion matrix

	Actual: Malicious sample	Actual: Benign sample
Predicted: Malicious sample	TP	FP
Predicted: Benign sample	FP	TN

混淆矩阵参数组成的评价指标分别为精确率 (precision)、召回率 (recall)、准确率 (accuracy)、F1 值 (F-measure)、虚警率 (False Positive Rate, FRP) 和漏警率 (False Negative Rate, FNR)。

精确率表示预测正确的异常流量样本和预测为异常流量样本的比值,其计算式如式(4)所示:

Precision(P)=TP/(TP+FP) (4)

召回率表示预测正确的异常流量样本和所有真实异常流量样本的比值,其计算式如式(5)所示:

Recall(R)=TP/(TP+FN) (5)

F1=2PR/(P+R) (6)

准确率表示预测正确的样本数和总样本数的比值,其计算式如式(7)所示:

Accuracy=(TP+TN)/(TP+FP+FN+TN) (7)

虚警率表示被预测为异常流量样本的正常流量样本和正常流量样本的比值,其计算式如式(8)所示:

FPR=FP/(TN+FP) (8)

漏警率表示被预测为正常流量样本的异常流量样本和异常流量样本的比值,其计算式如式(9)所示:

FNR=FN/(TP+FN) (9)

4.2.2 实验结果与分析

(1)特征选择算法的有效性

为了验证 KDE-FS 算法的有效性,选取 Doorbell(Danmini)设备流量数据集进行实验,并同 t-SNE 特征降维算法^[20]进比较。实验中 Doorbell(Danmini)数据集经过 t-SNE 特征降

维后得到二维特征值子集,记为 s-SNE;KDE-FS 算法降维后得到的特征值子集记为 s-KDE。然后,在所产生的不同样本子集

上,通过对 KDE-LIATD 方法的 6 个评价指标的实验对比,从侧面验证 KDE-FS 算法的有效性。实验结果如表 4 所列。

表 4 不同特征下的异常检测实验结果
Table 4 Experiment results of anomaly detection under different features

	Precision/%	Recall/%	F1/%	Accuracy/%	FPR/%	FNR/%	Number of features
Raw-Danmini	87.922	69.740	77.783	70.120	28.740	30.260	115
s-SNE	96.759	1.393	2.747	26.010	0.140	98.600	2
s-KDE	99.820	100.000	99.910	99.865	0.540	0	15

使用 t-SNE 降维算法获得的特征明显不适用于本文的异常检测模型,虽然其精确率达到了 96.759%,虚警率为 0.140%,但是从其他的指标可以发现,使用 t-SNE 获得的二维特征在进行异常检测时,几乎会将所有的样本都划分为正常样本,说明 t-SNE 降维算法使得数据集中正常样本与异常样本特征值概率分布之间的差异变得不够明显。使用本文提出的 KDE-FS 算法获得的特征子集,不但使特征维数有了明显的降低,而且实验结果中精确率、F1 值、准确率都超过了 99%,特别是召回率达到了 100%,这说明使用 KDE-FS 算法获得的特征对类似 Doorbell(Danmini)异常样本集进行异常检测时,既能准确检测出异常样本,又能有效地区分正常样本。使用全部特征进行异常检测时,所有实验指标都明显不如 KDE-FS 算法。这一情况说明所有特征中存在一些与异常检测相关性不强的特征,导致一部分异常样本被误判为正常样本。在实验中,KDE-FS 算法参数 α 为 0.8,KDE-LIATD 方法百分比参数 τ 为 0.1%,特征的数值区间间隔 $k=200$,本文后面所有的实验的输入参数与之相同。

(2)异常检测模型对设备兼容性的评价

为了验证面向轻量级物联网的异常流量检测模型在不同物联网设备上的适应性,本文使用 KDE-LIATD 方法对 7 种物联网设备数据集分别进行异常检测实验,并将 7 种设备的数据集混合在一起进行异常检测实验,计算出所有检测结果的精确率、召回率、F1 值和准确率 10 次实验的平均值,实验检测结果如图 2 所示。

异常检测,检测结果的 4 种评价指标都高于 99.5%,说明本文提出的 KDE-LIATD 方法不会受到异构物联网设备混杂的影响,无须为每一种设备单独配置一种异常检测模型。这一实验结果充分说明 KDE-LIATD 方法具有比较强的鲁棒性,同时说明了本文提出的 KDE-LIATD 方法在物联网异常流量检测过程中具有一般性。

(3)KDE-LIATD 方法的高效性

为了验证 KDE-LIATD 方法能够有效且高效地检测家庭和个人物联网的异常流量,本文将 KDE-LIATD 方法与线性分类支持向量机(LSVC)^[10]、逻辑回归方法(LR)^[10]和 PCA-BPNN 方法^[11]从准确率、虚警率、漏警率三大指标进行了比较。由于在原始的数据集中,异常样本占比更大,可能会获得更高的异常检测准确率,因此为更加凸显实验效果和实验比较的公平性,本文的对比实验使用了平衡数据集,即从原始数据集中随机抽取相同比例的异常样本和正常样本进行实验。

实验结果的准确率如图 3 所示。本文提出的 KDE-LIATD 方法异常检测效果明显优于线性分类支持向量机以及逻辑回归方法。虽然 PCA-BPNN 方法在 Security_Camera(XCS7_1002_WHT)和 Security_Camera(PT_737E)设备上的异常检测的准确率与 KDE-LIATD 方法相近,但在其他设备上,KDE-LIATD 方法具有明显的优势,这是因为 KDE-LIATD 方法对每个设备提取的异常检测阈值都能够对正常流量样本与异常流量样本进行有效区分。另外,在多设备混合检测时,KDE-LIATD 方法同样表现出了优越的检测效果,异常检测表现十分稳定,而 PCA-BPNN 方法的检测准确率有明显的下降,这是因为所有设备的正常流量样本与异常流量样本之间的差异比较明显,同时不同设备的正常流量样本之间和异常流量样本之间还存在一定的差异性,导致 PCA-BPNN 方法无法对不同设备的正常流量样本与异常流量样本进行有效识别。

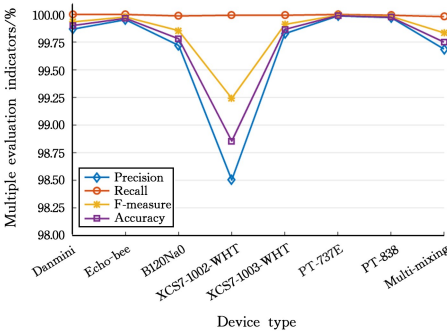


图 2 不同型号设备异常检测的多个评价指标对比图
Fig. 2 Comparison of multiple evaluation indicators for abnormal detection of different types of equipment

由图 2 可知,Security_Camera(e. g.,XCS7_1002_WHT)设备异常检测的精确率、准确率、F1 值略低于其他设备,但是依然都保持在 98.5% 以上,所有设备的召回率都高于 99.5%,这说明不同攻击产生的异常流量都能够被 KDE-LIATD 方法准确识别。将多种设备的数据混合在一起进行

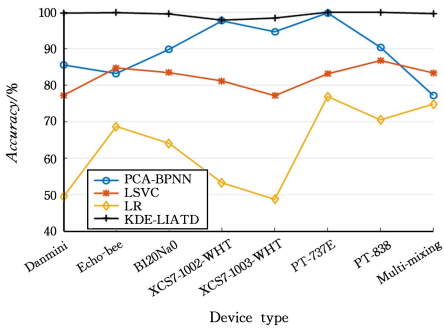


图 3 不同异常检测方法的准确率对比
Fig. 3 Comparison of accuracy of different anomaly detection methods

图 4 给出了不同异常检测方法的虚警率对比结果。由图 4 可知,相较于 KDE-LIATD 方法,其他 3 种异常检测方法的虚警率在不同设备上有着较大的起伏。除了在型号为 XCS7_1002_WHT 的设备上 KDE-LIATD 方法的虚警率略高于 PCA-BPNN 方法和线性分类支持向量机,在其他设备或者多设备混合的情况下,KDE-LIATD 方法的虚警率都处于 1% 以下,明显低于其他 3 种对比方法,这是因为 KDE-LIATD 方法的异常检测阈值是从训练集的正常样本中进行提取的,在异常检测过程中,正常样本几乎不会被划分为异常样本。

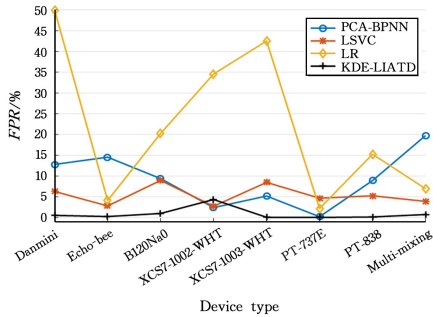


图 4 不同异常检测方法的虚警率对比

Fig. 4 Comparison of false positive rates among different anomaly detection methods

图 5 给出了不同异常检测方法的漏警率对比结果。

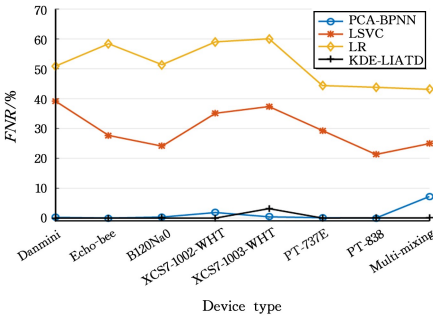


图 5 不同异常检测方法的漏警率对比

Fig. 5 Comparison of false negative rates among different anomaly detection methods

由图 5 可知,在对不同设备单独检测的情况下,KDE-LIATD方法与 PCA-BPNN 方法能够有效检测出物联网异常流量样本,而逻辑回归方法将大量的异常流量样本划分为正常流量样本,这是因为样本的特征空间太大,出现了欠拟合的现象。在多设备混合检测的情况下,KDE-LIATD 方法的检测效果明显优于其他 3 种方法,说明了 KDE-LIATD 方法从所有设备的正常样本中提取的异常检测阈值能够有效区分出异常流量样本,同时也进一步证明了所有设备的正常流量样本与异常流量样本之间具有明显的差异性。

总之,KDE-LIATD 方法不仅能够对数据样本进行特征降维,降低样本特征的维数,而且对于物联网设备具有相当的兼容性,不会受到异构物联网设备异质特性的影响,能够在多种物联网设备混杂的情况下进行异常流量检测,并且在大多数指标上有着很好的表现。

结束语 本文针对在物联网异常流量检测中家用物联网网关资源不足的客观情况,提出了一种基于核密度估计的轻

量级物联网异常流量检测方法。该方法利用高斯核密度估计方法训练得到训练集中正常样本的每一维特征的特征值概率密度函数与对应的概率密度。为了达到轻量级检测的目的,提出利用基于核密度估计的特征选择算法来抽取异常检测表现相对突出的特征,进一步利用三次样条插值的方法,获得了测试样本的异常评估值以进行异常检测。通过在公开数据集上的仿真实验,验证了本文提出的方法能够有效检测多种物联网设备的僵尸网络异常流量。实验结果表明,相比其他方法,本文提出的方法在混合多种物联网设备进行检测的情况下,异常检测效果保持稳定。虽然核密度估计方法能够作为无监督异常检测方法,但本文提出的方法中,特征选择算法部分依然需要使用已标注的异常样本集进行训练,未来的工作将尝试研究使用无监督学习的方法,以期获得与本文方法相同或者更好的检测效果。

参 考 文 献

[1] DAVIS G. Life with 50 billion connected devices [C]//2018 IEEE International Conference on Consumer Electronics (ICCE). IEEE,2018;1.

[2] ANDREA I,CHRYSOSTOMOU C,HADJICHRISTOFI G, et al. Internet of things: Security vulnerabilities and challenges [C]//2015 IEEE Symposium on Computers and Communication (ISCC). IEEE,2015;180-187.

[3] MAKHDOOM I,ABOLHASAN M,LIPMAN J,et al. Anatomy of threats to the internet of things[J]. IEEE Communications Surveys & Tutorials,2018,21(2):1636-1675.

[4] KOLIAS C,KAMBOURAKIS G,STAVROU A,et al. DDoS in the IoT: Mirai and Other Botnets[J]. Computer,2017,50(7): 80-84.

[5] VITALY S. Imperva Blocks Our Largest DDoS L7/Brute Force Attack Ever (Peaking at 292,000 RPS)[EB/OL]. (2019-07-24) [2020-03-10]. [https://www. imperva. com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps](https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps).

[6] SILVEIRA F,DIOT C,TAFT N,et al. ASTUTE: Detecting a different class of traffic anomalies[J]. ACM SIGCOMM Computer Communication Review,2010,40(4):267-278.

[7] LIASKOS C,KOTRONIS V,DIMITROPOULOS X. A novel framework for modeling and mitigating distributed link flooding attacks[C]//IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. IEEE, 2016;1-9.

[8] SEDJELMACI H,SENOUCI S M,TALEB T. An accurate security game for low-resource IoT devices[J]. IEEE Transactions on Vehicular Technology,2017,66(10):9381-9393.

[9] SMMERVILLE D H,ZACH K M,CHEN Y. Ultra-lightweight deep packet anomaly detection for Internet of Things devices [C]//2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC). IEEE,2015;1-8.

[10] HASAN M,ISLAM M M,ZARIF M I I,et al. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches[J]. Internet of Things,2019,7:100059.

[11] YANG W C, GUO Y B, ZHONG Y, et al. IoT Traffic Anomaly Detection Based on Device Type Identification and BP Neural Network[J]. Netinfo Security, 2019, 19(12): 53-63.

[12] ÖZÇELİK M, CHALABIANLOO N, GÜR G. Software-Defined Edge Defense against IoT-Based DDoS[C]// 2017 IEEE International Conference on Computer and Information Technology (CIT). IEEE, 2017: 308-313.

[13] MCDERMOTT C D, MAJDANI F, PETROVSKI A V. Botnet Detection in the Internet of Things using Deep Learning Approaches[C]// 2018 International Joint Conference on Neural Networks (IJCNN). IEEE, 2018: 1-8.

[14] DOSHI R, APTHORPE N, FEAMSTER N. Machine Learning DDoS Detection for Consumer Internet of Things Devices[C]// 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018: 29-35.

[15] DIETZ C, CASTRO R L, STEINBERGER J, et al. IoT-Botnet Detection and Isolation by Access Routers[C]// 2018 9th International Conference on the Network of the Future (NOF). IEEE, 2018: 88-95.

[16] APTHORPE N, REISMAN D, FEAMSTER N. Poster: A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic[J]. arXiv: 1705. 06805, 2017.

[17] MEIDAN Y, BOHADANA M, MATHOV Y, et al. N-BaIoT—Network-based Detection of IoT Botnet Attacks Using Deep

Autoencoders[J]. IEEE Pervasive Computing, 2018, 17(3): 12-22.

[18] MENDONÇA G, SANTOS G H A, SILVA E S, et al. An Extremely Lightweight Approach for DDoS Detection at Home Gateways[C]// 2019 IEEE International Conference on Big Data (Big Data). IEEE, 2019: 5012-5021.

[19] SILVERMAN B W. Density estimation for statistics and data analysis[M]// Boca Raton. CRC Press, 1986: 9-15.

[20] MAATEN L, HINTON G. Visualizing data using t-SNE[J]. Journal of Machine Learning Research, 2008, 9(11): 2579-2605.



ZHANG Ye, born in 1996, postgraduate, is a member of China Computer Federation. His main research interests include IoT security and information security.



LI Zhi-hua, born in 1969, Ph.D, associate professor. His main research interests include cloud computing and information security.