doi:10.3772/j.issn.1002-0470.2023.01.001

基于 BagR-CNN 检测模型的物联网网关安全加固方法①

赵 静②[*,**] 李 俊[*,**] 龙 春③[*,**] 吴玉磊[***] 万 巍[*,**] 魏金侠[*] 王显珉[****]

([*]中国科学院计算机网络信息中心 北京 100190)

([**]中国科学院大学计算机科学与技术学院 北京 100190)

([***]College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, EX4 4QF, UK)

([****]广州大学人工智能与区块链研究院 广州 511442)

摘 要 物联网(IoT)网关作为多种网络间异构数据传输与交换的关键节点近年来长期遭受大规模攻击,可靠性差,大规模流量处理延时大、抗攻击能力差等问题显著。而现有对物联网网关的可靠性研究主要集中在加密技术和可信认证机制方面,没有解决大规模攻击环境下物联网的可靠性及安全性问题。因此,本文提出了基于 BagR-CNN 检测模型的物联网网关安全加固方法,设计了可低功耗集成在物联网网关上并能够快速检测出大规模多步骤攻击的模型。首先,不同于传统的单一流量分类,本方法将相关流量聚合到一个包中,并利用基于信息熵相关性的特征增强算法提高检测准确率。其次,区别于传统的特征提取与约简方法,本文提出基于包内相似度的特征扩展方法,挖掘出隐藏的关联信息并能保证包内数据在噪声扰动下的不变性。最后,本文提出基于高斯混合模型(GMM)的特征压缩算法,将聚合包映射为一维向量并由此训练简单的卷积神经网络,以提高检测效率。实验结果表明,基于 BagR-CNN 检测模型在准确率、召回率和 F1 值等方面均优于目前对于大规模多步骤攻击的检测方法。同时,在模拟网关上运行时平均 CPU 利用率(不使用 GPU)低于 20%,证明该方法适合集成到网关而不影响网关正常的数据传输工作。

关键词 物联网(IoT)网关;安全性;可靠性;大规模攻击;聚合包表示;卷积神经网络(CNN)

0 引 言

据统计,截至 2025 年物联网(Internet of Things, IoT)设备数量预计将达到 754.4 亿[1]。无处不在的物联网设备对包括医疗健康、农业、交通、能源和环境监测在内的众多领域都产生了深远影响。不可靠的物联网设备故障可能会导致灾难性的后果,如任务失败、经济损失、人身伤害和环境危害等。

物联网是一个多网融合的网络环境,其感知层通常由各种传感网络构成用以执行不同的测量任务,支撑层则往往构建在计算能力强的传统网络上用于海量信息的计算、分析与存储[2]。物联网网关作为感知层和支撑层之间的关键连接节点,主要负责采集各种传感网络的海量异构测量数据,实现在多种感知网络之间的协议转换,集成不同来源的信息,向传统网络云端传输大规模数据并返回计算结果。此外,物联网网关还能够实现对传感子网内节点的管理,如获取节点的标识、状态、属性和资源,远程实现唤醒、控制、诊断、升级和维护功能。一旦网关被攻击者入侵,连接到网关上的物联网设备极有可能成为攻击目标;如果物联网网关宕机,所有与其相连的设备都将无法访问。因此,提高物联网网关

① 国家自然科学基金(62072127)和京津冀协同创新区综合科技服务平台研发与应用示范(YFB1405100)资助项目。

② 女,1987 年生,硕士,高级工程师;研究方向:网络安全;E-mail:jingzhao@cnic.cn。

③ 通信作者,E-mail:anquanip@cnic.cn。

(收稿日期:2021-09-18)

的安全性至关重要[3]。

目前,许多现有的解决方案已经提高了物联网网关的安全性[4-6],主要包括增强物联网网关的多向加密通道[4]、物联网网关的强身份认证方案[5]、在网关中增加攻击缓解方法及早期预警功能[6]等。但这些方案没有研究解决在面对大规模攻击时物联网网关的安全性及可靠性问题。大量的物联网智能设备往往存在匿名登录漏洞,使其很容易被黑客利用组成僵尸网络发起大规模攻击,而物联网网关则是最容易受到攻击的节点。入侵网关时,黑客会发起连续的多步隐蔽攻击,不同于分布式拒绝服务攻击(distributed denial of service, DDoS),这种攻击会占用信道资源而不被发现,不能被及时阻断[7]。

在实际应用中,一个健壮的物联网网关应该能够在大规模攻击的环境下依旧以低能耗传输和分析数据流,同时保持稳定运行[8]。然而,现有的研究并没有解决这个问题,与之相似的问题诸如攻击检测/异常检测也是作为网关的旁路方案分开考虑,大多数基于机器学习的攻击检测系统[9-10]均侧重于提高准确性和降低误报率,不适合集成到物联网网关。

目前基于机器学习的物联网攻击检测系统也存在一些明显的问题[11-13]。首先,在真实网络中,物联网网关需要进行海量的数据传输和处理,那么收到一条流就启动检测程序明显是低效的。其次,现有的研究主要关注单一网络流或数据包的分类,缺乏通过前后流量的关联,容易造成误报或漏报。而本质上,大规模爆发的网络攻击是在短时间内的多步攻击[14],单独分析每个流无法提取关键信息。并且,现有的异常检测模型为了降低后期数据处理的复杂度,往往在前期特征约简时去掉了原始的网络时间戳。失去时间戳的数据流丢失了前后关联性,丧失了最原始最有价值的信息。因此,考虑一定时间内数据流之间的关联性,重构流量在一段时间内的分布,能够挖掘出有价值的隐蔽信息。现有的一些研究在尝试解决这类问题[15-17],但不能有效检测大规模多步骤持续复杂攻击。

对此,本文设计了一种基于 BagR-CNN 检测模型的物联网网关安全加固方法,该方法可以集成到物联网网关中,确保在网关遭受到大规模攻击时依旧能稳定运行。本文的主要贡献总结如下。

(1)为了能有效集成到任何物联网网关中,并将对网关能耗的影响降到最低,本文提出了一种基于聚合包的流量表示方法。不同于现有的解决方案,即每收到一条流量都需要调用检测程序,本方法将同一类流量聚合为一个包,并提出一个新的压缩算法将包压缩为一维向量,实现上千条流量的同步检测,提高了数十倍检测效率。

(2)为了提高对大规模攻击的检测准确性,本文提出了新的特征表示方法,引入了聚合包内距离特征,距离特征通过自相似矩阵提取,反映了很多不变属性的隐藏特征。距离特征的引入保证即使一些原始流量由于信道噪声等因素发生变化,新特征表示中的值仍然保持不变。实验表明,对于大规模多步攻击的检测,本方法在精确度方面明显优于现有方法。

(3)为了评估本方法的有效性,本文设计了一个新的评估策略。在模拟网关上生成检测模型时,测试集和训练集采用不同的数据集,即一个数据集用于训练,另一个数据集用于测试。实现结果显示,产生模型 F1 分值为 88%。根据 Al-Riyami 的研究[18],如果 F1 分值超过 50%,则意味着该模型(在一个数据集上训练)开始从新的数据集中学习入侵。因此,实验证明了本文提出的方法具有普适性,可以广泛应用于各种物联网场景中。

1 相关研究

近年来,研究人员在物联网各层(包括感知层、通信层、支持层和应用层)均进行了安全性加固的研究[19],包括硬件、软件、操作系统和接口等方面,并提出了安全态势评估方法[20]。然而,物联网网关作为物联网通信层的关键设备与重要节点,对其本身的可靠性和安全性研究却明显不足,不能解决根本的痛点问题。

面向攻击环境下的物联网网关安全及可靠运行问题,Wazid 等人[21]在物联网边缘路由器中设计了检测路由攻击的入侵方案,称为“RAD-EI”,通过测量不同的网络参数判断攻击,检测率达到 95%。在

稍后的研究中,Jan 等人[22]提出了基于支持向量机(support vector machine,SVM)的轻量级嵌入式入侵检系统,能够实现多种攻击的检测,但该方法在特征选取时丢失了大量的原始特征,实验数据异常样本单一,泛化能力弱。Eskandari 等人[23]考虑到异常样本少的问题,利用传统机器学习算法学习正常特征,设计可集成于网关的智能入侵检测系统。实验结果表明,该方法对于 DDoS 类的大规模攻击识别率只有 90% 左右,且不能识别复杂攻击。物联网网关安全性及可靠性研究相关工作如表 1 所示。

目前研究很少考虑与网关融合的攻击检测方案,大部分依旧沿用了互联网的思路,设计旁路接入网关的攻击检测系统,主要聚焦于如何提高检测准确率[37]。在这一方面,基于神经网络的检测模型设计一直是研究热点,比如基于循环神经网络(recurrent neural network, RNN)的模型[38]、基于长短期记忆网络(long short-term memory,LSTM)的模型[39]、基于自动编码器的模型[40]、基于遗传算法[41]等模型。在各类方法中,卷积神经网络(convolutional neural network, CNN)作为一个经典的有监督分类模型,具有两大明显的特点:(1)权值共享;(2)平移不变性。近两年,CNN 的混合模型常用于异常检测。2019 年,杨彦荣等人[42]提出一种基于卷积神经网络和极限学习机(extreme learning machine, ELM)的组合式入侵检测算法(CNN-ELM),利用卷积神经网络模型学习原始网络数据的深层特征,用极限学习机对学习到的数据进行深层特征分类。李勇和张波[43]在 CNN 的基础上,引入 Inception 模型和残差网络,采用激活函数 ReLU,提高模型的收敛速度,使得被训练的模型泛化能力更强。2021 年,Kan 等人[44]提出了一种基于自适应粒子群优化卷积神经网络(adaptive particle swarm optimization based CNN, APSO-CNN)方法,该方法使用 PSO 算法自适应地优化一维 CNN 的结构参数,使检测模型具备自学习能力,根据损失自动调整参数。从近几年的研究可以看出,使用集成 CNN 模型能够提高模型检测准确率,但无论是与其他网络结合的方法,还是动态调整参数的方法,在检测效率方面并没有改善,反而导致模型训练时间过长。为了验证 CNN 混合模型的有效性,Ceponis 和 Goranin[45]分析了 LSTM-FCN(LSTM-fully convolutional network)、GRU-FCN(gated recurrent unit-FCN)、CNN-LSTM、CNN-GRU 等多个混合模型。结果表明,在特征维度比较单一的情况下使用集成模型,将会引入不必要的复杂度,增加训练和异常检测时间,简单模型反而更加有效。

表 1　物联网网关安全性及可靠性研究相关工作

现有工作	研究目标	研究方法	缺点
Shin[24]	可信接入	一种集成于网关的链接算法哈希表	未考虑攻击场景
Wang et al.[25]	网关的数据可靠性	自适应数据复制策略	未考虑攻击场景
Kim and Keum[26]	攻击抑制	物联网 IP 信任域	不支持大规模攻击
Lv[27]	攻击抑制	一种 Max-PSN 缓存算法	不支持大规模攻击
Yin et al.[28]	DDoS 攻击检测与抑制	一种软件定义的物联网框架及余弦相似算法	架构复杂及低准确率
Yahyaoui et al.[29]	攻击检测	支持向量机(SVM)	不支持大规模攻击
Brun and Yin[30]	攻击检测	循环神经网络(RNN)	未考虑性能与资源损耗
Hafeez et al.[31]	攻击检测	基于模糊 C-均值聚类和模糊插值的轻量级系统	98% 准确率及 40% 平均 CPU 利用率
Abdollahi and Fathi[32]	死亡 Ping 攻击检测低	基于规则的 IDS 包队列	不支持大规模攻击且性能较差
Brun et al.[33]	攻击检测	随机密度 RNN	未考虑资源损耗
Kasinathan et al.[34-35]	DDoS 攻击检测	一种分析引擎与嗅探引擎分离的检测系统	性能易受网络质量限制
BProcopiou et al.[36]	DDoS 攻击检测	基于预测与混沌理论的检测方法	94.93% ~100% 准确率

流量特征预处理是攻击检测之前的必要步骤，高质量的数据是攻击检测性能优秀的保证。在目前研究中，基于不同目的采取不同特征处理方法的研究层出不穷。在特征增强方面，Abdulhammed 等人[46]利用自动编码器和主成分分析技术，对信息增益更大的特征进行了提取，选取最优的特征。在特征数据压缩方面，在 2017 年的美国计算机协会计算机和通信安全会议上，Nasr 等人[47]为实现大规模的流量分类，利用线性投影算法对流量特征进行压缩，取得了很好的效果，但该方法仅关注流量分类，没有考虑到异常特征。2021 年，Fu 等人[48]提出了一种利用频域特征实现高维流量精准检测的方法，主要侧重于实现针对各类规避攻击具有鲁棒性。在特征扩展融合方面，李雅倩等人[49]提出了一种提取并融合多尺度特征的目标检测网络，融合多维特征生成高质量特征图以提高检测精度。在众多的特征处理方法中，高斯混合模型（Gaussian mixed model，GMM）[50]是常用的方法之一，例如在 Venugopal 和 Sundaram[51]的研究中使用 GMM 处理特征，量化了每个特征向量与其所属特征空间的关联程度，但该方法未考虑特征压缩，为后续的数据分析工作带来了一定的复杂性。

在基于流量的攻击检测研究中，大部分旨在解决单个流量的异常检测和分类，而忽略了前后流量的相关性[52]。因此，Nelms 等人[53]提出了一种流量聚合的思路，但这种方法过度依赖于流量特征，如果进行特征变换，部分属性可能会丢失或改变。为了解决这一问题，Bartos 等人[54]提出了一种新的流量聚合表示方法，该方法在特征缩放和移动时能够保持不变并实现了 90% 的准确率和 67% 的召回率。然而，在文献[54]中使用归一化直方图只是对特征进行简单的统计分析，没有考虑特征之间的差异，这种方法在分类决策函数的优化过程中较为复杂，时间复杂度高，不适用于大规模流量的处理和检测。Atli 等人[55]使用前缀树和目标 IPv4 地址的分层重击（hierarchical heavy hitters，HHH）算法来高效聚合网络数据，但前缀树的构造过程比较耗时，不能证明在大规模流量中的适用性。

基于以上对相关工作的调研与分析，在目前的研究中，针对大规模攻击下物联网网关的安全性研究相对缺少，而互联网中传统的大规模攻击检测方法因缺乏对关联性、低功耗等考虑，不能适用在物联网网关上，因此，本文的研究具有实际意义和应用价值。

2 本文方法

本节将详细介绍基于 BagR-CNN 检测模型的物联网网关安全加固方法。

整体的方法流程图如图 1 所示。

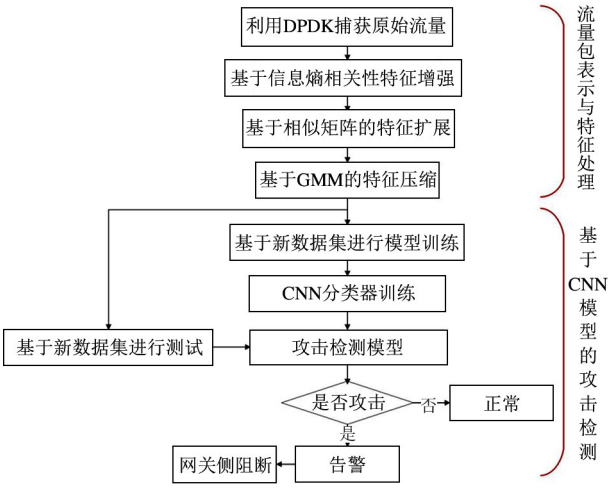


图 1 基于 BagR-CNN 检测模型的物联网网关安全加固方法整体流程

2.1 物联网流量的包表示与特征处理增强

本方法采集所有进入网关的 IoT 流量，使用数据平面开发套件（Data Plane Development Kit，DPDK）技术[56]捕获与解析高速数据流。捕获后的数据流将根据时间进行聚合分包，在聚合的数据包中，流量之间是相互关联的（例如属于同一 IP 域）。对大规模的网络流量进行聚合分包，时间切片粒度的选择对攻击检测结果影响较大。（1）检测的时效性。时间切片粒度越小，对攻击的检测就会越及时。但同时，不仅会增加数据处理的规模和模型训练的时间，而且会损失一些流量之间的关联性。（2）时序建模的有效性。选择合适的时间切片粒度会使序列在异常和正常情况下呈现明显不同的规律，从而影响后续检测结果对时间间隔的依赖。具体的选择方法将在 3.2.1 小节的实验部分详细描述。

假设大规模流量已根据时间切片完成分包,每个包内包含 m 个样本,且每个样本具有 v 个特征,则一个包可以表示为一个矩阵 $\boldsymbol{X}$:

$$\boldsymbol{X}=\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}=\begin{pmatrix}x_{11} & x_{12} & \cdots & x_{1v}\\ & & \vdots & \\ x_{m1} & x_{m2} & \cdots & x_{mv}\end{pmatrix} \tag{1}$$

其中 x_{mv} 表示为第 m 个样本的第 v 个特征,每个矩阵 $\boldsymbol{X}$ 代表了在一定时间段内相同目标地址域的流量集合。整体包变换流程如图 2 所示。

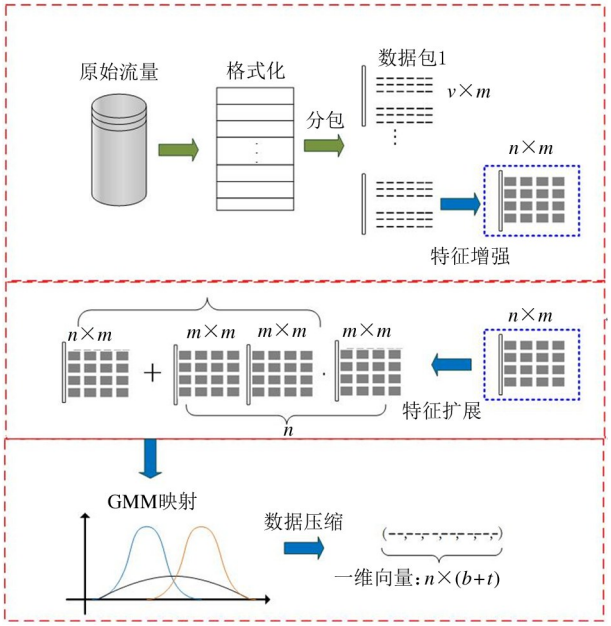


图 2　数据包变换为一维向量的处理流程

2.1.1　聚合包的零均值归一化

首先,对矩阵 $\boldsymbol{X}$ 进行归一化,并进行修正,消除极少数离群点,以提高后续的准确率。零均值化即中心化,可以加快后续神经网络的收敛速度。为了去除根号运算,加快数据处理速度,本文提出一种新的变形零均值方法,对矩阵 $\boldsymbol{X}$ 进行归一化处理,得到:

$$\tilde{\boldsymbol{X}}=\begin{pmatrix}\tilde{x}_{11} & \tilde{x}_{12} & \cdots & \tilde{x}_{1v}\\ & & \vdots & \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \cdots & \tilde{x}_{mv}\end{pmatrix},\ \tilde{x}_{lk}=\frac{x_{lk}-u(x_{lk})}{\delta(x_{lk})^2} \tag{2}$$

其中,x_{lk} 为矩阵中第 l 行第 k 列的元素,$u(x_{lk})$ 为所有样本的均值,$\delta(x_{lk})$ 为所有样本的标准差。

2.1.2　基于信息熵相关性的特征增强算法

流量中含有的冗余和噪声等特征,将会增加后续检测方法的训练时间和复杂度,相关度高的 2 个特征同时用于检测不仅对准确度的提高没有作用,反而会影响检测性能。因此,本文利用基于相关性的特征增强算法去除无用特征,进行特征增强。

针对一个特征,根据信息熵公式[57],以数据包为单位,第 k 个特征的特征熵可以计算为

$$H(X_k)=-\sum_{i=1}^{u}p(x_i)\log_2 p(x_i) \tag{3}$$

其中 u 表示特征 k 有 u 类信息,$p(x_i)$ 代表在包类别下(一个数据包中的数据只有一类标签) k 为第 i 类信息所占的比例。

针对不同的特征 a 和 b,根据条件概率熵定义,$H(X_a\mid X_b)$ 表示在已知特征 b 的情况下,特征 a 的不确定性,不确定性越高,说明 2 个特征相差越大。根据条件概率熵公式[57],在特征 b 下 a 的条件概率密度特征熵计算为

$$H(X_a\mid X_b)=\sum_{i=1}^{u'}\sum_{j=1}^{u''}p(x_i,x_j)\log_2\frac{p(x_j)}{p(x_i,x_j)} \tag{4}$$

其中,u' 和 u'' 分别代表特征 a 和特征 b 的信息类数目。由此,根据式(3)和式(4)计算一个数据包中每一维特征的相关性,表示为 $C(X_a,X_b)=\dfrac{H(X_a)-H(X_a\mid X_b)}{H(X_a)+H(X_b)}$,$0\leqslant C(X_a,X_b)\leqslant 1$。当 $C(X_a,X_b)$ 等于 0 时,表示特征 a 和 b 完全不相关,当 $C(X_a,X_b)$ 等于 1 时,表示特征 a 和 b 完全相关。

具体特征增强步骤如下。

(1)利用 SVM 算法计算全部特征的分类准确率,记为 ACC_0。

(2)根据特征熵大小进行排序,选取熵最大的特征,分别计算它与其他特征之间的相关度并排序,去掉相关度最小的特征,得到新数据包,计算得到的分类准确度为 ACC_1。如果 $ACC_1>ACC_0$,则去掉该特征,否则,则保留。以此类推,直到遍历完成,得集合 Q。

(3)在集合 Q 中,选取熵第二大的特征,重复步骤(2),以此类推,获得最优准确率的集合即为最优特征。

由此,获得新的数据包:

$$\boldsymbol{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ & & \vdots & \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix} \tag{5}$$

包内特征由 v 维强化为 n 维。在以下的研究中,数据包被认为是一个攻击检测器的输入样本。

2.1.3 基于相似度矩阵的包内距离特征扩展

考虑到一个数据包内不同样本的同维特征之间存在关联性,本节引入距离做为新特征,扩展包内原有特征,增强各样本之间的关联性。同时,距离特征的引入可以保证当包内流量遭受到同样的外界干扰(如信息污染)时,特征之间的固有属性不变,在很大程度上提高了检测准确率。

定义距离变换 $F:\mathbb{Z}\times\mathbb{Z}\rightarrow\mathbb{Z}$,以实现特征的不变性。定义 x_{pk} 和 x_{qk} 分别为一个包内第 p 行第 k 个特征及第 q 行第 k 个特征,它们之间的距离函数定义为 $f(x_{pk}, x_{qk}) = d_{pq}^k = (x_{pk} - x_{qk})^2$。根据该函数对整个矩阵 $\boldsymbol{X}$ 进行自相似矩阵变换,第 k 个特征的自相似矩阵 $\boldsymbol{D}^k \in \mathbb{R}^{m\times m}$ 被计算为

$$\boldsymbol{D}^k = \begin{pmatrix} d_{11}^k & d_{12}^k & \cdots & d_{1m}^k \\ & & \vdots & \\ d_{m1}^k & d_{m2}^k & \cdots & d_{mm}^k \end{pmatrix},\ k = 1,2,\cdots,n \tag{6}$$

则包含 n 维特征一个包矩阵 $\tilde{\boldsymbol{X}}$ 可以引入距离特征扩展为 n 个 $m\times m$ 的方阵,记为 $\boldsymbol{S} = \{\boldsymbol{D}^1, \boldsymbol{D}^2, \cdots, \boldsymbol{D}^n\}$。

特征增强后的包矩阵 $\boldsymbol{X}$ 及相似度矩阵集和 $\boldsymbol{S}$ 可以结合起来扩展为新的特征集,$\boldsymbol{X}$ 中的特征保持了原有特征的不变性,而 $\boldsymbol{S}$ 则蕴含了更多的关联信息,使得新特征集更为丰富,同时揭示了包内各样本之间的相对不变性。$\boldsymbol{X}$ 矩阵的第 k 个特征表示为 $\boldsymbol{z}_k^{\boldsymbol{X}} = (\tilde{x}_{1k}, \tilde{x}_{2k}, \cdots, \tilde{x}_{mk})^{\mathrm{T}}$, $1 \leqslant k \leqslant n$。$\boldsymbol{D}^k$ 为对称矩阵,其对角线上的元素都为 0,而其上三角及下三角上的元素完全一致可以被认为具有相同信息。因此,选择上三角元素并排成列,则 $\boldsymbol{S}$ 中第 k 个自相似矩阵可以表示大小为 $r = (m-1)\times\frac{m}{2}$ 的扁平向量 $\boldsymbol{z}_k^{\boldsymbol{D}} = (d_{21}^k, \cdots, d_{m1}^k, d_{32}^k, \cdots, d_{m2}^k, \cdots, d_{m,m-1}^k)^{\mathrm{T}}$。

至此,一个数据包则可以由 2 个矩阵集合表示。

$$\begin{aligned} \boldsymbol{X} &= (\boldsymbol{Z}^{\boldsymbol{X}}, \boldsymbol{Z}^{\boldsymbol{D}}) \\ \boldsymbol{Z}^{\boldsymbol{X}} &= (\boldsymbol{z}_1^{\boldsymbol{X}}, \boldsymbol{z}_2^{\boldsymbol{X}}, \cdots, \boldsymbol{z}_n^{\boldsymbol{X}})^{\mathrm{T}} \\ \boldsymbol{Z}^{\boldsymbol{D}} &= (\boldsymbol{z}_1^{\boldsymbol{D}}, \boldsymbol{z}_2^{\boldsymbol{D}} \cdots, \boldsymbol{z}_n^{\boldsymbol{D}})^{\mathrm{T}} \end{aligned} \tag{7}$$

与传统的特征约简及选取方法不同,本文加入了更多的数据包信息,能够更好地支持后面的模型训练。

2.1.4 基于 GMM 特征映射的数据压缩

为了提高后续攻击检测的效率,便于检测模型能以更低的能耗集成到网关中,本节提出一种基于 GMM 特征映射的数据压缩方法,将 2.1.3 节中扩展得到的包集合变换为一维向量。

众所周知,数据集中的数据分布及关系比数据本身更具有意义,例如:一条信息“年龄在 20 ~ 30 岁的人有 10 000 人”,并不能清晰表明该年龄段的人是多数还是少数,但如果将信息改为“年龄在 20 ~30 岁的人占到总人数的 30%”,则能够清楚表述。因此,本文考虑将包内的数据变换为包内数据的分布。直方图、正态分布图都是表述数据分布的经典模型,GMM 作为能够灵活地模拟任意多维数据分布的模型则是本文的首选,GMM 能够实现对无标签数据的简单分类,在图像处理、语音处理、文本分析等领域应用广泛。

基于高斯模型混合算法基础,本文定义一个向量映射函数 $\varphi(\cdot)$ 实现将扁平向量 $\boldsymbol{z}_k^{\boldsymbol{X}}$ 和 $\boldsymbol{z}_k^{\boldsymbol{D}}$ 转换成概率分布,$\varphi(\cdot)$ 表示为

$$\varphi(\boldsymbol{z};\theta_i) = \frac{1}{e}\sum_{j=1}^{e} Num\{z_j \text{ in } p(z_j \mid \theta_i)\} \tag{8}$$

其中,e 为输入向量 $\boldsymbol{z}$ 的大小,$Num\{z_j \text{ in } p(z_j \mid \theta_i)\}$ 表示输入向量的每个分量落在权值为 θ_i 上的次数,$\varphi(\boldsymbol{z};\theta_i)$ 则表示 $\boldsymbol{z}$ 中每一个元素在第 i 个高斯分量上的概率。

根据向量映射函数 $\varphi(\cdot)$,向量 $\boldsymbol{z}_k^{\boldsymbol{X}}$ 可表示为 $\psi(\boldsymbol{z}_k^{\boldsymbol{X}} \mid \theta_k^{\boldsymbol{X}}) = (\varphi(\boldsymbol{z}_k^{\boldsymbol{X}};\theta_1), \cdots, \varphi(\boldsymbol{z}_k^{\boldsymbol{X}};\theta_w))$,$w$ 为 $\boldsymbol{z}_k^{\boldsymbol{X}}$ 拟合为高斯分布上的高斯分量个数。同样,向量 $\boldsymbol{z}_k^{\boldsymbol{D}}$ 可以表示为 $\psi(\boldsymbol{z}_k^{\boldsymbol{D}} \mid \theta_k^{\boldsymbol{D}}) = (\varphi(\boldsymbol{z}_k^{\boldsymbol{D}};\theta_1), \cdots, \varphi(\boldsymbol{z}_k^{\boldsymbol{D}};\theta_t))$,$t$ 为 $\boldsymbol{z}_k^{\boldsymbol{D}}$ 拟合为高斯分布上的高斯分量个数。根据式(9)可以定义矩阵映射函数 $\psi(\boldsymbol{X},\boldsymbol{S},\theta):\mathbb{R}^{n\times(m+r)} \rightarrow \mathbb{R}^{n\times(w+t)}$,数据包 $\boldsymbol{X}$ 可以映射一个大小为 $n\times(w+t)$ 的一维向量 $(\psi(\boldsymbol{z}_1^{\boldsymbol{X}} \mid \theta_1^{\boldsymbol{X}}), \cdots, \psi(\boldsymbol{z}_n^{\boldsymbol{X}} \mid \theta_n^{\boldsymbol{X}}), \psi(\boldsymbol{z}_1^{\boldsymbol{D}} \mid \theta_1^{\boldsymbol{D}}),$

$\cdots,\psi(z_n^D \mid \theta_n^D))$。

w 和 t 表示高斯混合模型的分量个数,如果高斯分布数量过多,产生的特征维度过大,将会浪费资源且影响效率;如果高斯分布数量过少,对于包内特征分布的描述又不够准确。因此,选择合适的高斯分布数量非常重要。理论上,每一个维度的特征向量都需要一个合适的高斯分量个数,但这会用到并行计算,考虑到实验效率,本文将确定一个统一的高斯分量个数,这部分结果将在实验中给出。

2.2　基于 CNN 的攻击检测模型

经过数据包的转换与变形,攻击检测模型的训练及检测数据已转换为包含完整数据包信息的向量,本节将基于转换后的数据训练简单的基于 CNN 的攻击检测网络,该网络采用简单的参数与激活函数,深度低、规模小,能够实现快速收敛。

本节最终训练完成的 CNN 包括 7 个单元,分为卷积网络和全连接层网络 2 部分。卷积网络由 4 个单元组成,每个单元由 2 个卷积层和 1 个最大池化层组成。卷积层的主要功能是特征提取,最大池化层则用于减少每个样本的维数。为了更好地提取样本的特征,在卷积运算和最大池化层采样后,将采用补码 0 展开的方法保持特征维数不变。卷积核及最大池化层过滤器的大小分别为 3×3 和 2×2,每一层的步长及各单元的输出见表 2。在激活函数的选择上,采用 ReLU 算法替代 Sigmoid/tanh,以降低计算的复杂度,加快模型的收敛速度。

表 2　CNN 模型参数

	单元	块大小	步长	填充	激活函数	输出大小
	Input		2		ReLU	13×13
1	Conv×2	3×3	2	same	ReLU	64×64
	MaxPool	2×2	1	same	ReLU	2×2
2	Conv×2	3×3	1	same	ReLU	128×128
	MaxPool	2×2	1	same	ReLU	2×2
3	Conv×2	3×3	1	same	ReLU	256×256
	MaxPool	2×2	1	same	ReLU	2×2
4	Conv×2	3×3	1	same	ReLU	512×512
	MaxPool	2×2	1	same	ReLU	2×2
5	FC				Sigmoid	256
6	FC				Sigmoid	128
7	FC				SoftMax	2

全连接层网络由第 5 单元到第 7 单元组成,采用全连接层作为最终的分类器,分别使用 Sigmoid 和 SoftMax 作为激活函数。在模型训练过程中,采用了 Adam 优化算法。另外,根据对实验结果的分析,将学习率(learning rate,LR)调整为 0.005,批量大小设置为 128,迭代轮次(epoch)大小设置为 6000。

整体的 BagR-CNN 方法流程的伪代码如算法 1 所示。

算法 1　BagR-CNN 方法流程

Input: *flows* //IOT 流量, *time_T* //聚合时间, *c* 高斯分量数量
Output: 0 //正常,1//异常
Begin
$\boldsymbol{X} = subcontract(flows, time\_T)$ //分包,$\boldsymbol{X}$ 为一段时间聚合后的数据包
$\boldsymbol{X} = zerof(\boldsymbol{X})$ //0 均值化
$\boldsymbol{X} = fEnhance(\boldsymbol{X})$ //特征增强
$m = Rowlen(\boldsymbol{X})$ // 数据包的样本个数,即矩阵 $\boldsymbol{X}$ 行数量
$n = Columnlen(\boldsymbol{X})$ // 每个样本特征维度,即矩阵 $\boldsymbol{X}$ 列数量
for ($var\ k = 1; k \leqslant n; i++$)
  for ($var\ i = 1; i \leqslant m; i++$)
    for ($var\ j = 1; j \leqslant m; j++$)
      $D^k = dist(X_{ki} - X_{kj})$　　//自相似矩阵
for ($var\ i = 1, v = 1; i \leqslant n; i++, v++$)
  $S(v) = D^i$
$\boldsymbol{X}_{new} = \boldsymbol{X} + S$　//新数据包距离特征扩展
$data = GMMalgo(\boldsymbol{X}_{new}, c)$ //经过 GMM 映射算法转为一维向量
$parameter = TrainCNN(data_{train})$
$y = TestCNN(data_{test}, parameter)$
return y
End

3　实验及结果分析

3.1　实验环境及数据说明

为验证本文提出方法的有效性,实验搭建了一套虚拟 IoT 网关,所使用计算机基于 Windows 10 系统,处理器等配置为 Intel(R) Core (TM), i7-4720HQ,CPU @ 2.60 GHz,8 GB RAM。实验采用 Python 语言作为编程语言。本文将使用两类数据集进行实验验证。定义模型性能评估指标分别为准确

率(accuracy, ACC)、召回率(recall, R)、误报率(false positive rate, FPR)和 F1-值(F1-Score)。

首先,为了评估检测模型的性能,本文使用公开数据集 Kyoto 2006 + [58] 进行实验验证。选择 Kyoto 2006 + 数据集的原因是,一方面它相较于其他数据集更接近真实流量;另一方面,其他大部分数据集例如 KDD Cup99 在时间上缺乏连续性,不能通过包表示的方式进行处理。

其次,为了验证本方法在 IoT 网络环境中的有效性,采用 Bot-IoT (2018)数据集[59]进行验证。该数据集整合了真实和模拟的 IoT 网络流数据,网络攻击包括探测攻击、拒绝服务和信息盗窃。

3.2　参数设置与模型性能评估

3.2.1　Kyoto 2006 + 数据集上的实验结果及分析

首先,需要确定高斯分布中分量个数 c, 初始选择 5 min 作为聚合时间。根据前期工作经验,c 首先被设置为 25,然而,考虑到可能的潜在影响,本文对 c 值以 5 为间隔分别进行了实验。表 3 显示,当 c = 5 时,除误报率外的其他所有性能指标都是最优的。因此,本实验的最终确定高斯分布中分量个数 c = 5。

表 3　不同高斯分布中分量个数 c 的实验性能对比

	c	准确率	精确率	召回率	误报率	F1 分值
0	5	0.9609	0.9781	0.9805	0.3597	0.9793
1	10	0.9731	0.9870	0.9844	0.2121	0.9857
2	15	0.9648	0.9774	0.9855	0.3730	0.9814
3	20	0.9735	0.9770	0.9953	0.3838	0.9861
4	25	0.9766	0.9841	0.9914	0.3107	0.9877
5	30	0.9425	0.9425	1.0000	0.9977	0.9704

其次,需要确定第 2 个参数:聚合时间。根据上述采样结果,以 5 min 为步长选取不同的时间间隔进行实验,表 4 的结果表明,当间隔时间为 $time\_T$ = 900 s 时,实验结果性能最好。

在确定好最重要的 2 个参数之后,开始评估本方法的性能。训练好的 CNN 分类器将分别应用于原始数据集和由包表示生成的新数据集上,以证明包表示的优势。在数据处理过程中,自相似矩阵能够保证即使一个包内的所有采样的一些原始特征值发生变化,在新数据集的表示中特征值仍然保持不变。本文采用 GMM 特征映射来捕获特征之间的内部差异,从而更精确地描述特征分布。为了证明几种方法的有效性,本文进行了对比实验。对比实验具体如下:方法 1“Ini Trans”为使用没有经过包表示方法的原始数据训练的 CNN 分类器,方法 2“Bag Rep1”为使用没有扩展自相似变换特征的数据训练的 CNN 分类器,方法 3“Bag Rep2”为使用经过第 3 节描述的完整包表示方法处理的数据训练的 CNN 分类器。

表 4　不同聚合时间下的性能对比

	间隔时间/s	准确率	精确率	召回率	误报率	F1 分值
0	15	0.9130	0.9685	0.9381	0.4986	0.9531
1	60	0.9643	0.9741	0.9884	0.4302	0.9812
2	300	0.9609	0.9781	0.9805	0.3597	0.9793
3	900	0.9797	0.9802	0.9986	0.3303	0.9893
4	3600	0.9744	0.9789	0.9942	0.3501	0.9865

图 3 ~ 图 5 表示了上述 3 种方法在 3 个不同测试数据集上的受试者工作特征(receiver operating characteristic, ROC)性能表现。A、B、C 3 个测试数据集分别取自 2014 年 11 月 21 日、2015 年 1 月 2 日、2015 年 5 月 11 日。图 6 展示了不同测试数据集 A、B 和 C 的模型评估指标(area under curve, AUC)值。实验结果表明,本文提出方法的性能不依赖于特定数据集,并且在任何数据集上都是最佳的。此外,

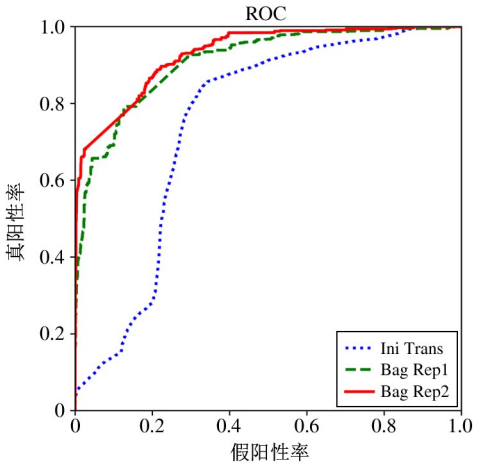


图 3　测试集 A 上 3 种数据表示方法下 CNN 分类器的 ROC 曲线

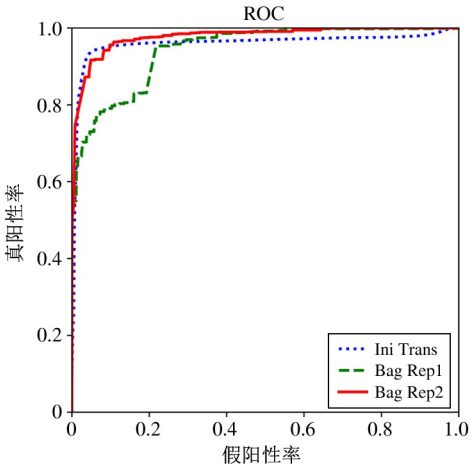


图 4　测试集 *B* 上 3 种数据表示方法下 CNN 分类器的 ROC 曲线

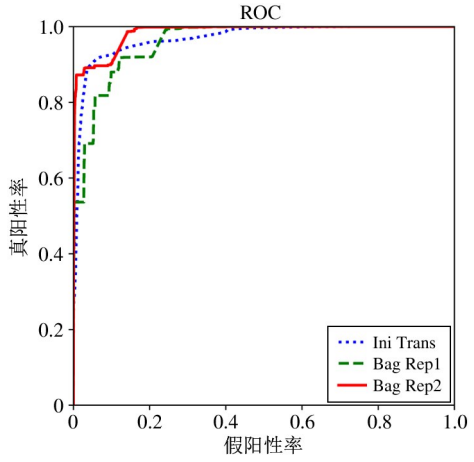


图 5　测试集 *C* 上 3 种数据表示方法下 CNN 分类器的 ROC 曲线

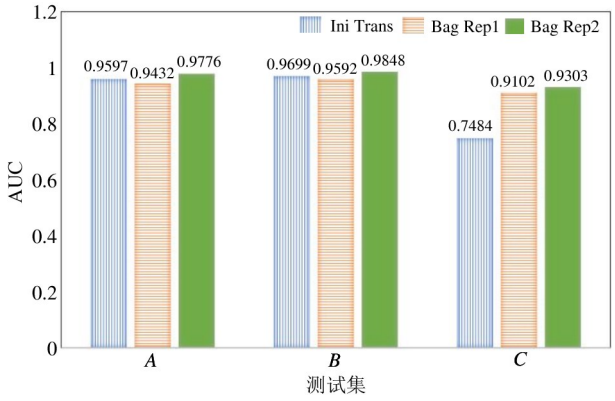


图 6　测试集 *A*、*B* 和 *C* 的 AUC 值

可以看到,本文提出的方法具有更高的真阳性率(true positive rate,TPR)和更低的假阳性率(false positive rate,FPR)。综上所述,本文提出的方法具有较高的 AUC 和较好的 ROC。

为了进一步验证本方法的先进性,实验将选取近年来部分已发表的方法与本文方法进行对比。对比结果如表 5 所示。首先与文献[60]和文献[61]中介绍的传统机器学习方法进行了比较,结果表明,本文的方法在精确率、召回率和 F1 值上都能达到更好的效果。同时,实验对比了 3 种基于 CNN 的模型[62-64],可以看出,文献[62]研究的方法综合性能最好,在准确率、精确率、召回率及误报率方面表现都很优异。文献[63]具有高精确率和低误报率,文献[64]在F1值上性能良好。相比之下,尽管本文

表 5　本文方法在不同数据集上的性能评价

检测方法	数据集	准确率	精确率	召回率	误报率	F1 分值
Salo et al.[60]	Kyoto 2006 +	/	0.898	0.851	/	0.874
Hu et al.[61]	KDD'99	/	0.896	0.849	/	0.814
Zhang et al.[62]	UNSW-NB15	0.988	0.917	0.997	0.013	0.955
Lin et al.[63]	NSL-KDD	0.851	0.917	0.811	0.097	0.861
Li et al.[64]	NSL-KDD	0.818	0.818	1.0	/	0.900
本文方法	Kyoto 2006 +	0.980	0.980	0.999	0.1	0.989

方法的误报率高于文献[62]和[64],但在其他评价指标方面具有优势。在实际应用中,最重要的目标是尽可能发现异常行为,提高检测的准确率和召回率,而 0.1 的误报率在可接受的范围内。综上所述,从整体实验结果来看,本文所提方法的整体优势仍然明显。

为进一步评估性能,本文使用较新的具有时序特征的数据集 UNSW-NB15 和 CUT13 进行对比实验,UNSW-NB15 数据集包含 49 维特征,它是由真实的正常流量和综合攻击流量混合而成;数据集 CUT13

具有 15 维特征,含有混合着正常流量的真实僵尸网络流量。表 6 显示,本文所提出方法在 Kyoto2006 + 和 CTU13 数据集上的准确率、精确率和召回率方面具有很大优势。同时,在 UNSW-NB15 数据集上的准确率和精度值也在可接受范围内。

文献[18]在第 18 届计算机和通信安全会议上提出了一个观点,即在同一个数据集中训练和测试模型,得出的实验结果是不充分的。因此,他在一个数据集中训练了模型并在另一个数据集中进行了测试,并给出了结论:如果 F1 分值低于 50%,则说明模型不适用于新的数据集;如果高于 50%,则说明模型可以学习到测试数据集的特征。基于这种理论,本文使用 kyoto 2006 + 来训练模型,并使用 CTU13 来测试模型。表 7 显示 F1 分值为 88.86%,进一步证明了本方法具有明显优势。

表 6 本文方法在不同数据集上的性能评价

数据集	准确率	精确率	召回率	误报率	F1 分值
Kyoto 2006 +	0.9800	0.9800	0.9990	0.1000	0.9890
CTU-13	0.9862	0.9862	0.9997	0.0300	0.9930
UNSW-NB15	0.9336	0.9532	0.7666	0.0122	0.8498

表 7 本文方法在不同数据集上的性能估计

训练数据	测试数据	准确率	精确率	召回率	误报率	F1 分值
Kyoto 2006 +	CTU-13	0.7995	0.9943	0.8032	0.05	0.8886
Kyoto 2006 +	UNSW-NB15	0.6500	0.8850	0.7580	0.12	0.6350
UNSW-NB15	CTU-13	0.6980	0.8350	0.7780	0.09	0.5450

3.2.2 Bot-IoT(2018)数据集上的实验结果及分析

本节将使用 UNSW 2018 IoT Botne Full5pc 4. csv 中的数据来进一步验证所提方法的有效性。其中的 70% 数据用作训练集,30% 用作测试集。定义 2 个数据集用于实验:数据集 *A* 为原始数据,数据集 *B* 为本文方法生成的聚合包。分别采用全部特征和 10 个最佳特征进行实验。

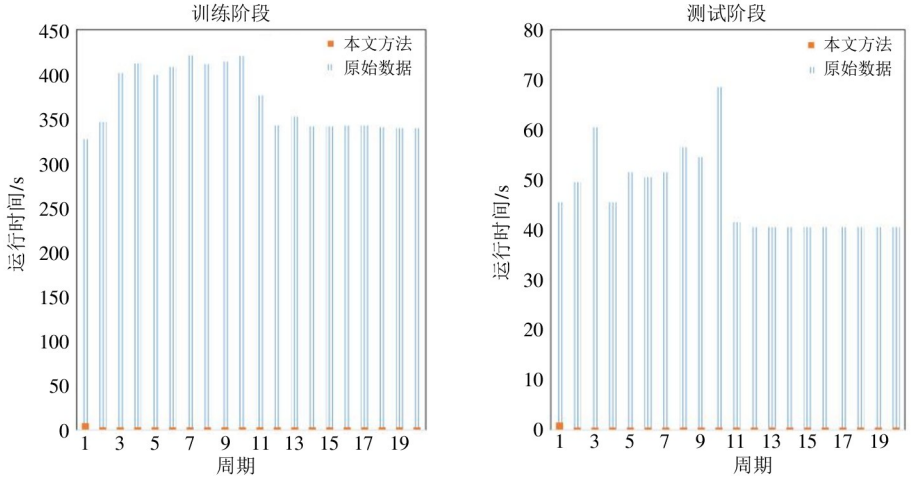
从表 8 可以看出,在数据集 *A* 上的实验结果表明采用所有特征进行实验的 F1 值低于采用 10 个最佳特征进行的实验。这说明一般的方法需要特征选择,过多的特征会降低检测精度。相比之下,在数据集 *B* 上的实验结果显示,采用所有特征进行实验的 F1 值高于采用 10 个最佳特征进行的实验,这是因为本文提出的原始流量处理方法在最大程度上保留了流量的关键特征。使用本文方法时,高维特征不会影响模型性能,反而会提高检测精度。唯一不足的是,本文方法在 IoT 网络中的假阳性率仍然较高。

表 8 本文所提方法在 BOT _ IoT 数据集上的性能

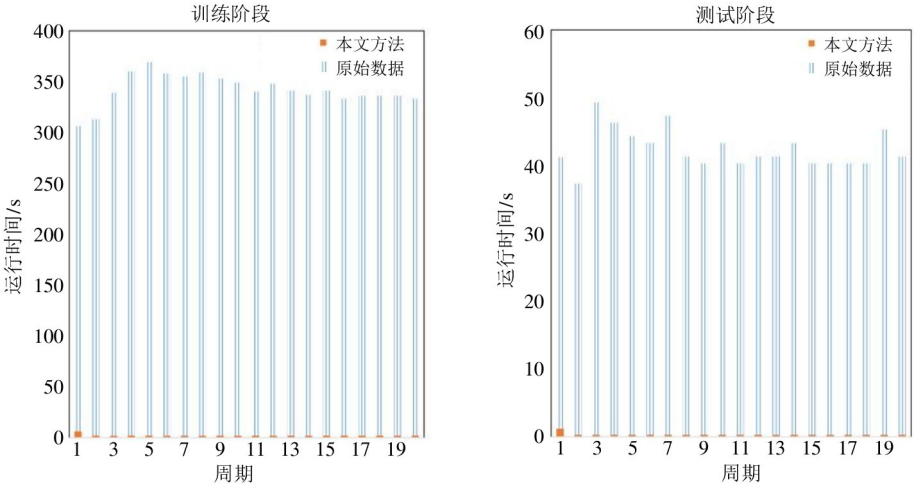
数据集	准确率	召回率	误报率	F1 分值
具有所有特征的 *A*	0.95	0.94	0.06	0.90
具有所有特征的 *B*	0.99	0.99	0.06	0.99
具有 10 个最佳特征的 *A*	0.96	0.96	0.04	0.91
具有 10 个最佳特征的 *B*	0.99	0.99	0.08	0.98

图 7(a)展示了在数据集 *A* 和 *B* 上使用所有特征进行训练时的训练时间和测试时间对比,图 7(b)展示了在数据集 *A* 和 *B* 上使用 10 个最佳特征进行训练时的训练时间和测试时间的对比。在原始数据上,平均训练时间约为 350 s,平均测试时间约为 45 s。可以看出,本文所提方法能够显著降低运行时间(平均训练时间小于 10 s,测试时间小于 2 s)。值得注意的是,选取的特征数量对运行时间几乎没有影响。

图 8 显示,当遭受大规模攻击时,计算机模拟网关的 CPU 占用率在整个实验过程中平均低于 20%,因此本文提出的方法在工作期间对计算机性能影响很小。



(a) 使用具有所有特征的 *A* 和 *B* 数据集训练时间和测试时间对比



(b) 使用具有 10 个最佳特征的 *A* 和 *B* 数据集训练时间和测试时间对比

图 7　使用不同特征的 *A* 和 *B* 数据集训练时间和测试时间对比

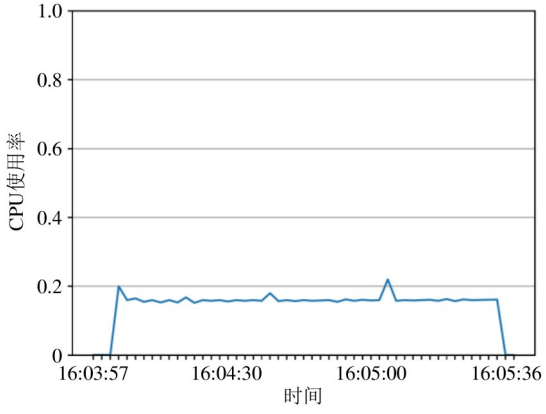


图 8　本文方法整体运行过程中的 CPU 利用率

4　结　论

本文提出了基于 BagR-CNN 检测模型的物联网网关安全加固方法,适用于集成在物联网网关中,并支持在大规模攻击环境下恶意攻击行为的轻量级检测。不同于传统的单一流量攻击检测模型,本文提出了一种基于聚合包的大规模攻击检测方法,该方法解决了现有方法存在的两大问题。问题一是忽略了流量之间的关联及噪声对流量的干扰,导致对于多步骤攻击的检测准确率低。针对这一问题,本文利用信息熵相关性算法进行了特征增强,同时,不同于传统的特征提取与约简方法,本文创新地提出基于相似度矩阵的距离特征扩展方法,挖掘隐藏信息,确保包内流量在噪声干扰下的不变性。问题二为检测效率低,每条流量的检测都需要调用检测程序,时间复杂度高。针对这一问题,本方法将同一类流量聚合为一个包,并提出一个基于 GMM 的特征压缩

算法将包压缩为一维向量,实现了上千条流量的同步检测,数十倍地提高了检测效率。实验结果表明,基于 BagR-CNN 检测模型在准确率、召回率和 F1 分值等方面均优于目前的检测方法。同时,在虚拟网关上的运行结果表明本方法检测快速、耗能低,非常适合集成在网关中。但是,本文提出的方法在误报率方面有待改善。再者,要全面保证网关在大规模攻击下的可靠运行不仅需要快速准确的检测,同时需要快速的攻击阻断,而本文因篇幅限制并未做过多说明和深入研究。后续研究将提出检测与阻断一体化的解决方案。

参考文献

[1] GAVRA V D, DOBRA I M, POP O A. A survey on threats and security solutions for IoT[C]//2020 43rd International Spring Seminar on Electronics Technology. Demanovska Valley: IEEE, 2020.

[2] AKSU D, AYDIN M A. A survey of IoT architectural reference models[C]//2019 16th International Multi-Conference on Systems, Signals & Devices. Istanbul: IEEE, 2019: 413-417.

[3] SHAKHOV V, JAN S U, AHMED S, et al. On lightweight method for intrusions detection in the Internet of Things[C]//2019 IEEE International Black Sea Conference on Communications and Networking. Sochi: IEEE, 2019.

[4] LIU C, ZHANG Y, ZHANG H. A novel approach to IoT security based on immunology[C]//2013 9th International Conference on Computational Intelligence and Security. Emeishan: IEEE, 2013: 771-775.

[5] LEE J Y, YU S J, PARK K S, et al. Secure three-factor authentication protocol for multi-gateway IoT environments[J]. Sensors, 2019,19(10):2358-2383.

[6] 王国卿, 庄雷, 王瑞民, 等. 基于时间自动机的物联网网关安全系统的建模及验证[J]. 通信学报, 2018, 39(3):63-75.

[7] DEOGIRIKAR J, VIDHATE A. Security attacks in IoT:a survey[C]//2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud). Palladam: IEEE, 2017: 32-37.

[8] ZARPELÃO B B, MIANI R S, KAWAKANI C T, et al. A survey of intrusion detection in Internet of Things[J]. Journal of Network and Computer Applications, 2017, 84: 25-37.

[9] SEDJELMACI H, SENOUCI S M, AL-BAHRI M. A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology[C]//2016 IEEE International Conference on Communications. Kuala Lumpur: IEEE, 2016.

[10] DA COSTA K A P, PAPA J P, LISBOA C O, et al. Internet of Things:a survey on machine learning-based intrusion detection approaches[J]. Computer Networks, 2019, 151: 147-157.

[11] HAJIHEIDARI S, WAKIL K, BADRI M, et al. Intrusion detection systems in the Internet of Things: a comprehensive investigation[J]. Computer Networks, 2019, 160: 165-191.

[12] ALQAHTANI M, MATHKOUR H, BEN LSMAIL M M. IoT botnet attack detection based on optimized extreme gradient boosting and feature selection[J]. Sensors, 2020, 20(21): 6336.

[13] 梁浩然, 伍军, 赵程程, 等. 基于博弈优化边缘学习的物联网入侵检测研究[J]. 物联网学报, 2021, 5(2): 37-47.

[14] DEOGIRIKAR J, VIDHATE A. Security attacks in IoT:a survey[C]//2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud). Palladam: IEEE, 2017: 32-37.

[15] HATEF M A, SHAKER V, JABBARPOUR M R, et al. HIDCC:a hybrid intrusion detection approach in cloud computing[J]. Concurrency and Computation: Practice and Experience, 2018, 30(3): 1-10.

[16] 马琳, 张莎莎, 宋姝雨,等. 基于 SDN 的智能入侵检测系统模型与算法[J]. 高技术通讯, 2020, 30(5): 103-107.

[17] ROSENBERG I, GUDES E. Bypassing system calls-based intrusion detection systems[J]. Concurrency and Computation: Practice and Experience, 2017, 29(16): 1-13.

[18] AL-RIYAMI S, COENEN F, LISITSA A. A re-evaluation of intrusion detection accuracy: alternative evaluation strategy[C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: Association for Computing Machinery, 2018: 2195-2197.

[19] XING L. Reliability in Internet of Things:current status and future perspectives[J]. IEEE Internet of Things Journal, 2020, 7(8): 6704-6721.

[20] 邵子豪, 王慧强, 孟庆川,等. 工业物联网安全态势评估方法研究综述[J]. 高技术通讯, 2020, 30(9): 908-917.

[21] WAZID M, RESHMA DSOUZA P, DAS A K, et al. RAD-EI: a routing attack detection scheme for edge-based Internet of Things environment[J]. International Journal of Communication Systems, 2019, 32(15): e4024.

[22] JAN S U, AHMED S, SHAKHOV V, et al. Toward a lightweight intrusion detection system for the Internet of Things[J]. IEEE Access, 2019, 7: 42450-42471.

[23] ESKANDARI M, JANJUA Z H, VECCHIO M, et al. Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices[J]. IEEE Internet of Things Journal, 2020, 7(8): 6882-6897.

[24] SHIN S H. Study on sensor gateway for reliable connection guarantee on large IoT environment[J]. Korea Knowledge Information Technology Society, 2015, 13(9): 131-136.

[25] WANG C, GILL C, LU C. Adaptive data replication in

real-time reliable edge computing for Internet of Things [C]//2020 IEEE/ACM 5th International Conference on Internet-of-Things Design and Implementation. Sydney: Association for Computing Machinery, 2020: 128-134.
[26] KIM E, KEUM C. Trustworthy gateway system providing IoT trust domain of smart home[C]//2017 9th International Conference on Ubiquitous and Future Networks. Milan: IEEE, 2017: 551-553.
[27] LV Z. Security of Internet of Things edge devices[J]. Software: Practice and Experience, 2020,(3):1-11.
[28] YIN D, ZHANG L, YANG K. A DDoS attack detection and mitigation with software-defined Internet of Things framework[J]. IEEE Access, 2018, 6: 24694-24705.
[29] YAHYAOUI A, ABDELLATIF T, ATTIA R. Hierarchical anomaly based intrusion detection and localization in IoT[C]//2019 15th International Wireless Communications & Mobile Computing Conference. Tangier: IEEE, 2019: 108-113.
[30] BRUN O, YIN Y. Random neural networks and deep learning for attack detection at the edge[C]//2019 IEEE International Conference on Fog Computing. Prague: IEEE, 2019: 11-14.
[31] HAFEEZ I, ANTIKAINEN M, DING A Y, et al. IoT-KEEPER:detecting malicious IoT network activity using online traffic analysis at the edge[J]. IEEE Transactions on Network and Service Management, 2020, 17(1): 45-59.
[32] ABDOLLAHI A, FATHI M. An intrusion detection system on ping of death attacks in IoT networks[J]. Wireless Personal Communications, 2020, 112: 2057-2070.
[33] BRUN O, YIN Y, GELENBE E, et al. Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments[C]//International ISCIS Security Workshop. London: IEEE, 2018: 79-89.
[34] KASINATHAN P,COSTAMAGNA G,KHALEEL H,et al. An IDS framework for Internet of Things empowered by 6LoWPAN[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: Association for Computing Machinery, 2013: 1337-1340.
[35] KASINATHAN P, PASTRONE C, SPIRITO M A, et al. Denial-of-service detection in 6LoWPAN based Internet of Things[C]//2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications. Lyon: IEEE, 2013: 600-607.
[36] PROCOPIOU A, KOMNINOS N, DOULIGERIS C. ForChaos: real time application DDoS detection using forecasting and chaos theory in smart home IoT network[J]. Wireless Communications and Mobile Computing, 2019: 1-14.
[37] ZARPELÃO B B, MIANI R S, KAWAKANI C T, et al. A survey of intrusion detection in Internet of Things[J]. Journal of Network and Computer Applications, 2017, 84: 25-37.
[38] FENG T, YUE C. Visualizing and interpreting RNN models in URL-based Phishing detection[C]//Proceedings of the 25th ACM Symposium on Access Control Models and Technologies. New York: Association for Computing Machinery, 2020: 13-24.
[39] FAN X, WAN G, ZHANG S. Industrial control system intrusion detection model based on LSTM & Attack Tree [C]//2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing. Chengdu: IEEE, 2020: 255-260.
[40] AOUEDI O, PIAMRAT K, BAGADTHEY D. A semi-supervised stacked autoencoder approach for network traffic classification[C]//2020 IEEE 28th International Conference on Network Protocols. Madrid: IEEE, 2020: 1-6.
[41] ASSIRI A. Anomaly classification using genetic algorithm-based random forest model for network attack detection [J]. CMC-Computers Materials & Continua, 2021, 66(1): 767-778.
[42] 杨彦荣, 宋荣杰, 胡国强. 基于CNN-ELM的入侵检测[J]. 计算机工程与设计, 2019,40(12): 3382-3387.
[43] 李勇, 张波. 一种基于深度 CNN 的入侵检测算法[J]. 计算机应用与软件, 2020,37(4): 324-328.
[44] KAN X, FAN Y, FANG Z, et al. A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network[J]. Information Sciences, 2021, 568: 147-162.
[45] ČEPONIS D, GORANIN N. Investigation of dual-flow deep learning models LSTM-FCN and GRU-FCN efficiency against single-flow CNN models for the host-based intrusion and malware detection task on univariate times series data[J]. Applied Sciences, 2020,10(7): 2373-2399.
[46] ABDULHAMMED R, MUSAFER H, ALESSA A, et al. Features dimensionality reduction approaches for machine learning based network intrusion detection[J]. Electronics, 2019, 8(3): 322-348.
[47] NASR M, HOUMANSADR A, MAZUMDAR A. Compressive traffic analysis: a new paradigm for scalable traffic analysis[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: Association for Computing Machinery, 2017: 2053-2069.
[48] FU C, LI Q, SHEN M, et al. Realtime robust malicious traffic detection via frequency domain analysis[C]//Proceedings of the 2021 ACM Conference on Computer and Communications Security. Seoul: Association for Computing Machinery, 2021.
[49] 李雅倩, 盖成远, 肖存军, 等. 基于细化多尺度深度特征的目标检测网络[J]. 电子学报, 2020, 48(12): 2360-2366.
[50] 管涛, 李玲玲. 高斯混合模型、求解算法及视觉应用综述[J]. 中国图象图形学报, 2012, 17(12): 1461-1471.
[51] VENUGOPAL V, SUNDARAM S. Online writer identification using GMM based feature representation and writer-specific weights[C]//2019 International Conference on Document Analysis and Recognition. Sydney: IAPR, 2019: 743-748.
[52] FAROOQI A H, KHAN F A. Intrusion detection systems for wireless sensor networks: a survey[C]//International Conference on Future Generation Communication and Networking. Berlin: IEEE, 2009: 234-241.
[53] NELMS T, PERDISCI R, ANTONAKAKIS M, et al. Webwitness: investigating, categorizing, and mitigating

malware download paths[C]//The 24th USENIX Security Symposium. Washington DC: USENIX Association, 2015: 1025-1040.
[54] BARTOS K, SOFKA M, FRANC V. Optimized invariant representation of network traffic for detecting unseen malware variants[C]//The 25th USENIX Security Symposium. Austin: USENIX Association, 2016: 807-822.
[55] ATLI B G, MICHE Y, KALLIOLA A, et al. Anomaly-based intrusion detection using extreme learning machine and aggregation of network traffic statistics in probability space[J]. Cognitive Computation, 2018, 10(5): 848-863.
[56] 赵宁, 谢淑翠. 基于 DPDK 的高效数据包捕获技术分析与应用[J]. 计算机工程与科学, 2016, 38(11): 2209-2215.
[57] 伍娟, 王仲根, 苏静明, 等.《信息理论与编码》课程教学探讨[J]. 科技风, 2021,19: 77-79.
[58] SONG J, TAKAKURA H, OKABE Y, et al. Statistical analysis of honeypot data and building of Kyoto 2006 + dataset for NIDS evaluation[C]// Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security. New York: Association for Computing Machinary, 2011: 29-36.
[59] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E, et al. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset[J]. Future Generation Computer Systems, 2019, 100: 779-796.
[60] SALO F, NASSIF A B, ESSEX A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection[J]. Computer Networks, 2019, 148: 164-175.
[61] HU B, WANG J, ZHU Y, et al. Dynamic deep forest: an ensemble classification method for network intrusion detection[J]. Electronics, 2019, 8(9): 968.
[62] ZHANG H, HUANG L, WU C Q, et al. An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset[J]. Computer Networks, 2020, 177: 107315.
[63] LIN S Z, SHI Y, XUE Z. Character-level intrusion detection based on convolutional neural networks[C]// 2018 International Joint Conference on Neural Networks. Rio de Janeiro: IEEE, 2018: 1-8.
[64] LI Z, QIN Z, HUANG K, et al. Intrusion detection using convolutional neural networks for representation learning[C]// International Conference on Neural Information Processing. Guangzhou: China Computer Federation, 2017: 858-866.

Security reinforcement method of IoT gateway based on BagR-CNN detection model

ZHAO Jing[*,**], LI Jun[*,**], LONG Chun[*,**], WU Yulei[***], WAN Wei[*,**], WEI Jinxia[*], WANG Xianmin[****]
([*] Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190)
([**] School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing 100190)
([***] College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, EX4 4QF, UK)
([****] Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou 511442)

Abstract

The reliability of Internet of Things (IoT) gateways has been significantly affected by large-scale attacks, resulting in poor reliability, high delay in processing large-scale traffic, and weak anti-attack capabilities. Existing research on the reliability of IoT gateways has mainly focused on encryption technology and trusted authentication mechanisms, without addressing the reliability and security issues of IoT in the context of large-scale attacks. Therefore, this paper proposes a security reinforcement method for IoT gateways based on the BagR-CNN detection model, which is designed to be low-power and integrated into IoT gateways, and can quickly detect large-scale multi-step attacks. Firstly, different from traditional single traffic classification, this method aggregates relevant traffic into a package and uses a feature enhancement algorithm based on information entropy correlation to improve detection accuracy. Secondly, unlike traditional feature extraction and reduction methods, this paper proposes a feature extension method based on intra-package similarity, which can mine hidden correlation information and ensure the invariance of package data under noise perturbation. Finally, this paper proposes a feature compression algorithm based on Gaussian mixed model (GMM), which maps the aggregated package to a one-dimensional vector and trains a simple convolutional neural network to improve detection efficiency. The experimental results show that the BagR-CNN detection model is superior to current detection methods for large-scale multi-step attacks in terms of accuracy, recall rate, and F1 value. Meanwhile, when running on a simulated gateway, the average CPU utilization rate (without GPU) is less than 20%, proving that this method is suitable for integration into the gateway without affecting the normal data transmission work of the gateway.

Key words: Internet of Things (IoT) gateway, security, dependability, large-scale attack, bag-representation, convolutional neural network (CNN)