第 2 卷◆第 3 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于 DANs 的设备信息安全策略分析与研究

冯烨
嘉兴职业技术学院
DOI:10.12238/acair.v2i3.8607

[摘　要] 一般情况下,双重注意网络(DANs)会通过多个步骤将设备模型的特定区域映射到加密词袋中的单词,从而整合两种模型的关键信息。在这一框架下,提出了两种DANs防护模型,旨在进行多模式的攻击和防御以及加密,以验证其性能卓越性。其推理模型允许在协作推理期间进行累积和受控的注意力引导,这对设备信息保护、信息安全等任务具有实用意义。这进一步验证了DANs在结合行为和习惯方面的有效性。
[关键词] 信息安全；词袋；注意力模型；机器学习
中图分类号：TP181　**文献标识码**：A

Analysis and research on equipment information security strategy based on DANs

Ye Feng
Jiaxing Vocational and Technical College

[Abstract] In general, dual attention networks (DANs) map specific regions of device models to words in encrypted word bags through multiple steps, thereby integrating key information from both models. Under this framework, two DANs protection models are proposed, aimed at conducting multi-mode attacks and defenses, as well as encryption, to verify their performance excellence. Its reasoning model allows for cumulative and controlled attention guidance during collaborative reasoning, which has practical significance for tasks such as device information protection and information security. This further validates the effectiveness of DANs in combining behavior and habits.
[Key words] information security; word bag; attention model; machine learning

引言

在当今数字化时代,设备信息安全已成为一个亟待解决的重要议题。随着网络威胁日益复杂多变,如何使设备具备自主防护能力,有效抵御各类信息攻击,成为了科研界和工业界共同关注的焦点。设备防护系统作为应对这一挑战的关键技术,其核心在于能够智能识别并应对各类网络信息访问问题,其性能则通常通过准确率和正确率等指标进行评估。

近年来,随着机器学习技术的飞速发展,研究人员开始探索将这一强大工具应用于设备信息安全领域,旨在通过算法让设备能够自主学习、自我防护。在这一背景下,双重注意力模型(DANs)作为一种创新的网络架构,因其能够高效处理复杂信息、提升系统防护能力而备受瞩目。[1]

1 DANs设备信息安全策略

Facebook AI Research的Jason Weston等人在2021年ICRL会议上提出了记忆网络。对于诸如自动问答、对话系统、安全策略等很多问题,系统渴望模型能够像人类一样拥有记忆功能,能够存储一定信息(比如上下文、知识库等)。为此,系统发明了多种记忆模型。其中,一种广为人知的记忆模型是长短时记忆网络(LSTM)。[2]然而,LSTM的记忆实质上是一种内部表示,只能保存使用时的一些历史信息。它类似于计算机的内存,可以存储使用时的历史输入信息(但将所有历史信息压缩到低维空间,会导致很多信息丢失),一旦不再需要,记忆就会被清除,且记忆容量非常有限。

1.1双重注意力模型

双重注意力模型(DANs)的核心思想在于利用注意力机制,将信息处理过程分解为多个步骤,并在每个步骤中精准地聚焦于关键信息,最终将两侧的有用信息有效整合。这一过程中,研究人员详细阐述了注意力机制在构建DANs各个部分时的具体应用方式,旨在通过精细化的信息处理方式,提升模型的准确性和鲁棒性。

在设备信息相关推理方面,DANs模型展现了其独特的优势。通过引入内存向量,模型能够动态地计算并更新可视化和信息化信息之间的相关性,实现两种注意力机制的深度互动。这一过程不仅增强了模型对复杂数据模式的理解能力,还为其在多样化场景下的应用提供了坚实的基础。

为了进一步提升DANs模型的性能,本系统提出了双重DANs结构,即习惯和行为注意力机制推理类(r-DANs)与匹配类(m-DANs)。r-DANs专注于多模式推理任务,能够深入挖掘数据中的潜在规律和模式;而m-DANs则侧重于多模式匹配,能够精准地识别并匹配不同来源的信息。两者虽共享同一框架,但在处理习惯和行为信息时采用了不同的策略和方法,从而实现了优势互补、协同工作的效果。

在具体实现上,本系统首先定义了双重DANs的共同框架和注意力机制的输入形式,为后续的研究奠定了统一的基础。随后,分别针对r-DANs和m-DANs在信息检测和注意力策略匹配中的具体细节进行了深入阐述,展示了它们在不同应用场景下的独特优势和潜力。

综上所述,DANs网络作为一种创新的设备信息安全防护技术,正逐步展现出其强大的潜力和广阔的应用前景。随着研究的不断深入和技术的不断完善,相信DANs网络将在未来发挥更加重要的作用,为设备信息安全保驾护航。

1.2深度LSTM阅读模型框架设计

机器学习安全策略作为一个热门方向已经经历了许多尝试。深度LSTM是相当成功的一种方法,长短期记忆网络(Long Short Term Memory networks,LSTM)是一种特殊的循环神经网络,能够解决深度学习中循环神经网络梯度消失的问题[3]。LSTM记忆模型由专门的记忆存储单元组成,通过精心设计的遗忘门、输入门和输出门来控制各个记忆存储单元的状态,通过门的控制保证了随着隐藏层在新的时间状态下不断叠加输入序列,前面的信息能够持续向后传播而不会消失。

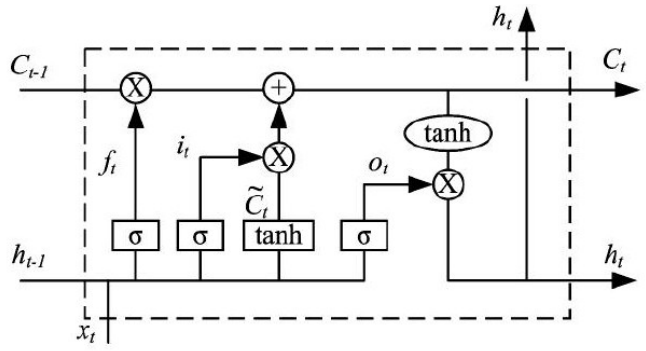

图1 LSTM记忆单元结构图

其在信息安全任务中表现卓越,将一段长的序列表示为向量,在这段向量中包含足够的信息来推导出自然语言的信息安全答案。网络将模型中的每个文档问题视为一个单一的长序列,给定嵌入的文档和查询时,网络预测的答案将随之呈现。

1.2.1模块设计

本系统将整体划分为若干模块,即用户管理、设备管理、资源管理、预约管理。这些功能使得本系统成为一个综合、可靠而高效的平台,可以有效管理用户信息、设备、资源,同时提供方便的预约服务,为学院教学提供了数字化、智能化、安全化的支持。[4]

系统选择Java开发语言及双重DANs结构神经网络,提高防护系统的稳定性和可维护性,不仅能够满足当前需求,还为未来工作提供充足的发展空间[5]。网络服务器端采用的技术是JavaEE。随着教育信息化的推进,各种新型信息技术在教育领域得到广泛应用,这促使信息技术经历了变革,也推动了设备信息和防护模式产生重大改变。

1.2.2系统部署

在系统部署阶段,通过制定系统上线的计划以确保系统能够顺利过渡到正式使用阶段。由于互联网的溢出,校企的网络应用规模和类型不断扩大,特别是对于存在分校或合作企业的学校,内网之间的交互通信安全问题显得尤为突出[6]。本系统的背景源自某大规模竞赛网络安全应用的实际案例,主要目的是分析网络安全事件和威胁风险监测情况,感知网络安全态势,并提出解决方案。

为了提供正常的网络支持服务,本方案需要考虑学校对内系统或对外门户进行统一管理。因此,本方案需要对学校安全进行远程评估和维护,对白名单内的域名进行防护,抵御恶意攻击。信息化和网络化带来了许多益处,但也暴露了许多安全隐患,这就需要通过系统的后续维护和升级计划来确保信息的稳定和安全。

2 实验分析与操作

在构建设备信息系统的过程中,确保网络服务的安全性是至关重要的,这直接关系到系统抵御潜在攻击的能力。为了实现这一目标,我们采用记忆网络作为核心模型之一,通过梯度下降算法优化基于排序(margin-based ranking)的损失函数,以训练网络参数。值得注意的是,训练记忆网络时,通常需要标记正确的记忆样本作为损失函数的依据,但在实际应用中,训练数据往往仅包含输入输出对,缺乏直接的记忆标签。为此,我们设计了功能拆分策略,按模块进行记忆计算,以确保训练的有效性和准确性。

2.1系统功能需求分析

为了满足设备信息系统的基本功能需求,系统必须包含以下几个关键模块:

(1)用户身份验证：通过实施严格的身份验证机制(如用户名密码验证、双因素认证等),确保只有经过授权的用户能够访问系统资源,从而保障系统的数据安全和功能完整性。

(2)资源管理：提供全面的资源管理功能,包括实验设备、空间等的分配、追踪和维护。管理员和用户均可通过系统实时查看资源状态、预约资源,提高资源利用率和管理效率。

(3)预约系统：通过预约系统,用户可以提前规划并锁定所需资源,有效避免资源冲突,提升使用便利性。

(4)报告上传：支持用户上传实验报告或相关文档,便于数据汇总、分析和共享。

2.2实验操作与数据集分析

在本次实验中,我们采用了DANs设备信息数据集,该数据集基于MSCOCO,包含了200K条真实的设备信息记录。每条设备信息

都与三种类型的问题相关联,且每个问题均配有人工添加的十个处理答案。为了评估模型性能,我们将数据集划分为四个部分：训练集(80K)、分训练集(40K)、分测试集(20K)和标准测试集(20K)。通过训练集和分训练集进行模型训练,利用分测试集进行模型验证,最终使用标准测试集评估模型效果。

实验任务分为开放性和多项选择两种形式,分别要求模型在回答问题时,根据是否提供候选答案集来给出最合适的答案。这种设计旨在全面检验模型在不同场景下的适应性和准确性。通过本次实验,我们期望能够进一步优化DANs模型在设备信息系统中的应用,提升其在实际环境中的表现。

为了全面评估DANs(双重注意力网络)在匹配任务中的性能,本系统采用了Flickr30K数据集。[7]该数据集包含了31,783条真实世界的图像及其对应的五个描述性句子,为图像与文本之间的关联研究提供了丰富的资源。为了实验的顺利进行,我们将数据集划分为三个部分:29,783条记录作为训练集,用于模型的训练过程；1,000条记录作为评估集,用于初步检验模型效果；剩余的1,000条记录则作为测试集,用于最终的性能评估。

在实验中,我们关注于双向信息检索任务,即图像到文本的检索以及文本到图像的检索。为了更全面地分析模型性能,我们通过调整参数k的值(k=1,5,10)来进行测试,以观察不同设置下模型的表现。

2.3结果和分析

实验结果显示,双重DANs在开放式和多项选择任务中均展现出了优异的性能,达到了最佳效果。这一成果不仅验证了双重DANs结构在处理复杂匹配任务时的有效性,也体现了其在信息防护领域的潜力。

针对计算机设备信息防护系统,本系统旨在实现以下目标：

(1)高效的资源利用,用户可以通过系统方便地预约资源,提高资源的利用率。

(2)信息透明度,用户可以实时了解使用情况,方便资源的管理和调配。

(3)安全性和稳定性,数据安全可靠,系统运行稳定,确保用户信息和数据的安全性。

尽管本文采用的方法相对基础,主要基于记忆网络的简单实现,但其展现出的强大扩展性不容忽视。每个模块均存在巨大的优化空间,为未来的研究提供了丰富的可能性。总体而言,记忆网络作为一种深度学习框架,在信息防护领域展现出了巨大的潜力,预计未来将有更多基于此框架的优秀研究成果涌现。

3 结语

综上所述,双重注意网络(DANs)成功地在可视化和信息化机制之间建立了桥梁,通过其独特的双重DANs结构实现了多模式推理与匹配。这些模型在先进的设备信息和图文匹配任务中表现出色,证明了其在提取关键信息方面的高效性。此外,双重DANs模型还具备广泛的应用前景,可拓展至计算机杀毒、敏感词检测、视频答疑等多个领域,为处理复杂行为和习惯分析任务提供有力支持。随着技术的不断进步和研究的深入,我们有理由相信,记忆网络将在信息防护领域发挥更加重要的作用。

[参考文献]

[1]宋长友.基于无人机的农村电网拓扑结构生成系统设计与实现[D].山东:山东大学,2022.

[2]张勇.基于JavaEE的远程安全评估系统的设计与实现[D].江苏:南京邮电大学,2020.

[3]罗东,钱玲,闫守洪,等.一种对FFT结果再处理以提高测频精度的方法[J].电子信息对抗技术,2021,36(6):76-78,88.

[4]宋长友.基于无人机的农村电网拓扑结构生成系统设计与实现[D].山东:山东大学,2022.

[5]Learning a hierarchical image manifold for Web image classification[J].浙江大学学报(英文版)(C辑:计算机与电子),2012,13(10):719-735.

[6]VIOLA P,JONES MJ.Robust real-time face detection[J].International Journal of Computer Vision,2004,57(2):137-154.

[7]张彬.基于大数据的Java程序设计课程辅助教学系统设计[J].信息与电脑,2022,34(13):251-253.

作者简介：

冯烨(1995--),女,汉族,浙江诸暨人,学士,职称：助理实验师,研究方向：计算机技术,互联网网络空间安全。