(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111628970 A
(43)申请公布日 2020.09.04

(21)申请号 202010332176.2

(22)申请日 2020.04.24

(71)申请人 中国科学院计算技术研究所
地址 100190 北京市海淀区中关村科学院南路6号

(72)发明人 熊威 姜海洋

(74)专利代理机构 北京泛华伟业知识产权代理有限公司 11280
代理人 郭广迅

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
G06N 3/08(2006.01)
G06N 3/04(2006.01)

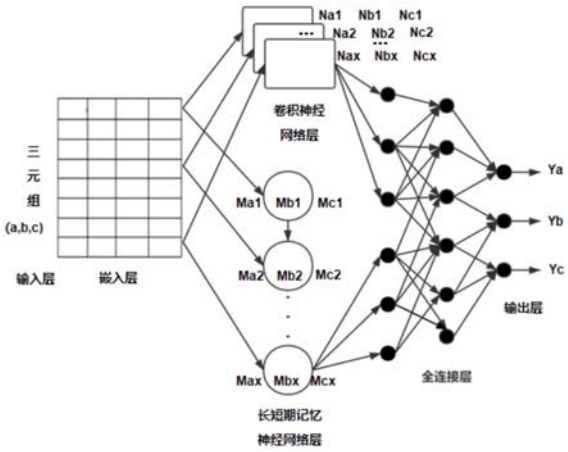
权利要求书3页 说明书14页 附图1页

(54)发明名称

一种DGA型僵尸网络的检测方法、介质和电子设备

(57)摘要

本发明实施例提供了一种DGA型僵尸网络的检测方法、介质和电子设备，该检测方法包括：B1、对所有待检测网络中的域名进行预处理得到以数值向量表示的域名；B2、将进行预处理后的待检测网络的域名输入深度神经网络模型，提取每个域名的域名深度特征向量；B3、基于提取到的每个域名的域名深度特征向量，使用聚类算法根据域名之间的距离对每个待检测网络内的域名进行聚类，以确定所述待检测网络是否是DGA型僵尸网络。本发明通过构造深度神经网络以监督学习的方式自学习域名特征，不需要人工干预，实现了域名深度特征提取，保证了域名特征的全面性和有效性，提升了检测精度。



CN 111628970 A

1.一种用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，包括：

A1、获取多个DGA域名和多个良性域名作为数据集，对数据集进行数据清洗和预处理；

A2、从经过清洗和预处理后的数据集中抽取多个域名组成训练集；

A3、将所述训练集导入深度神经网络模型进行多轮监督学习以训练其提取域名深度特征向量，将深度神经网络模型训练至收敛。

2.根据权利要求1所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述深度神经网络模型包括：输入层、嵌入层、卷积神经网络层、长短期记忆神经网络层、全连接层和输出层；其中，

输入层，用于输入以数值向量的形式表示的域名；

嵌入层，用于将域名转化为词向量矩阵；

卷积神经网络层，用于从嵌入层得到的词向量矩阵中提取域名空间特征；

长短期记忆神经网络层，用于从嵌入层得到的词向量矩阵中提取域名序列特征；

全连接层，用于对卷积神经网络输出的域名空间特征和长短期记忆神经网络层输出的域名序列特征进行整合；

输出层，用于输出经整合得到域名深度特征向量。

3.根据权利要求2所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述步骤A1包括：

A11、对数据集进行清洗，得到多个合法域名；

A12、建立域名字符与数字的映射关系，将域名的字符按照映射关系转化成数值向量，和将域名的数值向量的长度统一为第一预设长度，得到以数值向量表示的域名。

4.根据权利要求3所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述步骤A12包括：

A121、建立域名字符与数字的字符映射关系，根据所述字符映射关系将所述多个合法域名中的每个合法域名的不同字符分别映射为不同的数字；

A122、在域名的数值向量的长度超过第一预设长度的情况下删除数值向量中超过第一预设长度的元素，在域名的数值向量的长度小于第一预设长度的情况下在数值向量的末尾填充一个或者多个数值零使得域名的数值向量的长度增加到第一预设长度。

5.根据权利要求3所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述步骤A2还包括：从经过清洗和预处理后的数据集中抽取多个域名组成验证集，用于验证深度神经网络模型的准确度。

6.根据权利要求5所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述数据集中的多个DGA域名源于多个不同的DGA家族，所述训练集包含多个训练样本，每个训练样本包括锚样本、正样本和负样本，验证集包含多个验证样本，每个验证样本包括锚样本、正样本和负样本，其中，训练样本的锚样本、正样本的DGA域名与验证样本的锚样本、正样本的DGA域名彼此不重复；

对于同一个训练样本或者验证样本：

锚样本是从数据集随机选择的DGA域名；

正样本是从数据集随机选择的与锚样本属于同一DGA家族的但彼此不同的DGA域名；

负样本是从数据集随机选择的良性域名或者与锚样本属于不同DGA家族的DGA域名。

7.根据权利要求6所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述步骤A2包括针对数据集中的每一个DGA家族执行如下步骤：

A21、从当前DGA家族中随机抽取第一预设个数的域名组成该DGA家族对应的第一数组；

A22、从DGA家族中除第一数组外的剩余域名中后随机抽取第一预设个数的域名组成该DGA家族对应的第二数组；

A23、从数据集中除当前DGA家族以外的其他DGA家族和良性域名中按预设的抽取比例随机抽取第一预设个数的域名组成第三数组；

A24、从第一、第二和第三数组中分别随机抽取一个域名作为三元组的锚样本、正样本和负样本，组成第一预设个数的三元组，任意两个三元组的域名不重复。

8.根据权利要求7所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，将步骤A2得到的所有三元组的一部分作为训练集，另一部分作为验证集，其中，训练集中包含的三元组的数量与验证集中包含的三元组的数量之比的取值范围为:9:1～19:1。

9.根据权利要求6至8任一项所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述步骤A3包括：

A31、提取训练集中锚样本、正样本和负样本的域名空间特征和域名序列特征；

A32、对锚样本、正样本和负样本的域名空间特征和域名序列特征进行特征整合并在损失函数的指导下，输出锚样本、正样本和负样本的域名深度特征向量，以通过监督学习使根据深度神经网络模型输出的域名深度特征向量计算出的锚样本和正样本的距离小于锚样本和负样本的距离。

10.根据权利要求5至8任一项所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，在所述步骤A3中，训练至收敛是指深度神经网络模型在某轮训练后与训练前相比其在验证集上的准确度变化不超过预设幅度阈值。

11.根据权利要求10所述的用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，其特征在于，所述预设幅度阈值的取值范围是0.5～1％。

12.一种DGA型僵尸网络的检测方法，其特征在于，包括：

B1、对所有待检测网络中的域名进行预处理得到以数值向量表示的域名；

B2、将进行预处理后的待检测网络的域名输入根据权利要求1至11任一项所述的方法得到的深度神经网络模型，提取每个域名的域名深度特征向量；

B3、基于提取到的每个域名的域名深度特征向量，使用聚类算法根据域名之间的距离对每个待检测网络内的域名进行聚类，以确定所述待检测网络是否是DGA型僵尸网络。

13.根据权利要求12所述的DGA型僵尸网络的检测方法，其特征在于，所述步骤B1包括：

B11、根据筛选条件对待分析的域名进行筛选，保留符合筛选条件的域名；

B12、将所属主机相同的域名分到同一个待检测网络；

B13、对所有待检测网络中的域名进行预处理，包括：

建立域名字符与数字的映射关系，将域名的字符按照映射关系转化成数值向量；和

将域名的数值向量的长度统一为第一预设长度，得到以数值向量表示的域名。

14.根据权利要求13所述的DGA型僵尸网络的检测方法，其特征在于，所述筛选条件包

括:域名必须由合法字符组成、域名是二级域名或三级动态域名、域名的随机标签长度大于第二预设长度、域名在一天之内不被同一个主机重复查询。

15.根据权利要求12所述的DGA型僵尸网络的检测方法,其特征在于,在聚类所形成的类簇中存在某个类簇包含域名的数量大于预设数量阈值时,则确定该类簇所在的待检测网络是DGA型僵尸网络,其中,域名之间的距离设为域名对应的深度特征向量之间的欧式距离。

16.根据权利要求12至15任一项所述的DGA型僵尸网络的检测方法,其特征在于,在所述步骤B3中,所述聚类算法是X-means算法、DBSCAN算法或者BIRCH算法。

17.一种计算机可读存储介质,其特征在于,其上包含有计算机程序,所述计算机程序可被处理器执行以实现权利要求1至11,和,12至16中任一项所述方法的步骤。

18.一种电子设备,其特征在于,包括:

一个或多个处理器;以及,

存储器,其中存储器用于存储一个或多个可执行指令;

所述一个或多个处理器被配置为经由执行所述一个或多个可执行指令以实现权利要求1至11,和,12至16中任一项所述方法的步骤。

一种DGA型僵尸网络的检测方法、介质和电子设备

技术领域

[0001] 本发明涉及僵尸网络检测技术领域，具体来说涉及DGA型僵尸网络检测技术领域，更具体地说，涉及一种DGA型僵尸网络的检测方法、介质和电子设备。

背景技术

[0002] 僵尸网络(Botnet)是指攻击者利用僵尸病毒感染大量僵尸主机(Bot)并通过命令和控制服务器(Command and Control Server,C&C Server,简称C&C服务器)实行一对多控制的网络。DGA型僵尸网络是一种特殊的僵尸网络，它使用域名生成算法(Domain Generation Algorithm,DGA)周期性生成一组域名，这些域名被称为DGA域名，如果攻击者注册了其中一个或多个域名用做C&C服务器的域名，僵尸主机在向DNS服务器查询这组域名时，将解析到C&C服务器的IP并连接上C&C服务器，从而完成集合点(rendezvous points)迁移。DGA型僵尸网络的优势在于解决了中心节点失效问题，即使C&C服务器被安全机构关闭了，攻击者只需要重建C&C服务器并注册DGA域名就能重新控制僵尸网络。

[0003] 由于相同DGA家族生成的域名之间具有结构相似性，因此，可以利用人工提取的域名特征定义域名间距离，然后对域名聚类以实现DGA型僵尸网络的检测。例如，公开号为CN109246083A的发明申请公开了基于人工定义的域名特征并对域名聚类实现DGA型僵尸网络检测。但是，该发明申请使用人工手段提取域名特征，难以保证域名特征的全面性和有效性，也就难以保证检测精度。因此，有必要对现有技术进行改进。

发明内容

[0004] 因此，本发明的目的在于克服上述现有技术的缺陷，提供一种DGA型僵尸网络的检测方法、介质和电子设备。

[0005] 本发明的目的是通过以下技术方案实现的：

[0006] 根据本发明的第一方面，提供一种用于辅助检测DGA型僵尸网络的深度神经网络模型训练方法，包括：A1、获取多个DGA域名和多个良性域名作为数据集，对数据集进行数据清洗和预处理；A2、从经过清洗和预处理后的数据集中抽取多个域名组成训练集；A3、将所述训练集导入深度神经网络模型进行多轮监督学习以训练其提取域名深度特征向量，将深度神经网络模型训练至收敛。该实施例的技术方案至少能够实现以下有益技术效果：本发明通过训练集对深度神经网络模型进行监督学习，实现了域名特征自动提取，无需人工提取域名特征，深度神经网络提取的域名特征更加全面而有效，使得域名聚类效果得到提高，从而提高了检测精度。

[0007] 在本发明的一些实施例中，所述深度神经网络模型包括：输入层、嵌入层、卷积神经网络层、长短期记忆神经网络层、全连接层和输出层；其中，输入层，用于输入以数值向量的形式表示的域名；嵌入层，用于将域名转化为词向量矩阵；卷积神经网络层，用于从嵌入层得到的词向量矩阵中提取域名空间特征；长短期记忆神经网络层，用于从嵌入层得到的词向量矩阵中提取域名序列特征；全连接层，用于对卷积神经网络输出的域名空间特征和

长短期记忆神经网络层输出的域名序列特征进行整合;输出层,用于输出经整合得到域名深度特征向量。

[0008] 在本发明的一些实施例中,所述步骤A1包括:A11、对数据集进行清洗,得到多个合法域名;A12、建立域名字符与数字的映射关系,将域名的字符按照映射关系转化成数值向量,和将域名的数值向量的长度统一为第一预设长度,得到以数值向量表示的域名。

[0009] 在本发明的一些实施例中,所述步骤A12包括:A121、建立域名字符与数字的字符映射关系,根据所述字符映射关系将所述多个合法域名中的每个合法域名的不同字符分别映射为不同的数字;A122、在域名的数值向量的长度超过第一预设长度的情况下删除数值向量中超过第一预设长度的元素,在域名的数值向量的长度小于第一预设长度的情况下在数值向量的末尾填充一个或者多个数值零使得域名的数值向量的长度增加到第一预设长度。

[0010] 在本发明的一些实施例中,所述步骤A2还包括:从经过清洗和预处理后的数据集中抽取多个域名组成验证集,用于验证深度神经网络模型的准确度。

[0011] 在本发明的一些实施例中,所述数据集中的多个DGA域名源于多个不同的DGA家族,所述训练集包含多个训练样本,每个训练样本包括锚样本、正样本和负样本,验证集包含多个验证样本,每个验证样本包括锚样本、正样本和负样本,其中,训练样本的锚样本、正样本的DGA域名与验证样本的锚样本、正样本的DGA域名彼此不重复。

[0012] 其中,对于同一个训练样本或者验证样本:锚样本是从数据集随机选择的DGA域名;正样本是从数据集随机选择的与锚样本属于同一DGA家族的但彼此不同的DGA域名;负样本是从数据集随机选择的良性域名或者与锚样本属于不同DGA家族的DGA域名。

[0013] 在本发明的一些实施例中,所述步骤A2包括针对数据集中的每一个DGA家族执行如下步骤:A21、从当前DGA家族中随机抽取第一预设个数的域名组成该DGA家族对应的第一数组;A22、从DGA家族中除第一数组外的剩余域名中后随机抽取第一预设个数的域名组成该DGA家族对应的第二数组;A23、从数据集中除当前DGA家族以外的其他DGA家族和良性域名中按预设的抽取比例随机抽取第一预设个数的域名组成第三数组;A24、从第一、第二和第三数组中分别随机抽取一个域名作为三元组的锚样本、正样本和负样本,组成第一预设个数的三元组,任意两个三元组的域名不重复。

[0014] 优选的,将步骤A2得到的所有三元组的一部分作为训练集,另一部分作为验证集,其中,训练集中包含的三元组的数量与验证集中包含的三元组的数量之比的取值范围为:9:1～19:1。

[0015] 在本发明的一些实施例中,所述步骤A3包括:A31、提取训练集中锚样本、正样本和负样本的域名空间特征和域名序列特征;A32、对锚样本、正样本和负样本的域名空间特征和域名序列特征进行特征整合并在损失函数的指导下,输出锚样本、正样本和负样本的域名深度特征向量,以通过监督学习使根据深度神经网络模型输出的域名深度特征向量计算出的锚样本和正样本的距离小于锚样本和负样本的距离。

[0016] 优选的,训练至收敛是指深度神经网络模型在某轮训练后与训练前相比其在验证集上的准确度变化不超过预设幅度阈值。

[0017] 优选的,所述预设幅度阈值的取值范围是0.5～1%。

[0018] 根据本发明的第二方面,提供一种DGA型僵尸网络的检测方法,包括:B1、对所有待

检测网络中的域名进行预处理得到以数值向量表示的域名;B2、将进行预处理后的待检测网络的域名输入根据权利要求1至11任一项所述的方法得到的深度神经网络模型,提取每个域名的域名深度特征向量;B3、基于提取到的每个域名的域名深度特征向量,使用聚类算法根据域名之间的距离对每个待检测网络内的域名进行聚类,以确定所述待检测网络是否是DGA型僵尸网络。

[0019] 在本发明的一些实施例中,所述步骤B1包括:B11、根据筛选条件对待分析的域名进行筛选,保留符合筛选条件的域名;B12、将所属主机相同的域名分到同一个待检测网络;B13、对所有待检测网络中的域名进行预处理,包括:建立域名字符与数字的映射关系,将域名的字符按照映射关系转化成数值向量;和将域名的数值向量的长度统一为第一预设长度,得到以数值向量表示的域名。

[0020] 优选的,所述筛选条件包括:域名必须由合法字符组成、域名是二级域名或三级动态域名、域名的随机标签长度大于第二预设长度、域名在一天之内不被同一个主机重复查询。

[0021] 优选的,在聚类所形成的类簇中存在某个类簇包含域名的数量大于预设数量阈值时,则确定该类簇所在的待检测网络是DGA型僵尸网络,其中,域名之间的距离设为域名对应的深度特征向量之间的欧式距离。

[0022] 优选的,所述聚类算法是X-means算法、DBSCAN算法或者BIRCH算法。

[0023] 根据本发明的第三方面,提供一种电子设备,包括:一个或多个处理器;以及,存储器,其中存储器用于存储一个或多个可执行指令;所述一个或多个处理器被配置为经由执行所述一个或多个可执行指令以实现第一方面,和/或,第二方面所述方法的步骤。

[0024] 与现有技术相比,本发明的优点在于:

[0025] 本发明通过构造深度神经网络以监督学习的方式自学习域名特征,不需要人工干预,实现了域名深度特征提取,保证了域名特征的全面性和有效性,提升了检测精度。

附图说明

[0026] 以下参照附图对本发明实施例作进一步说明,其中:

[0027] 图1为根据本发明实施例的深度神经网络模型结构示意图;

[0028] 图2为根据本发明实施例的DGA型僵尸网络的检测方法的流程示意图。

具体实施方式

[0029] 为了使本发明的目的,技术方案及优点更加清楚明白,以下结合附图通过具体实施例对本发明进一步详细说明。应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0030] 如在背景技术部分提到的,现有的基于域名聚类的DGA型僵尸网络检测方法利用人工提取的域名特征定义域名间距离,然后对域名聚类以实现检测。这种使用人工手段提取域名特征,难以保证域名特征的全面性和有效性,也就难以保证检测精度。而本发明通过将训练集导入深度神经网络模型进行多轮监督学习以训练其提取域名深度特征向量,用训练好的深度神经网络模型提取待检测网络中域名的域名深度特征向量,并使用聚类算法根据域名深度特征向量定义的域名之间的距离对每个待检测网络内的域名进行聚类,从而发

现其中的DGA型僵尸网络。本发明通过构造深度神经网络以监督学习的方式自学习域名特征，不需要人工干预，实现了域名深度特征提取，保证了域名特征的全面性和有效性，提升了检测精度。

[0031] 在对本发明的实施例进行具体介绍之前，先对其中使用到的部分术语作如下解释：

[0032] DGA域名，是指通过域名生成算法(DGA)生成的域名。

[0033] 域名空间特征，是指将以词向量矩阵表示的域名视为图像的像素矩阵提取的空间特征。因为，域名可以表示为由词向量组成的矩阵，将词向量矩阵视为像素矩阵，则域名可以视为图像。比如，用卷积神经网络(Convolutional Neural Networks,CNN)可以提取图像的空间特征，故可用于提取域名的空间特征。典型的卷积神经网络模型有Text-CNN模型。

[0034] 域名序列特征，是指将域名表示为域名字符按一定排序组成的字符串的情况下提取的排序特征。

[0035] 域名深度特征向量，是指对域名空间特征和域名序列特征进行整合得到的特征向量。

[0036] 根据本发明的一个实施例，提供一种用于辅助检测DGA型僵尸网络的模型训练方法，包括：

[0037] 步骤A1：获取多个DGA域名和多个良性域名作为数据集，对数据集进行数据清洗和预处理。优选的，数据集中的多个DGA域名源于多个不同的DGA家族。

[0038] 根据本发明的一个实施例，多个DGA域名的DGA域名样本来自各个机构收集的DGA域名数据集。例如，包括DGArchive网站的DGA域名数据集、360公司的DGA域名数据集。DGA域名样本由88个DGA家族所生成，其中54个DGA家族生成的域名数量小于DGA域名总数的千分之一，这些DGA家族的样本数量过少，模型难以提取到这些家族的域名特征。为了使得样本平衡，只保留其余34个DGA家族所生成的域名。34个DGA家族的名称为：bamital、banjori、chinad、conficker、corebot、cryptolocker、dnschanger、dyre、emotet、gameover、gozi、locky、murofet、murofetweekly、necurs、nymaim、padcrypt、post、proslikefan、pushdo、pykspa、pykspav1、qadars、qakbot、ramnit、ranbyus、rovnix、sphinx、suppobox、symmi、tinba、tinynuke、urlzone、vidro。多个良性域名的良性域名样本来自各个机构收集的良性域名数据集。例如包括Alexa网站排名前100万的域名，del.chinaz.com查询到的合法的过期域名。

[0039] 根据本发明的一个实施例，步骤A1包括：

[0040] A11、对数据集进行清洗，包括：将域名中的大写的英文字符转为小写形式、去除重复的域名以及由不合法的字符构成的域名，得到多个合法域名；

[0041] A12、对经过清洗的数据集进行预处理，包括：

[0042] 建立域名字符与数字的映射关系，将域名的字符按照映射关系转化成数值向量，和

[0043] 将域名的数值向量的长度统一为第一预设长度，得到以数值向量表示的域名。

[0044] 优选的，构成域名的合法字符为：a、b、c、d、e、f、g、h、i、j、k、l、m、n、o、p、q、r、s、t、u、v、w、x、y、z、0、1、2、3、4、5、6、7、8、9、-、.、_。建立域名字符与数字的映射关系，例如将这里举出的39个字符分别映射到数字1至39，将域名按照字符映射关系转化成数值向量。例如：a

→1,b→2,c→3,d→4,e→5,f→6,g→7,h→8,i→9,j→10,k→11,l→12,m→13,n→14,o→15,p→16,q→17,r→18,s→19,t→20,u→21,v→22,w→23,x→24,y→25,z→26,0→27,1→28,2→29,3→30,4→31,5→32,6→33,7→34,8→35,9→36,-→37,.→38,_→39。箭头表示映射,比如,a→1则表示将a映射为1。若按照这种映射关系,abc.com转化后的数值向量为[1,2,3,38,3,15,13]。应当理解的是,此处仅是示意性的,根据不同的用户设定,具体的合法字符可以根据用户的需要设定,具体的映射关系也可根据用户的需要设定,本发明对此不作任何限制。

[0045] 根据本发明的一个实施例,步骤A12包括:

[0046] A121、建立域名字符与数字的字符映射关系,根据字符映射关系将多个合法域名中的每个合法域名的不同字符分别映射为不同的数字;

[0047] A122、在域名的数值向量的长度超过第一预设长度的情况下删除数值向量中超过第一预设长度的元素,在域名的数值向量的长度小于第一预设长度的情况下在数值向量的末尾填充一个或者多个数值零使得域名的数值向量的长度增加到第一预设长度。

[0048] 优选的,第一预设长度的取值范围例如是60～80。尤其优选,第一预设长度设为70。例如,如果域名数值向量的长度超过70,则只保留域名数值向量的前70个元素。以aa…{此处有66个字符}…abec.com为例,转换后的数值向量为[1,1,…{此处有66个数字}…,1,2,5,3,38,3,15,13],域名数值向量的长度为76,超过了70,则仅保留前70个元素,即[1,1,{此处有66个数字},1,2]。如果域名数值向量的长度小于70,则通过在向量末尾填充数字0,使得域名数值向量的长度增加为70。以前面的abc.com为例,转化后的数值向量为[1,2,3,38,3,15,13],域名数值向量的长度为7,则在13后增加63个0。

[0049] 步骤A2:从经过清洗和预处理后的数据集中抽取多个域名组成训练集。

[0050] 根据本发明的一个实施例,步骤A2还包括:从经过清洗和预处理后的数据集中抽取多个域名组成验证集,用于验证训练的深度神经网络模型的准确度。其中,训练集包含多个训练样本,每个训练样本包括锚样本、正样本和负样本,验证集包含多个验证样本,验证样本包括锚样本、正样本和负样本。训练样本的锚样本和正样本的DGA域名与验证样本的锚样本和正样本的DGA域名彼此不重复。

[0051] 对于同一个训练样本或者验证样本:

[0052] 锚样本是从数据集中随机选择的DGA域名;

[0053] 正样本是从数据集随机选择的与锚样本属于同一DGA家族的但彼此不同的DGA域名;

[0054] 负样本是从数据集随机选择的良性域名或者与锚样本属于不同DGA家族的DGA域名。该实施例的技术方案至少能够实现以下有益技术效果:由于不同的DGA家族的采用的DGA算法彼此不同,其深度特征会有区别,因此,为了区分DGA域名和良性域名的区别,以及不同DGA家族之间的域名,本发明将负样本设置为良性域名或者与正样本的DGA域名属于不同DGA家族的DGA域名,从而提高了后续检测僵尸网络的精度。

[0055] 根据本发明的一个实施例,步骤A2包括针对数据集中的每一个DGA家族执行如下步骤:

[0056] A21、从当前DGA家族中随机抽取第一预设个数的域名组成该DGA家族对应的第一数组;

[0057] A22、从DGA家族中除第一数组外的剩余域名中后随机抽取第一预设个数的域名组成该DGA家族对应的第二数组；

[0058] A23、从数据集中除当前DGA家族以外的其他DGA家族和良性域名中按预设的抽取比例随机抽取第一预设个数的域名组成第三数组；

[0059] A24、从第一、第二和第三数组中分别随机抽取一个域名作为三元组的锚样本、正样本和负样本，组成第一预设个数的三元组，其中，任意两个三元组的域名不重复。

[0060] 优选的，将步骤A2得到的所有三元组的一部分作为训练集，另一部分作为验证集，其中，训练集中包含的三元组的数量与验证集中包含的三元组的数量之比的取值范围为：9:1～19:1。

[0061] 根据本发明的一个示例，训练样本或者验证样本的结构为：(a,b,c)。(a,b,c)是由3个不同的域名组成的域名三元组，a表示锚样本(Anchor Sample)、b表示正样本(Positive Sample)，c表示负样本(Negative Sample)。需要满足条件：a和b属于相同DGA家族，a和c不属于相同DGA家族或者c是良性域名。简单的说，锚样本和正样本是同类的，锚样本和负样本是不同类的。或者说，锚样本和正样本是相似的，锚样本和负样本是非相似的。训练深度神经网络模型的目的，是要根据深度神经网络模型输出的域名深度特征向量计算出的锚样本和正样本的距离小于锚样本和负样本的距离。

[0062] 获取训练样本和验证样本时，先从多个DGA家族中的每个DGA家族中获取等量域名对，再从其他家族和良性域名数据集中按比例随机选取域名，组成多个三元组。根据本发明的一个实施例，具体流程如下：

[0063] 数据来源：

[0064] 数据集/*34个DGA家族生成的域名集合分别记为F_1,F_2,…,F_i,…,F_{34}*/

[0065] 参数：

[0066] 在每个DGA家族中抽取的域名数量M；

[0067] 抽取比例R；

[0068] 选取域名的过程对应的伪代码：

[0069] 三元组集合sample＝{}；

[0070] for i in{1,2,…,34}；

[0071] 从F_i中随机抽取M个域名，组成数组A；

[0072] 从F_i\A中随机抽取M个域名，组成数组B；

[0073] 从其他家族和良性域名数据集中按抽取比例R随机抽取M个域名，组成数组C；

[0074] for k in{1,…,M}

[0075] sample.add((A[k],B[k],C[k]))

[0076] 输出：

[0077] 三元组集合sample。

[0078] 上述实施例，考虑到样本平衡问题，根据各DGA家族的域名样本数量及良性域名的数量，M取值的设置范围为：40000到60000。尤其优选，M设为50000。在抽取负样本时，从其他家族和良性域名抽取域名的抽取比例R为3:1～5:1。尤其优选，从其他家族和良性域名抽取域名的抽取比例R为8:2。负样本中，其他家族的占比大于良性域名的占比，有助于模型更好的区分不同DGA家族的特征，从而提高检测的经度。这里总共获得136万到204万个三元组。

假设M设为50000，则获得170万个三元组。从其中选取大部分作为训练样本组成训练集，剩余部分作为验证样本组成验证集。比如，假设获得170万个三元组，选160万个三元组组成训练集用以优化深度特征提取模型，10万个三元组组成验证集用于验证深度特征提取模型。验证集内的样本不同于训练集。

[0079] 步骤A3：将训练集导入深度神经网络模型进行多轮监督学习以训练其提取域名深度特征向量，将深度神经网络模型训练至收敛。

[0080] 根据本发明的一个实施例，步骤A3包括：

[0081] A31、将训练集导入深度神经网络模型，由深度神经网络模型提取训练集中锚样本、正样本和负样本的域名空间特征和域名序列特征；

[0082] A32、对锚样本、正样本和负样本的域名空间特征和域名序列特征进行特征整合并在损失函数的指导下，输出锚样本、正样本和负样本的域名深度特征向量，以通过监督学习使根据深度神经网络模型输出的域名深度特征向量计算出的锚样本和正样本的距离小于锚样本和负样本的距离。

[0083] 优选的，训练至收敛是指深度神经网络模型在某轮训练后与训练前相比其在验证集上的准确度变化不超过预设幅度阈值。预设幅度阈值的取值范围是0.5～1％。在验证集上验证时，对于一个验证样本，若根据深度神经网络模型输出的域名深度特征向量计算出的锚样本和正样本的距离小于锚样本和负样本的距离，则深度神经网络模型针对该验证样本的输出是准确的，否则，深度神经网络模型的输出是错误的。准确度是所有准确输出的验证样本的数量与验证样本的总数量之比。

[0084] 优选的，损失函数使用三元组损失函数(Triplet Loss)。

[0085] 下面将参照一个具体的深度神经网络模型，介绍如何利用上述训练方法对其进行训练。该深度神经网络模型的结构如图1所示，包括：输入层、嵌入层、卷积神经网络层、长短期记忆神经网络层、全连接层和输出层。

[0086] 其中，输入层用于输入以数值向量的形式表示的域名。其中，输入以数值向量的形式表示的域名是将三元组形式的训练样本作为一个训练单元输入输入层。换言之，输入层输入的是三元组形式的样本。即，把锚样本、正样本和负样本组成的一个三元组一起输入到输入层，然后得到三元组中每个域名的域名深度特征向量，目的是要用训练集对深度神经网络模型进行不断的监督训练以使根据深度神经网络模型输出的锚样本域名深度特征向量和正样本域名深度特征向量的距离小于锚样本域名深度特征向量和负样本域名深度特征向量的距离。例如，在训练时，输入层输入三元组形式的训练样本，即三元组(a,b,c)。一个训练样本作为一个训练单元训练完成后再输入下一个训练样本。

[0087] 嵌入层用于将域名转化为词向量矩阵。例如，将以数值向量形式表示的a、b、c转换为以词向量形式表示的a’、b’、c’。

[0088] 卷积神经网络层用于从嵌入层得到的词向量矩阵中提取域名空间特征。例如，针对锚样本a，提取其域名空间特征[Na1,Na2,……,Nax]，针对正样本b，提取其域名空间特征[Nb1,Nb2,……,Nbx]，针对负样本c，提取其域名空间特征[Nc1,Nc2,……,Ncx]。其中，x是指各域名的域名空间特征中的元素的个数。Na1,Na2,……,Nax,Nb1,Nb2,……,Nbx,Nc1,Nc2,……,Ncx中的每个元素都是向量矩阵。

[0089] 长短期记忆神经网络层用于从嵌入层得到的词向量矩阵中提取域名序列特征。例

如,针对锚样本a,提取其域名序列特征[Ma1,Ma2,……,Max],针对正样本b,提取其域名序列特征[Mb1,Mb2,……,Mbx],针对负样本c,提取其域名序列特征[Mc1,Mc2,……,Mcx]。其中,x是指各域名的域名序列特征中的元素的个数。Ma1,Ma2,……,Max,Mb1,Mb2,……,Mbx,Mc1,Mc2,……,Mcx中的每个元素都是向量矩阵。

[0090] 全连接层用于对卷积神经网络输出的域名空间特征和长短期记忆神经网络层输出的域名序列特征进行抽象和整合。即,对锚样本a的域名空间特征[Na1,Na2,……,Nax]和[Ma1,Ma2,……,Max]进行整合,对正样本b的域名空间特征[Nb1,Nb2,……,Nbx]和域名序列特征[Mb1,Mb2,……,Mbx]进行整合,对负样本的域名空间特征[Nc1,Nc2,……,Ncx]和域名序列特征[Mc1,Mc2,……,Mcx]进行整合。

[0091] 输出层用于输出经整合得到域名深度特征向量。每一个训练样本训练完成后,会输出三元组中各域名的域名深度特征向量。例如,输出锚样本的域名深度特征向量Ya、正样本的域名深度特征向量Yb、负样本的域名深度特征向量Yc。

[0092] 其中,嵌入层(Embedding层)的作用是学习出域名字符的向量表示。Embedding层通过嵌入矩阵对字符进行线性变换,将不同的字符映射为不同的向量,并且通过反向传播更新嵌入矩阵,改变字符与向量的映射关系。

[0093] 变换公式如下所示:

[0094] $$e_i = x_i^T * w$$

[0095] 其中,x_i表示某个字符的独热码(one-hot)编码向量,T表示转置,w表示嵌入矩阵,e_i为嵌入层的输出向量。

[0096] 经过嵌入层转换后,域名字符之间不再是独立的,而是具有内在联系,因而有利于卷积神经网络层(CNN层)和长短期记忆神经网络层(LSTM层)提取域名特征。

[0097] 词向量矩阵的大小为第一预设长度乘以预设维度。预设维度的取值范围优选为48～96维,尤其优选为64维。如果第一预设长度设为70,预设维度设为64维,则词向量矩阵的大小为70×64,即每个域名字符被映射为一个64维的数值向量。

[0098] 卷积神经网络层的作用是利用卷积神经网络CNN抽象域名的局部特征,实现空间维度上的域名特征提取。卷积神经网络层执行的操作包括卷积操作和池化操作。

[0099] 在卷积操作中,使用多个不同尺寸的卷积核扫描字符矩阵,获得不同的感受视野,然后通过池化操作降低特征维度,最终通过特征融合,获得域名在空间维度上的特征。卷积(Convolution)操作利用卷积核感知域名局部特征。卷积核的参数是共享的,即在卷积过程中的卷积核的权重不会改变,这说明可以使用一个卷积核提取域名不同位置的相同特征,因而通过增加卷积核的数目和改变卷积核的尺寸,就可以提取到不同视野范围内的不同局部特征。例如,使用大小为2*64、3*64、4*64、5*64、7*64的卷积核各10个。

[0100] 在池化(Pooling)操作中,通过保留主要的特征,降低特征维度,能有效防止过拟合。

[0101] 上述技术方案,使用1-Max池化得到卷积层输出向量的最大元素值。

[0102] 计算公式如下:

[0103] $f_n = \max(c_1, c_2, ... c_t, ..., c_T)$

[0104] 其中,c_t表示的输入向量c的第t位置的元素值,T表示向量长度,f_n表示输出值。

[0105] 长短期记忆神经网络层的长短期记忆神经网络(LSTM)是一种特殊的循环神经网

络。长短期记忆神经网络通过引入门机制，解决了普通RNN存在的梯度消失和梯度爆炸问题，能够长期保留上下文历史信息，从而实现域名的字符的域名序列特征提取。DGA域名的字符排列规律通常不同于良性域名，比如，良性域名中辅音字母后面经常会出现元音字母，具有可发音的特性，而DGA域名的字符组合通常具有更大的随机性。将域名字符按从左至右的顺序输入长短期记忆神经网络，经过多轮迭代后域名中隐藏的序列特征被长短期记忆神经网络学习出来。由于DGA域名普遍较长，相比于普通RNN，长短期记忆神经网络能记住更长时间的信息，因而具有更强学习能力。优选的，长短期记忆神经网络层的神经元(cell)的数量的设置范围为96到156。尤其优选，长短期记忆神经网络层的神经元(cell)的数量设为128。

[0106] 全连接层的作用是将两种域名特征向量拼接后，通过权值矩阵对拼接向量进行线性变换，以实现两种特征的融合(整合)，并最终输出域名深度特征向量。本发明通过提取域名空间特征和域名序列特征，并在损失函数的指导下对域名空间特征和域名序列特征进行特征整合得到域名深度特征向量，不用人工定义特征，这些过程都是自动的，不需要人工干预，由此，让本发明的模型具有更加全面、有效地提取域名的特征向量的能力，有助于提升检测DGA型僵尸网络的检测精度。

[0107] 优选的，全连接层使用随机失活(Dropout)机制以防止过拟合，并通过线性变换对卷积神经网络层提取的域名空间特征和长短期记忆神经网络层提取的域名序列特征进行整合和抽象，最终输出域名的深度特征向量。优选的，随机失活机制的丢弃率的设置范围为0.45到0.55。尤其优选，随机失活机制的丢弃率设为0.5。全连接层含有一个或者两个隐藏层。隐藏层的节点个数的设置范围为128～156。尤其优选，隐藏层的节点个数为128。输出层的节点个数的设置范围为90到99。尤其优选，输出层的节点个数为96。

[0108] 应当注意的是，上述实施例的深度神经网络模型的结构仅是一个最优结构，还存在其他可以适用的结构，本发明对此不作任何限制。

[0109] 图2示出利用上述训练方法获得的模型对DGA型僵尸网络进行检测的检测方法的一个实施例，包括：

[0110] 步骤B1：对所有待检测网络中的域名进行预处理得到以数值向量表示的域名。

[0111] 根据本发明的一个实施例，步骤B1包括：

[0112] B11、根据筛选条件对待分析的域名进行筛选，保留符合筛选条件的域名；

[0113] B12、将所属主机相同的域名分到同一个待检测网络；

[0114] B13、对所有待检测网络中的域名进行预处理，包括：

[0115] 建立域名字符与数字的映射关系，将域名的字符按照映射关系转化成数值向量，和

[0116] 将域名的数值向量的长度统一为第一预设长度，得到以数值向量表示的域名。步骤B1中对域名的预处理的过程和步骤A2中对域名的预处理的过程相同，此处不再赘述。

[0117] 优选的，筛选条件包括：域名必须由合法字符组成、域名是二级域名或三级动态域名、域名的随机标签长度大于第二预设长度、域名在一天之内不被同一个主机重复查询。

[0118] 设置筛选条件：域名必须由合法字符组成的原因是，DGA域名被用做备用的C&C域名，故需要满足域名注册条件，因此必须由合法字符组成。按照前面给出的一个示例，合法字符例如包括英文字母(A-Z,a-z)、数字(0-9)、连接符(-)、点(.)和下划线(_)。

[0119] 设置筛选条件:域名是二级域名或三级动态域名的原因是,DGA域名不需要多余的层级并且由于动态域名注册方便、受到的监管也较少,某些DGA家族生成动态域名。

[0120] 设置筛选条件:域名的随机标签长度大于第二预设长度的原因是,大量的短域名已经被其他机构注册了,为了保证DGA域名是未被注册的域名,DGA生成的随机标签一般较长。

[0121] 设置筛选条件:域名在一天之内不被同一个主机重复查询的原因是,僵尸主机在查询DGA域名时,不会在短时间内的重复查询,因为这样做不仅没有意义而且容易引起安全人员的警惕。

[0122] 经过上述筛选条件筛选后,有助于让本发明更高效、准确地检测出DGA型僵尸网络。

[0123] 随机标签是指:DGA域名中伪随机算法所生成的字符串。如DGA域名woefdnvcognsdnvohfe.com的随机标签为woefdnvcognsdnvohfe,其长度为19。

[0124] 所属主机是指域名的所属主机,即,在被检测的DNS流量中,对该域名发起了DNS查询请求的主机组成的集合。根据所属主机按如下规则进行待检测网络划分:对于域名a和域名b,设它们对应的所属主机分别为主机A和主机B,若A=B,则域名a和域名b被划分到相同的检测网络中,若A≠B,则域名a和域名b被划分到不同的待检测网络中。

[0125] 步骤B2:将进行预处理后的待检测网络的域名输入根据前述实施例的方法得到的深度神经网络模型,提取每个域名的域名深度特征向量。

[0126] 由于在训练时,是采用三元组形式的训练样本将其中的三个域名作为一个训练单元输入深度神经网络模型提取三个域名的域名深度特征向量。因此,在提取待检测网络的域名对应的域名深度特征向量时,也是以三元组的形式输入的。即,预处理后的待检测网络的域名是以三元组的形式输入深度神经网络模型。该三元组的锚样本设为预处理后的待检测网络的域名,正样本和负样本设为零。即,正样本和负样本的矩阵中的元素全为0。最终,将该三元组的锚样本对应的域名深度特征向量作为域名对应的域名深度特征向量。

[0127] 步骤B3:基于提取到的每个域名的域名深度特征向量,使用聚类算法根据域名之间的距离对每个待检测网络内的域名进行聚类,以确定所述待检测网络是否是DGA型僵尸网络。优选的,在聚类所形成的类簇中存在某个类簇包含域名的数量大于预设数量阈值时,则确定该类簇所在的待检测网络是DGA型僵尸网络,其中,域名之间的距离设为域名对应的深度特征向量之间的欧式距离。

[0128] 优选的,聚类算法是不需要指定聚类类别数的基于划分的聚类算法、基于层次的聚类算法和基于密度的聚类算法。

[0129] 对于基于划分的聚类算法,其主要思想是:给定聚类类别数K,首先创建一个初始划分,然后通过某种迭代方法,寻求全局最优划分。代表性的算法有k-means、X-means、k-medoids、k-modes、k-medians等。划分法一般需要指定K值,然而实际聚类时并不能预知K值,所以本发明选择能够通过BIC分数自决定K值的X-means。BIC是指贝叶斯信息准则(Bayesian Information Criterion)。K值通常称为:预先定义的聚类类别数、类簇数量。

[0130] 对于基于层次的聚类算法,其主要思想是:对给定数据集进行层次合并或分裂,直到达到某个终止条件而结束。代表性的算法有BIRCH算法、CURE算法、CHAMELEON算法等。

[0131] 对于基于密度的聚类算法。其主要思想是:通过数据点的密度分布进行聚类,克服

了基于距离的算法只能发现“类圆形”的聚类的缺点。代表性的算法有DBSCAN算法、OPTICS算法、DENCLUE算法。

[0132] 尤其优选的，聚类算法是X-means算法、DBSCAN算法或者BIRCH算法。这三种聚类算法都可以在无需设置类簇数量的情况下对域名进行聚类。

[0133] 其中，X-means算法是指基于划分的聚类算法，简称划分法。优选的，X-means算法设定的类簇数量范围的最大值的设置范围为15到25。尤其优选，X-means算法设定的类簇数量范围的最大值为20。即，虽然不设置具体的类簇数量，但是设置一个最大的类簇数量的限制，如20，则生成的类簇最终为20个及以下。

[0134] DBSCAN算法(Density-Based Spatial Clustering of Applications with Noise)是指基于密度的带噪空间聚类算法。优选的，DBSCAN算法的参数可以设置为：扫描半径eps＝1.5到2之间、最小包含点数minPts＝5到10之间。

[0135] BIRCH算法(Balanced Iterative Reducing and Clustering using Hierarchies)是指基于层次结构的平衡迭代聚类算法。优选的，BIRCH算法的参数可以设置为：叶节点每个CF的最大样本半径阈值threshold的取值范围为：0.4到0.6之间、CF Tree内部节点的最大CF数branching_factor的取值范围为：50到70之间。

[0136] 优选的，预设数量阈值的设置范围为8～30。尤其优选，预设数量阈值设为10。

[0137] 下面通过具体的评价指标来说明本发明的方法和现有方法的效果对比。

[0138] 先大致介绍下将要对比的两种现有方法：

[0139] 现有方法1：

[0140] 现有方法1是Zou等人提出的一种通过提取人工特征来检测僵尸网络的方法，该方法共提取出8个域名特征，记为人工特征M1，其描述见表1。

[0141] 表1

[0142]

类型	人工特征M1的描述
结构特征	域名长度
	域名标签数量
随机标签特征	随机标签所在层次
	随机标签长度
	随机标签所含的不同的字母数量
	随机标签所含的不同的数字数量
	随机标签是否含连字符
	随机标签不同字符比例

[0143] 现有方法2：

[0144] 现有方法2是Antonakakis等人提出的另一种通过提取人工特征来检测僵尸网络的方法，该方法将域名分组，提取组间相似特征，为了保证可比较性，我们假设分组大小为1，即单个域名为一组，由此获得18个域名特征，记为人工特征M2。

[0145] 表2

[0146]

类型	人工特征M2的描述
n-gram特征	域名1-gram概率分布的中位数 域名1-gram概率分布的均值 域名1-gram概率分布的标准差 域名2-gram概率分布的中位数 域名2-gram概率分布的均值

[0147]

	域名2-gram概率分布的标准差 域名3-gram概率分布的中位数 域名3-gram概率分布的均值 域名3-gram概率分布的标准差 域名4-gram概率分布的中位数 域名4-gram概率分布的均值 域名4-gram概率分布的标准差
熵值特征	域名的2LDs的熵值 域名的3LDs的熵值 域名的熵值
结构特征	域名长度 域名所含的不同的字符数量 域名层级数

[0148] 对于上述两种现有方法的更多的信息以及它们的工作原理,可以参照例如下面的技术文献,其通过引用合并于此,犹如明确地阐述:

[0149] [1]Zou F,Li L,Wu Y,et al.Detecting Doma in-Flux Malware Using DNS Failure Traffic[J].International Journal of Software Engineering and Knowledge Engineering,2018,28(02):151-173.

[0150] [2]Antonakakis M,Perdisci R.From throw-away traffic to bots:detecting the rise of DGA-based malware[C]//Usenix Conference on Security Symposium.USA:Usenix,2012.

[0151] 本示例中,进行效果对比时所采用的聚类算法为通过BIC分数自决定K值的X-means算法、BIRCH算法和DBSCAN算法。

[0152] 评估流程及评估结果如下:

[0153] 评估在测试集上进行,首先对测试集中每个域名提取3种域名特征:域名深度特征向量(本发明)、人工特征M1(现有方法1)和人工特征M2(现有方法2),基于域名特征可以定义域名间距离:两个域名的距离为它们的特征向量的欧式距离,于是域名被映射到3个不同距离空间中,使用3种聚类算法:X-means,BRICH和DBSCAN,对每个距离空间中的域名聚类。因此,基于9种(特征,算法)组合可获得9种聚类结果。最好的聚类结果为:34个DGA家族生成

的域名分别包含在34个类簇中并且所有良性NXDomain都不与其他域名同属一个类簇。

[0154] 由于可以获得最佳聚类,则可通过外部方法评估聚类效果。选择以下3个评价指标衡量聚类效果:均一性和完整性的加权平均V-measure、调整兰德系数(Adjusted Rand Index)ARI和调整互信息评分(Adjusted Mutual Information)AMI,每个指标都通过调节算法参数获得最优值。

[0155] V-measure是对聚类结果的均一性和完整性的加权平均。其中,均一性是指一个簇中只包含一个类别的样本,完整性是指同类别样本被归类到相同簇中。V-measure的取值范围为[0,1],值越大,聚类效果越佳。基于V-measure评价指标的评价结果如表3所示:

[0156] 表3

[0157]

	X-means	BRICH	DBSCAN
域名深度特征向量	0.8478	0.8166	0.7872
人工特征M1	0.5434	0.5432	0.5297
人工特征M2	0.4531	0.4712	0.4647

[0158] 从表3可以观察到,域名深度特征向量和人工特征M1通过与X-means算法组合、人工特征M2通过与BRICH算法组合取得了最大V-measure值,在使用最佳聚类算法的条件下,域名深度特征向量聚类的V-measure值比人工特征M1聚类高出56.0%,比人工特征M2聚类高出87.1%。

[0159] ARI衡量聚类结果和真实情况的吻合程度,ARI的取值范围为[-1,1],值越大,聚类效果越佳。基于ARI评价指标的评价结果如表4所示:

[0160] 表4

[0161]

	X-means	BRICH	DBSCAN
域名深度特征向量	0.6921	0.6639	0.5260
人工特征M1	0.2549	0.2193	0.1318
人工特征M2	0.1622	0.1536	0.1227

[0162] 从表4可以观察到,域名深度特征向量、人工特征M1、M2都通过与X-means算法组合取得了各自的最大ARI值,在使用最佳聚类算法的条件下,域名深度特征向量聚类的ARI值比人工特征M1聚类高出171.5%,比人工特征M2聚类高出326.7%。

[0163] AMI基于互信息的方法衡量聚类效果,取值范围为[-1,1],值越大,聚类效果越佳。基于AMI评价指标的评价结果如表5所示:

[0164] 表5

[0165]

	X-means	BRICH	DBSCAN
域名深度特征向量	0.8198	0.7688	0.7610
人工特征M1	0.5176	0.5178	0.4115
人工特征M2	0.4193	0.4347	0.3766

[0166] 从表5可以观察到,域名深度特征向量通过与X-means算法组合、人工特征通过与BRICH算法组合取得了最大AMI值,在使用最佳聚类算法的条件下,域名深度特征向量聚类的AMI值比人工特征M1聚类高出58.3%,比人工特征M2聚类高出88.6%。

[0167] 通过使用评价指标V-measure、ARI和AMI对聚类效果进行量化评估,可见,基于本

发明的域名深度特征向量聚类的聚类效果优于基于人工特征聚类的聚类效果。

[0168] 根据本发明的一个实施例，提供一种电子设备，包括：一个或多个处理器；以及存储器，其中存储器用于存储一个或多个可执行指令；所述一个或多个处理器被配置为经由执行所述一个或多个可执行指令以实现前述实施例所述的用于辅助检测DGA型僵尸网络的模型训练方法和/或DGA型僵尸网络的检测方法。

[0169] 需要说明的是，虽然上文按照特定顺序描述了各个步骤，但是并不意味着必须按照上述特定顺序来执行各个步骤，实际上，这些步骤中的一些可以并发执行，甚至改变顺序，只要能够实现所需要的功能即可。

[0170] 本发明可以是系统、方法和/或计算机程序产品。计算机程序产品可以包括计算机可读存储介质，其上载有用于使处理器实现本发明的各个方面的计算机可读程序指令。

[0171] 计算机可读存储介质可以是保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以包括但不限于电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式压缩盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。

[0172] 以上已经描述了本发明的各实施例，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实施例的原理、实际应用或对市场中的技术改进，或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

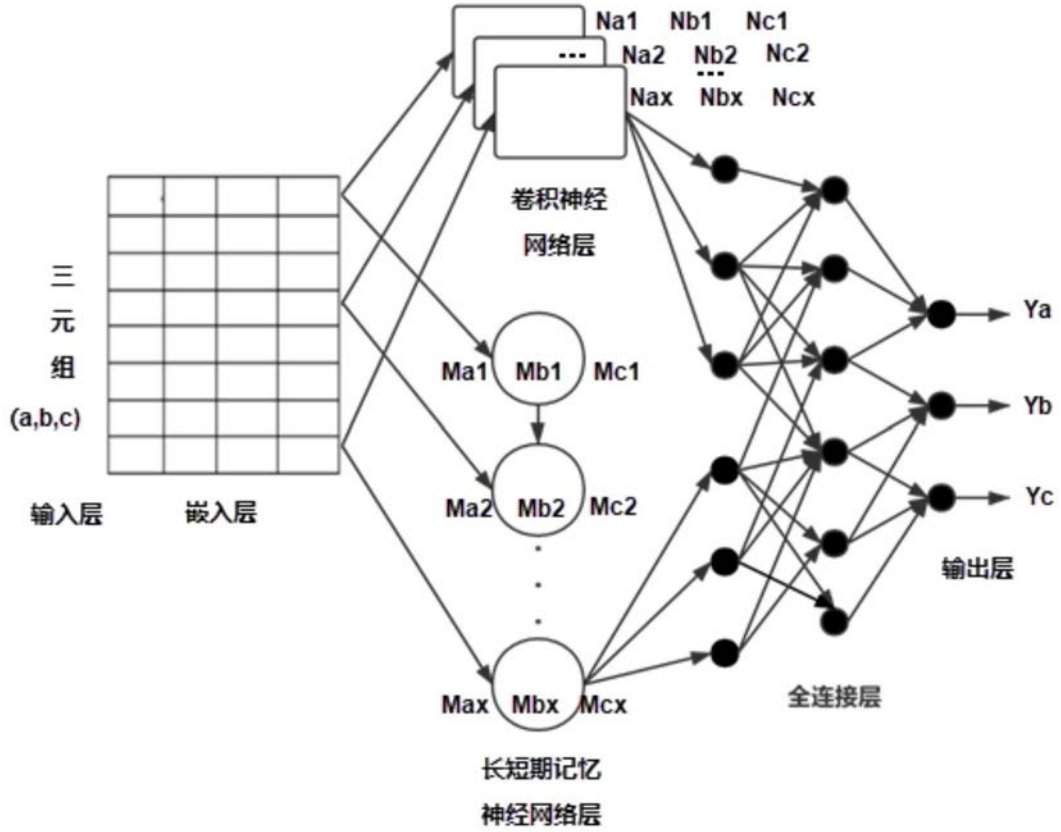

Na1 Nb1 Nc1
Na2 Nb2 Nc2
Nax Nbx Ncx
卷积神经
网络层
三
元
组
(a,b,c)
输入层
嵌入层
Ma1 Mb1 Mc1
Ma2 Mb2 Mc2
Max Mbx Mcx
长短期记忆
神经网络层
全连接层
输出层
Ya
Yb
Yc

图1

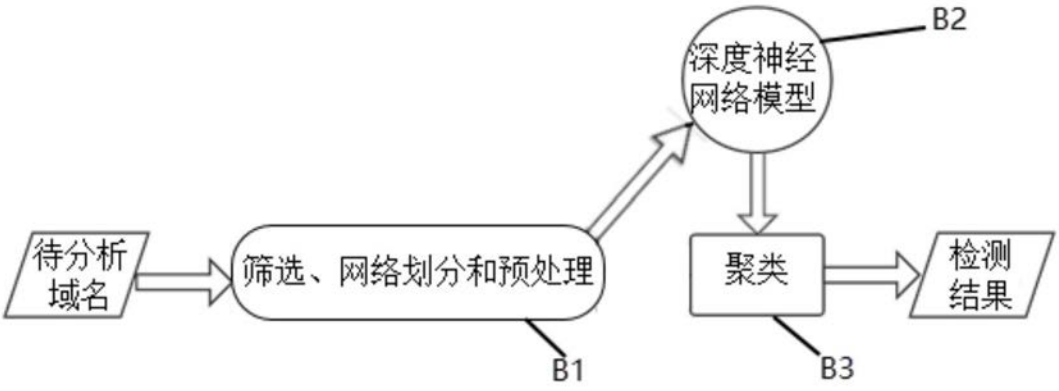

B2
深度神经
网络模型
待分析
域名
筛选、网络划分和预处理
聚类
检测
结果
B1
B3

图2