(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118540072 A
(43)申请公布日 2024.08.23

(21)申请号 202310140407.3

(22)申请日 2023.02.21

(71)申请人 中国科学院计算机网络信息中心
地址 100190 北京市海淀区中关村南四街4号院内2号楼

(72)发明人 魏金侠 龙春 付豪 宫良一 李婧 杨帆

(74)专利代理机构 北京知舟专利事务所(普通合伙) 11550
专利代理师 周玉玲

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 61/4511(2022.01)
G06F 18/24(2023.01)
G06N 3/0464(2023.01)
G06N 3/048(2023.01)
G06N 3/08(2023.01)

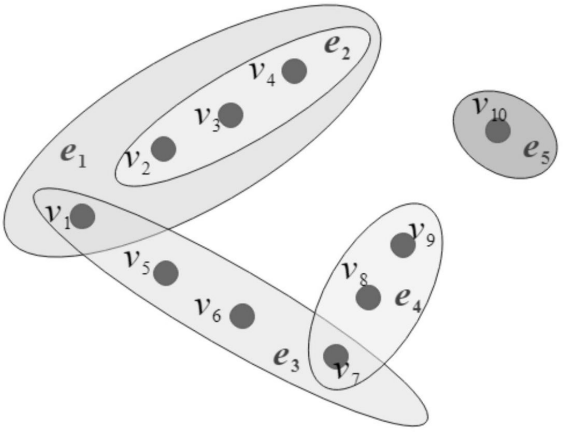
权利要求书2页 说明书7页 附图2页

(54)发明名称

基于动态超图学习的恶意域名检测方法

(57)摘要

本发明涉及网络安全技术领域，为提高恶意域名检测结果的准确性，提供了一种基于动态超图学习的恶意域名检测方法，采集包括恶意域名与正常域名的域名样本集；为域名样本集中每个域名样本提取特征向量；采用决策树对域名样本进行分类，相同类别的域名样本具有相同的特征属性；将域名样本作为顶点，并将相同类别的顶点连接以形成超边，从而构建出超图；结合超图与域名-IP强关联关系图对动态超图神经网络进行训练；将待测域名输入训练完成后的动态超图神经网络进行分类识别。本发明结合超图与域名-IP强关联关系图对动态超图对特征进行增强，可以将相关联的域和IP进行全面刻画，能够有效提高检测结果的准确性。



CN 118540072 A

1.一种基于动态超图学习的恶意域名检测方法,其特征在于,包括以下步骤:

采集包括恶意域名与正常域名的域名样本集;

为域名样本集中每个域名样本提取特征向量;

采用决策树对域名样本进行分类,相同类别的域名样本具有相同的特征属性;

将域名样本作为顶点,并将相同类别的顶点连接以形成超边,从而构建出超图;

结合超图与域名-IP强关联关系图对动态超图神经网络进行训练;

将待测域名输入训练完成后的动态超图神经网络进行分类识别。

2.根据权利要求1所述的基于动态超图学习的恶意域名检测方法,其特征在于,在训练过程中不断地采集真实网络环境中新出现的域名样本,并根据新出现的域名样本对超图进行重构,使动态超图神经网络能够随着网络环境的变化进行更新。

3.根据权利要求1所述的基于动态超图学习的恶意域名检测方法,其特征在于,所述域名-IP强关联关系图按如下方式建立:设立至少两项关联规则,分别根据每项关联规则构建出相应的域名-IP弱关联关系图;将各个域名-IP弱关联关系图结合到一起形成域名-IP强关联关系图。

4.根据权利要求3所述的基于动态超图学习的恶意域名检测方法,其特征在于,设置以下三项关联规则:

1)、两个域名共享IP来自至少两个托管服务提供商;

2)、两个域名共享至少一个专用IP;

3)、两个域名属于同一个专用顶级域名或共享来自不同托管服务提供商的公共IP。

5.根据权利要求1所述的基于动态超图学习的恶意域名检测方法,其特征在于,所述特征向量中包括空间特征、时间特征与文本特征。

6.根据权利要求5所述的基于动态超图学习的恶意域名检测方法,其特征在于,空间特征包括A记录、TTL值、IP与响应包大小。

7.根据权利要求5所述的基于动态超图学习的恶意域名检测方法,其特征在于,时间特征包括应答包中的请求响应时间差、主机连接目标IP的回连时长、与访问时间分布。

8.根据权利要求5所述的基于动态超图学习的恶意域名检测方法,其特征在于,文本特征包括域名长度、域名中数字占比、域名中最长的连续数字的长度与最长连续数字序列的偏移值。

9.根据权利要求1所述的基于动态超图学习的恶意域名检测方法,其特征在于,结合超图与域名-IP强关联关系图对动态超图神经网络进行训练,包括如下步骤:在动态超图神经网络的卷积层利用超图的表示矩阵对域名-IP强关联关系图的编码特征进行卷积变换,使得超图中各顶点的特征向量得到增强;将增强后的特征向量输入到动态超图神经网络进行分类识别。

10.根据权利要求9所述的基于动态超图学习的恶意域名检测方法,其特征在于,卷积变换的公式如下:

$$X^{(l+1)}=s\left(D_v^{-1/2}HWD_e^{-1}H^TD_v^{-1/2}X^{(l)}Q^{(l)}\right)$$

式中,s表示非线性激活函数;$D_v^{-1/2}$表示超边度矩阵的对角矩阵的求逆分解;H表示超图

的邻接矩阵;W表示用于记录超图中各条超边权重的对角矩阵;D_e^{-1}表示超图顶点度矩阵的对角矩阵的逆矩阵;$X^{(1)}$表示第1层卷积神经网络的嵌入量;$Q^{(1)}$表示网络参数。

基于动态超图学习的恶意域名检测方法

技术领域

[0001] 本发明涉及网络安全技术领域,具体涉及一种基于动态超图学习的恶意域名检测方法。

背景技术

[0002] 在早期的僵尸网络中,控制者通常会把C&C服务器的域名或者IP地址硬编码到恶意程序中,僵尸主机通过这些信息定时访问C&C主机获取命令。但同时安全人员也能够通过逆向恶意程序,得到C&C服务器的域名或者IP,利用这些信息定位C&C主机,安全人员就可以隔断C&C主机从而破坏僵尸网络。不少控制者为了保护C&C主机,使用Fast-flux技术来提高C&C服务器的健壮性。Fast-flux技术是指不断改变域名和IP地址映射关系的一种技术,也就是说在短时间内查询使用Fast-flux技术部署的域名,会得到不同的结果。

[0003] 结合了Fast-flux技术的僵尸网络对恶意域名的检测来说是关乎网络安全的新一轮挑战。面临的主要困境如下:

[0004] 1)基于规则、传统的访问特征的机器学习算法存在明显的不足:通常需要黑名单才能完成检测;单纯利用单个僵尸主机行为相似性的方法容易出现误判;无法区分Fast Flux与CDN正常访问。

[0005] 2)恶意域名检测模型在处理新的恶意域名类型时的模型更新问题:在真实的应用环境中,Fast-Flux僵尸网络和网络系统是随着实际网络环境不断变化的,因此非更新的恶意域名检测模型难以很好适应实时产生的恶意域名的检测场景。

[0006] 3)现有检测模型需要对数据进行复杂处理和特征提取,并且需要借助大量第三方数据源,如查询Whois信息、IP对应的自治系统号等,影响系统的实时性,难以应用于实际的恶意域名检测,导致检测的实时性较差,并且受网络环境波动影响较大,导致检测结果的稳定性不好。

发明内容

[0007] 本发明的目的在于解决上述现有技术中存在的难题,提供一种基于动态超图学习的恶意域名检测方法,提高检测结果的准确性。

[0008] 本发明是通过以下技术方案实现的:

[0009] 一种基于动态超图学习的恶意域名检测方法,包括以下步骤:

[0010] 采集包括恶意域名与正常域名的域名样本集;

[0011] 为域名样本集中每个域名样本提取特征向量;

[0012] 采用决策树对域名样本进行分类,相同类别的域名样本具有相同的特征属性;

[0013] 将域名样本作为顶点,并将相同类别的顶点连接以形成超边,从而构建出超图;

[0014] 结合超图与域名-IP强关联关系图对动态超图神经网络进行训练;

[0015] 将待测域名输入训练完成后的动态超图神经网络进行分类识别。

[0016] 进一步的,在训练过程中不断地采集真实网络环境中新出现的域名样本,并根据

新出现的域名样本对超图进行重构,使动态超图神经网络能够随着网络环境的变化进行更新。

[0017] 进一步的,所述域名-IP强关联关系图按如下方式建立:设立至少两项关联规则,分别根据每项关联规则构建出相应的域名-IP弱关联关系图;将各个域名-IP弱关联关系图结合到一起形成域名-IP强关联关系图。

[0018] 进一步的,设置以下三项关联规则:

[0019] 1)、两个域名共享IP来自至少两个托管服务提供商;

[0020] 2)、两个域名共享至少一个专用IP;

[0021] 3)、两个域名属于同一个专用顶级域名或共享来自不同托管服务提供商的公共IP。

[0022] 进一步的,所述特征向量中包括空间特征、时间特征与文本特征。

[0023] 进一步的,空间特征包括A记录、TTL值、IP与响应包大小。

[0024] 进一步的,时间特征包括应答包中的请求响应时间差、主机连接目标IP的回连时长、与访问时间分布。

[0025] 进一步的,文本特征包括域名长度、域名中数字占比、域名中最长的连续数字的长度与最长连续数字序列的偏移值。

[0026] 进一步的,结合超图与域名-IP强关联关系图对动态超图神经网络进行训练,包括如下步骤:在动态超图神经网络的卷积层利用超图的表示矩阵对域名-IP强关联关系图的编码特征进行卷积变换,使得超图中各顶点的特征向量得到增强;将增强后的特征向量输入到动态超图神经网络进行分类识别。

[0027] 进一步的,卷积变换的公式如下:

[0028] $$X^{(l+1)}=s\left(D_v^{-1/2}HWD_e^{-1}H^TD_v^{-1/2}X^{(l)}Q^{(l)}\right)$$

[0029] 式中,s表示非线性激活函数;$D_v^{-1/2}$表示超边度矩阵的对角矩阵的求逆分解;H表示超图的邻接矩阵;W表示用于记录超图中各条超边权重的对角矩阵;D_e^{-1}表示超图顶点度矩阵的对角矩阵的逆矩阵;$X^{(1)}$表示第l层卷积神经网络的嵌入量;$Q^{(1)}$表示网络参数。

[0030] 与现有技术相比,本发明的有益效果包括:

[0031] 1、现有技术单纯利用僵尸主机行为相似性的方法较为片面,容易出现误判。本发明结合超图与域名-IP强关联关系图对动态超图对特征进行增强,超图可以将域名流量之间的高阶关系清晰表达出来,而域名-IP关系图可以将域名及IP之间的关系进行深层次挖掘,这样两者结合可以将相关联的域和IP进行全面刻画,能够有效提高检测结果的准确性。

[0032] 2、利用空间、时间、文本信息三个维度的特征来构建超图结构,通过超图结构把具有关联关系的域名划分到一个超边区域内,呈现了域名之间的空间全局关联关系。

[0033] 3、在训练过程中不断地采集真实网络环境中新出现的域名样本,并根据新出现的域名样本对超图进行重构,使动态超图神经网络能够随着网络环境的变化进行更新,从而能够很好适应实时产生的恶意域名的检测场景。

[0034] 4、根据本发明所提出的三项关联规则建立域名-IP强关联关系图,就能通过分析新输入域名与某些恶意域名是否具有相同专用IP或者相关顶级域名来分析新输入域名是否为恶意的。

附图说明

[0035] 图1为超图的形态示意图。

[0036] 图2为域名、IP与托管服务提供商的映射图；

[0037] 图3为根据第一项关联规则得到的域名-IP弱关联关系图；

[0038] 图4为根据第二项关联规则得到的域名-IP弱关联关系图；

[0039] 图5为根据第三项关联规则得到的域名-IP弱关联关系图；

[0040] 图6为结合弱关联关系图得到的域名-IP强关联关系图。

具体实施方式

[0041] 下面结合附图对本发明作进一步详细描述：

[0042] 一种基于动态超图学习的恶意域名检测方法，包括以下步骤：

[0043] 采集包括恶意域名与正常域名的域名样本集；

[0044] 为域名样本集中每个域名样本提取特征向量；

[0045] 采用决策树对域名样本进行分类，相同类别的域名样本具有相同的特征属性；

[0046] 将域名样本作为顶点，并将相同类别的顶点连接以形成超边，从而构建出超图；

[0047] 结合超图与域名-IP强关联关系图对动态超图神经网络进行训练；

[0048] 将待测域名输入训练完成后的动态超图神经网络进行分类识别。

[0049] 一)、提取域名样本的特征向量

[0050] 考虑进行恶意域名分析时特征表示的全面性，本发明从空间、时间、文本信息三个维度来综合分析。

[0051] 空间特征包括A记录、TTL值、IP、响应包大小等，时间特征包括应答包中的请求时间与响应时差(请求响应时间)、主机连接目标IP的回连时长、访问时间分布等，文本信息主要是指域名本身的内容。

[0052] A.空间特征是从域名流量的请求和应答包中提取。空间特征中的A记录在Fast-Flux恶意域名解析过程中大多分布在数量较多的区域，而CDN域名的分布则集中在数量较少的区域。这是因为CDN域名会通过降低其TTL值来动态改变域名解析得到的IP地址，因此，对于Fast-Flux恶意域名和CDN域名来说A记录数量分布差异比较明显；TTL值在正常域名中分布较平均，而Fast-Flux恶意域名的TTL值集中分布在数值较低的区域；Fast-Flux恶意域名解析结果中存在大量A记录，其响应包较大，而正常域名响应包所包含的信息一般较少，其响应包较小。

[0053] B.时间特征是从域名流量中主机连接域名应答包中解析IP的时长计算得出的。在时间特征方面，正常域名会在一段时间内被多次访问，一般缓存在本地DNS服务器上。但是Fast-Flux恶意域名只会被僵尸主机访问，在进行地址解析时，一旦本地没有缓存，大概率需进行迭代查询，导致DNS请求响应时间较长。同时，主机连接目标IP的回连时长在正常解析情况下时长稳定，不会出现大的波动，但是对于fast-Flux恶意域名来说，时长大小分布不均。

[0054] 通过分析真实DNS流量发现，Fast-flux域名在大部分时间极少被访问，只是在特定时间被集中访问，因此访问时间分布这项特征能够明显区分Fast-flux域名被访问的情况以及CDN正常域名被访问情况。访问时间分布是根据对流量数据的统计得出来的，比如收

集一定时间段的域名流量,然后分析该周期内Fast-flux域名被访问的情况以及CDN正常域名被访问情况

[0055] C.文本信息主要指域名本身不用计算和统计的字符信息,对于一个域名来说,文本特侦包括域名的长度,域名中的数字占比,域名中最长的连续数字的长度,最长连续数字序列的偏移值。

[0056] 二)、构建超图

[0057] 对于一个简单图,其每条边均与两个顶点相关联,即每条边的度被限制为2,而超图则允许每一条边的度为任何非负整数。

[0058] 超图的数学定义可以表述为,超图是一个三元组G=<V,E,W>,其中V表示顶点集合,E表示超边集合,W表示记录各条超边权重的对角矩阵。可以用邻接矩阵H来表述一个超图,H是一个|VgE|的矩阵,表示方式定义为:

[0059] $$h(v,e)=\begin{cases}1, & v\in e\\ 0, & v\notin e\end{cases}$$

[0060] 其中h表示矩阵H的元素,v∈V,e∈E,参考图1中的10个顶点v构成了集合V,5条超边e构成了集合E。

[0061] 令d(v)和δ(e)分别表示顶点的度和超边的度,$d(v)=\sum_{e\in E}w(e)gh(v,e)$,$\delta(e)=\sum_{v\in V}h(v,e)$。$D_e$和$D_v$分别表示超图顶点度矩阵和超边度矩阵的对角矩阵。

[0062] 超图的顶点(超边)分类问题的学习目标函数:

[0063] $$\arg\min_{g}\{R_{emp}(g)+\Omega(g)\}$$

[0064] 其中g(g)为分类函数,形成超图的分类函数为决策树,Ω(g)为标准化损失函数,$R_{emf}(g)$为有监督的经验误差,标准化损失函数的计算方法:

[0065] $$W(g)=\frac{1}{2}\sum_{e\hat{I}E}\sum_{\{u,v\}\hat{I}V}\frac{w(e)h(u,e)h(v,e)}{d(e)}\left(\frac{g(u)}{\sqrt{d(u)}}-\frac{g(v)}{\sqrt{d(v)}}\right)^2$$

[0066] 为了呈现域名之间的空间全局关联关系,利用空间、时间、文本信息三个维度来构建超图结构,通过超图结构把具有关联关系的域名划分到一个超边区域内。在超图算法中,超边构建的好坏直接影响到模型的整体检测效果。

[0067] 本发明利用域名的空间、时间、文本信息三个维度来构建超图结构,其中域名空间特征包括A记录、TTL值、IP、响应包大小等,时间特征包括应答包中的请求时间与响应时差(请求响应时间)、主机连接目标IP的回连时长、访问时间分布等,文本信息主要是指域名本身的内容。大多是数量特征或者类别特征,比较适合决策树的分类方法。

[0068] 以28万条域名样本为例,超图构建过程分为如下4个阶段。

[0069] 阶段1:针对选取的28万条域名样本进行空间特征提取操作,提取39维域名空间统计特征,$N_p=\{x_{p,1},x_{p,2},L,x_{p,39}\}$为一条域名样本特征向量,其中p表示集合中域名样本的数量;

[0070] 阶段2:从样本中选取1万条数据作为训练样本对决策树模型进行训练,得到最优参数组合的决策数据分类模型;

[0071] 阶段3:将其余27万条测试样本输入决策树,根据每一个叶节点的预测结果将样本

分成不同的类别,然后根据样本划分类别形成超边集E,决策树算法分到同一个类别里的样本形成顶点集合V。

[0072] 阶段4:计算超图的邻接矩阵H,超图顶点度矩阵的对角矩阵和超边度矩阵的对角矩阵D_e和D_v。

[0073] 为了进一步强化域名特征,完整的表示出域名之间全局关系,结合超图与域名-IP强关联关系图对动态超图神经网络进行训练。超图可以将域名流量之间的高阶关系清晰表达出来,而域名-IP关系图可以将域名及IP之间的关系进行深层次挖掘,这样两者结合可以将相关联的域和IP进行全局刻画。

[0074] 三)、构建域名-IP强关联关系图

[0075] 基于随机森林设计IP分类器和域名分类器,其中IP分类器将IP标记为专用IP和公共IP,专用IP用于网络内部以及本地网络,用于局域网;公共IP面向用户,用户可以通过Internet访问,域名分类器根据顶级域名将域名分为专用域名和公共域名。

[0076] 参考图2所示,一个IP地址可以对应多个域名,两个或多个域名的IP地址可能来自不同的托管服务提供商也可能来自一个托管服务提供商。图中菱形D1、D2、D3、D4表示专用域名、椭圆形D5、D6、D7、D8表示公共域名;六边形IP1、IP2、IP3、IP4、IP5、IP6表示专用IP;长方形IP7、IP8、IP9表示公共IP;Hosting表示托管服务提供商;Apex表示顶级域名。

[0077] 域名-IP强关联关系图按如下方式建立:设立至少两项关联规则,分别根据每项关联规则构建出相应的域名-IP弱关联关系图;将各个域名-IP弱关联关系图结合到一起形成域名-IP强关联关系图。这样原本存在关联的域名的关联关系更加强化,就可以通过新输入域名与已知恶意域名的相关性来推断新输入域名是否为恶意域名。

[0078] 本具体实施方式设置以下三项关联规则:

[0079] 1)、两个域名共享IP来自至少两个托管服务提供商;根据该项关联规则得到的域名-IP弱关联关系图参考图3所示。

[0080] 2)、两个域名共享至少一个专用IP;根据该项关联规则得到的域名-IP弱关联关系图参考图4所示。

[0081] 3)、两个域名属于同一个专用顶级域名或共享来自不同托管服务提供商的公共IP。根据该项关联规则得到的域名-IP弱关联关系图参考图5所示。

[0082] 结合图3至5图的域名-IP弱关联关系图得到的域名-IP强关联关系图参考图6所示,图6包含了图3至5图中的域名之间的全部关联关系。

[0083] 根据上述三项关联规则建立域名-IP强关联关系图,就能通过分析新输入域名与某些恶意域名是否具有相同专用IP或者相关顶级域名来分析新输入域名是否为恶意的。比如,某个新输入域名与某个恶意域名共享IP来自三个托管服务提供商、且属于同一个专用级域名、且共享多个专用IP,则这个新输入的域名大概率是恶意的,需要进一步分析其与恶意域名的相似性。

[0084] 四)、训练动态超图神经网络

[0085] 结合超图与域名-IP强关联关系图对动态超图神经网络进行训练:在动态超图神经网络的卷积层利用超图的表示矩阵对域名-IP强关联关系图的编码特征进行卷积变换,使得超图中各顶点的特征向量得到增强;将增强后的特征向量输入到动态超图神经网络进行分类识别。

[0086] 卷积变换的公式如下：

[0087] $$X^{(l+1)}=s\left(D_v^{-1/2}HWD_e^{-1}H^TD_v^{-1/2}X^{(l)}Q^{(l)}\right)$$

[0088] 式中，s表示非线性激活函数；$D_v^{-1/2}$表示超边度矩阵对角阵求逆的分解(D_v超边度矩阵的对角矩阵，矩阵分解可以理解为：比如A*A＝B，则A＝$B^{1/2}$)；H表示超图的邻接矩阵；W表示用于记录超图中各条超边权重的对角矩阵；D_e^{-1}表示超图顶点度矩阵对角阵的逆矩阵(D_e表示超图顶点度矩阵的对角矩阵)；$X^{(1)}$表示第1层卷积神经网络的嵌入量；$Q^{(1)}$表示网络参数。

[0089] 在训练过程中不断地采集真实网络环境中新出现的域名样本，并根据新出现的域名样本对超图进行重构，使动态超图神经网络能够随着网络环境的变化进行更新。重构的过程包括：提取新出现的域名样本的特征向量，然后采用决策树根据特征属性对新出现的域名进行分类，根据分类结果构建出新的超边。

[0090] 将待测域名输入训练完成后的动态超图神经网络进行分类识别，实现对fast-flux恶意域名的有效检测并发现与已检测出恶意域名相关的可疑域名，便于及时对相关域名及时处置。

[0091] 五)效果对比

[0092] 发明人分别将基于域名字符串统计特征实现恶意域名检测、基于DNS流量统计特征实现恶意域名检测以及基于关联关系实现恶意域名检测方法应用于中国科技网骨干网的恶意域名检测中，收集了从2022年1月到2022年7月的域名流量数据，从中识别出恶意的域名，经过实验分析得到相关结论：

[0093] 1)通过域名字符串统计特征实现恶意域名检测的方法只需要字符串就可以提取，易于实现，尤其是在DGA域名监测中效果好一些，但是这类特征比较简单，效果比较局限，采用该方法对本发明收集的域名流量数据进行检测，取得了87.45％的准确率和83.44％召回率。

[0094] 2)DNS流量统计特征包括解析内容、活动时间记录、TTL值等信息，这些特征在良性域名和恶意域名上存在较明显的差异，虽然利用庞大的DNS流量特征可以有效检测出恶意域名，但是往往容易忽略流量之间攻击行为之间的关系，采用该方法对本发明收集的域名流量数据进行检测，取得了90.36％的准确率和92.54％的召回率。

[0095] 3)基于关联关系的方法可以充分发掘域名之间关联性，能够通过这些关联发现更加高级隐蔽的恶意域名，这种关系是在攻击者实施攻击过程中就形成的，不容易被篡改，采用该方法对本发明收集的域名流量数据进行检测，取得86.58％的准确率和85.72％的召回率。

[0096] 经过分析，上述现有三类方法在准确率和召回率方面还有待于进一步提升的原因是不能够全面表示域名各个属性之间的高阶关系，无法达到多维指标的高效平衡。

[0097] 4)本发明提出一种基于动态超图学习的恶意域名检测方法，首先采用决策树对域名样本进行分类，相同类别的域名样本具有相同的特征属性；将域名样本作为顶点，并将相同类别的顶点连接以形成超边，从而构建出超图；结合超图与域名-IP强关联关系图对动态超图神经网络进行训练；将待测域名输入训练完成后的动态超图神经网络进行分类识别。将该方法应用于本发明收集的数据中实现恶意域名检测，取得98.29％的准确率和98.73％

的召回率。

[0098] 上述技术方案只是本发明的一种实施方式，对于本领域内的技术人员而言，在本发明公开了原理的基础上，很容易做出各种类型的改进或变形，而不仅限于本发明上述具体实施例所描述的技术方案，因此前面描述的只是优选的，而并不具有限制性的意义。

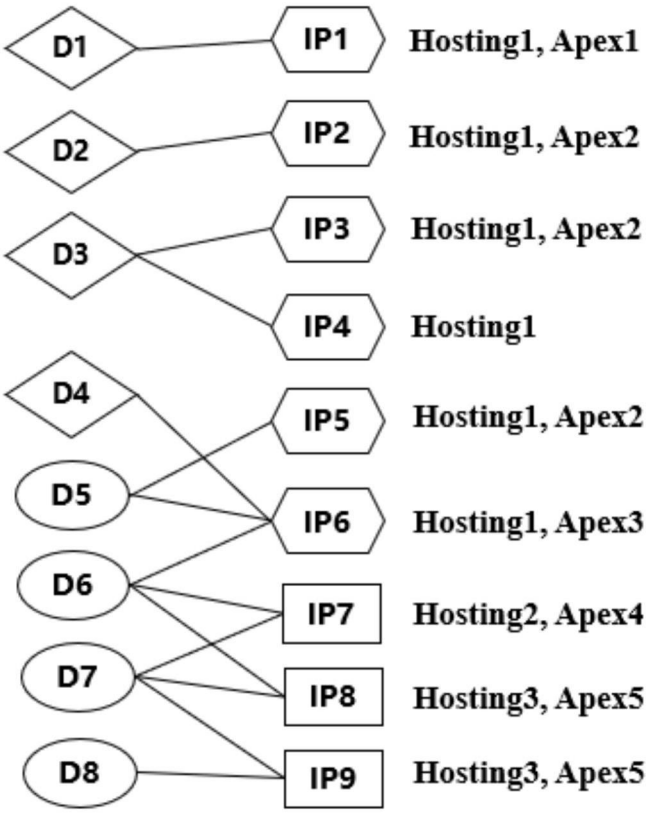

D1
D2
D3
D4
D5
D6
D7
D8
IP1
IP2
IP3
IP4
IP5
IP6
IP7
IP8
IP9
Hosting1, Apex1
Hosting1, Apex2
Hosting1, Apex2
Hosting1
Hosting1, Apex2
Hosting1, Apex3
Hosting2, Apex4
Hosting3, Apex5
Hosting3, Apex5

图1

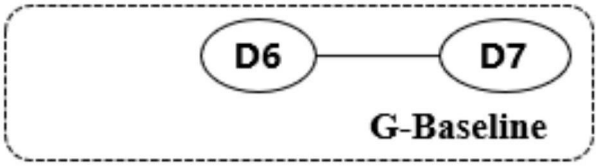

D6
D7
G-Baseline

图2

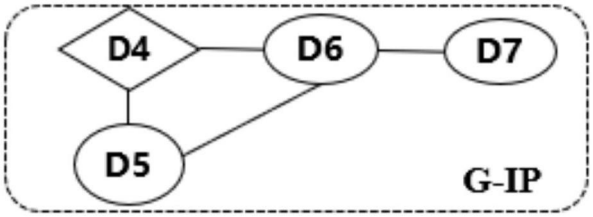

D4
D6
D7
D5
G-IP

图3

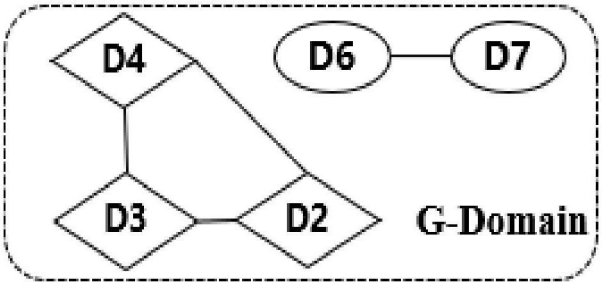

D4
D6
D7
D3
D2
G-Domain

图4

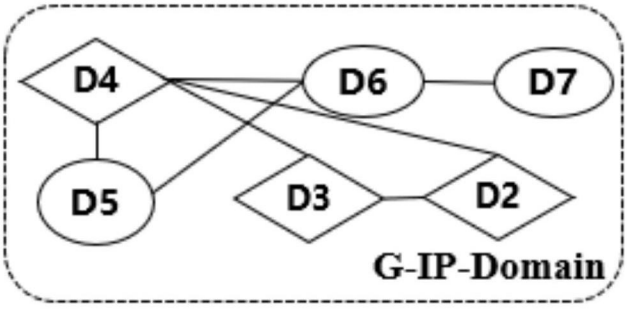

D4
D6
D7
D5
D3
D2
G-IP-Domain

图5

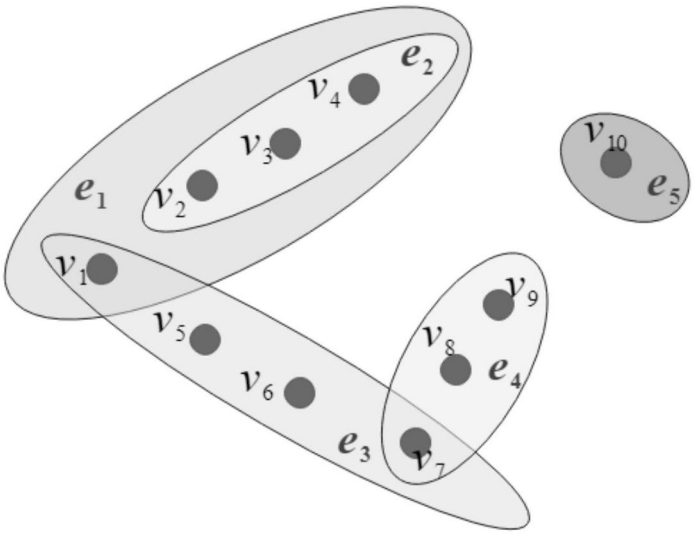

e_2
v_4
v_3
e_1
v_2
v_{10}
e_5
v_1
v_9
v_5
v_8
e_4
v_6
e_3
v_7

图6