(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 1 月 20 日 (20.01.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/011977 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2020/138820

(22) 国际申请日: 2020 年 12 月 24 日 (24.12.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010680957.0 2020年7月15日 (15.07.2020) CN

(71) 申请人: 中国科学院深圳先进技术研究院 (**SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY CHINESE ACADEMY OF SCIENCES**) [CN/CN]; 中国广东省深圳市南山区深圳大学城学苑大道 1068 号, Guangdong 518055 (CN)。

(72) 发明人: **叶可江 (YE, Kejiang)**; 中国广东省深圳市南山区深圳大学城学苑大道 1068 号, Guangdong 518055 (CN)。 **林鹏 (LIN, Peng)**; 中国广东省深圳市南山区深圳大学城学苑大道 1068 号, Guangdong 518055 (CN)。 **须成忠 (XU, Chengzhong)**; 中国广东省深圳市南山区深圳大学城学苑大道1068号, Guangdong 518055 (CN)。

(74) 代理人: 北京中巡通大知识产权代理有限公司 (**BEIJING ZHONG XUN TONG DA INTELLECTUAL PROPERTY AGENCY CO., LTD.**); 中国北京市海淀区杏石口路 50 号中间建筑 1 区 148 号, Beijing 100195 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) **Title:** NETWORK ANOMALY DETECTION METHOD AND SYSTEM, TERMINAL AND STORAGE MEDIUM

(54) **发明名称**: 一种网络异常检测方法、系统、终端以及存储介质

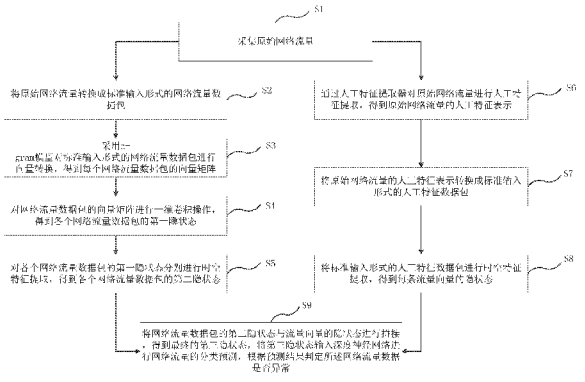

图1

S1 Acquire original network traffic
S2 Convert the original network traffic into network traffic data packets in a standard input form
S3 Perform vector conversion on the network traffic data packets in a standard input form by using an n-gram model, to obtain a vector matrix of each network traffic data packet
S4 Perform one-dimensional convolution operation on the vector matrices of the network traffic data packets, to obtain first hidden states of the network traffic data packets
S5 Perform spatial-temporal feature extraction on the first hidden states of the network traffic data packets, to obtain second hidden states of the network traffic data packets
S6 Perform artificial feature extraction on the original network traffic by means of an artificial feature extractor, to obtain artificial feature representation of the original network traffic
S7 Convert the artificial feature representation of the original network traffic into artificial feature data packets in a standard input form
S8 Perform spatial-temporal feature extraction on the artificial feature data packets in a standard input form, to obtain hidden states of traffic vectors
S9 Splice the second hidden states of the network traffic data packets and the hidden states of the traffic vectors, to obtain a final third hidden state, input the third hidden state to a deep neural network for classification and prediction of the network traffic, and determine, according to the prediction result, whether the network traffic data is anomalous

(57) **Abstract:** The present application relates to a network anomaly detection method and system, a terminal and a storage medium. Said method comprises: performing vector conversion on network traffic by using an n-gram model, to obtain a vector matrix of the network traffic; performing spatial-temporal feature extraction on the vector matrix of the network traffic by using a long short-term memory network and a bidirectional gated recurrent unit, to obtain a hidden state of the network traffic; extracting an artificial feature of the network traffic by using an artificial feature extractor, and performing spatial-temporal feature extraction on the artificial feature, to obtain a hidden state of the artificial feature; and splicing the hidden state of the network traffic and the hidden state of the artificial feature, then inputting same to a deep neural network for classification and prediction of the network traffic, and determining, according to the prediction result, whether the network traffic is anomalous. In the present application, a fused feature is used for modeling of a model, being able to better represent network traffic, increasing the upper limit of a model prediction effect, and being able to achieve a better classification effect.

WO 2022/011977 A1

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请涉及一种网络异常检测方法、系统、终端以及存储介质。包括：采用n-gram模型对网络流量进行向量转换，得到所述网络流量的向量矩阵；采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态；通过人工特征提取器提取所述网络流量的人工特征，并对所述人工特征进行时空特征提取，得到所述人工特征的隐状态；将所述网络流量的隐状态与所述人工特征的隐状态进行拼接后，输入深度神经网络进行所述网络流量的分类预测，根据所述预测结果判定网络流量是否异常。本申请使用融合的特征进行模型的建模，能够更好地表示网络流量，增加了模型预测效果的上限，可以达到更好的分类效果。

一种网络异常检测方法、系统、终端以及存储介质

技术领域

本申请属于网络安全技术领域，特别涉及一种网络异常检测方法、系统、终端以及存储介质。

背景技术

根据中国互联网络信息中心(CNNIC)的第45次中国互联网络发展状况统计报告，截止2020年3月，我国网民规模突破九亿，互联网普及率达64.5%。但随着网络技术的蓬勃发展，网络安全事件也层出不穷。据深信服科技报告，恶意软件在2019年表现非常活跃，病毒感染、勒索软件、网络攻击等恶意行为层出不穷。当前网络安全威胁非常严峻，如果能在网络入侵的早期发现这些异常的网络流量，并对其进行拦截，就可以有效减少网络入侵事件的发生，增加信息系统的稳定性。网络异常检测系统，正是被用于解决这个问题的，它的目的是识别出网络流量中不符合正常行为模式的网络流量。

目前，网络异常检测技术可以分为两类：

一、基于指纹的（Signature-based）检测方法：它的原理是分析已知异常的流量数据，从中提取出特定的字符串模式，以此为基础建立异常流量指纹数据库。当发现新的网络流量时将该流量与数据库中的指纹一一对比，一旦发现含有恶意流量的指纹，即可判定当前流量为异常。基于指纹的检测方法是一种比较成熟的检测方法，这种方法准确率高，但是它需要经验丰富的专家来提取指纹，且需要长期维护指纹数据库，随着异常流量越来越多，日益臃肿的指纹数据库必然会影响网络异常检测的速度；再者，该方法只能识别已知的恶意攻击，无法应对未知的新攻击，例如0day漏洞检测等。

二、基于异常的（Anomaly-based）检测方法：基于异常的检测方法是当前ADS的主流研究方向。该方法的核心思想是为合法的用户行为建立可信的活动模型，然后将该模型用于计算新行为满足合法行为的概率，如果得分越低，说明该行为有可能是异常行为。建立模型的方法往往使用了数理统计、数据挖掘、机器学习等知识。该方法可以检

测未知的网络流量，但是如何建立一个有效的、误警率低、漏报率低的模型，一直是一个挑战。

基于异常的检测方法，目前也存在大量的研究工作。但为了使用机器学习等方法训练分类器，必须先将网络流量转换成一组向量表示，而这部分目前往往是由人工实现的。大部分的研究工作基于人工设定的流量特征数据集，这显然不能特征设计的好坏决定了分类器的上限。也有部分工作尝试使用原始数据建模，但所使用的流量嵌入方式多为字节级别的one-hot编码，存在一定的缺陷，不能很好地反应数据的内部隐含关系。

发明内容

本申请提供了一种网络异常检测方法、系统、终端以及存储介质，旨在至少在一定程度上解决现有技术中的上述技术问题之一。

为了解决上述问题，本申请提供了如下技术方案：

一种网络异常检测方法，包括以下步骤：

采用n-gram模型对网络流量进行向量转换，得到所述网络流量的向量矩阵；

采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态；

通过人工特征提取器提取所述网络流量的人工特征，并对所述人工特征进行时空特征提取，得到所述人工特征的隐状态；

将所述网络流量的隐状态与所述人工特征的隐状态进行拼接后，输入深度神经网络进行所述网络流量的分类预测，根据所述预测结果判定网络流量是否异常。

本申请实施例采取的技术方案还包括：所述采用n-gram模型对网络流量数据进行向量转换前还包括：

将所述网络流量转换成标准输入形式的网络流量数据包；具体为：

将所述网络流量按照五元组<源IP，目标IP，源端口，目标端口，传输协议>分成m个组，每一组代表一个双向通信流；

取每个组中的前p个数据包，得到$m*p$个数据包；

取每个数据包的前q个字节，得到$m*p*q$个字节；

将m个组中前p个数据包的前q字节进行拼接，形成一个$m*p*q$的张量。

本申请实施例采取的技术方案还包括：所述采用n-gram模型对网络流量进行向量转换包括：

设置长度为256的1-gram哈希字节表，并设置长度为l_1的2-gram哈希字节表和长度为l_2的3-gram哈希字节表；

将每个2-gram和3-gram的字节组合分别映射到2-gram哈希字节表和3-gram哈希字节表中，相同位置的组合使用共享的嵌入表示；

对所述1-gram、2-gram、3gram哈希字节表中的每项元素分别设置一个对应的d维向量；

将所述$m*p*q$的张量中的q个字节分别经过所述1-gram、2-gram、3gram哈希字节表进行向量转换，得到v_1,v_1,v_3，并将v_1,v_1,v_3进行拼接，得到输出维度为$m*p*n*3d$的张量，其中$n=p+p/2+p/3$。

本申请实施例采取的技术方案还包括：所述采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态包括：

对所述$m*p$个网络流量数据包的向量矩阵分别进行一维卷积操作，得到各个网络流量数据包的第一隐状态h_1；

对所述$m*p$个网络流量数据包的第一隐状态h_1分别进行时空特征提取，得到各个网络流量数据包的第二隐状态h_2。

本申请实施例采取的技术方案还包括：所述对所述$m*p$个网络流量数据包的向量矩阵分别进行一维卷积操作包括：

分别设置尺寸为$3*3d$、$4*3d$和$5*3d$的卷积核，每种卷积核使用的数量为r，所述卷积核总数为$3r$；

对第i个（$0<i\leq p$）网络流量数据包进行行方向的一维卷积操作，得到$3r$个特征图；

对所述$3r$个特征图分别进行最大池化操作，得到$3r$个值，将所述$3r$个值进行拼接，得到第i个网络流量数据包的第一隐状态h_{i1}。

本申请实施例采取的技术方案还包括：所述对所述$m*p$个网络流量数据包的第一隐状态h_1分别进行时空特征提取包括：

将第i个网络流量数据包的第一隐状态h_{i1}送进双向的长短时记忆网络中学习每一个时间步的第一隐状态s_{i1}；

将所有的第一隐状态s_{i1}送进双向门控循环单元学习每一个时间步的第二隐状态h_{i2}；

根据第二隐状态h_{i2}计算每一个时间步的注意力权重:$e_i = tanh(Wh_{i2} + b)$，$\alpha_i = \frac{exp(e_i)}{i\sum exp(e_i)}$;

对所有第二隐状态h_{i2}进行加权求和，得到第i个网络流量数据包的第二隐状态:$h_2 = \sum_i \alpha_i * h_{i2}$。

本申请实施例采取的技术方案还包括：所述通过人工特征提取器提取所述网络流量的人工特征还包括：

使用流量特征提取工具从所述网络流量中提取80个手工设计的网络流量特征；

将所述网络流量中的每一条网络流分别表示成一个尺寸为1*80的流量向量，每一列代表一个特征值。

本申请实施例采取的技术方案还包括：所述对所述人工特征进行时空特征提取，得到所述人工特征的隐状态包括：

将所述网络流量的人工特征转换成标准输入形式的人工特征数据包；

将所述标准输入形式的人工特征数据包进行时空特征提取，得到每条流量向量的隐状态h'_2。

本申请实施例采取的另一技术方案为：一种网络异常检测系统，包括：

向量转换模块：用于采用n-gram模型对网络流量进行向量转换，得到所述网络流量的向量矩阵；

第一时空特征提取模块：用于采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态；

人工特征提取模块：用于通过人工特征提取器提取所述网络流量的人工特征；

第二时空特征提取模块：用于对所述人工特征进行时空特征提取，得到所述人工特征的隐状态；

网络流量预测模块：用于将所述网络流量的隐状态与所述人工特征的隐状态进行拼接后，输入深度神经网络进行所述网络流量的分类预测，根据所述预测结果判定网络流量是否异常。

本申请实施例采取的又一技术方案为：一种终端，所述终端包括处理器、与所述处理器耦接的存储器，其中，

所述存储器存储有用于实现所述网络异常检测方法的程序指令；

所述处理器用于执行所述存储器存储的所述程序指令以控制网络异常检测。

本申请实施例采取的又一技术方案为：一种存储介质，存储有处理器可运行的程序指令，所述程序指令用于执行所述网络异常检测方法。

相对于现有技术，本申请实施例产生的有益效果在于：本申请实施例的网络异常检测方法、系统、终端及存储介质通过使用n-gram模型建立网络流量的组合表，并对每一个组合学习一个低维空间中的向量表示，并使用融合的特征进行模型的建模，即在人工设计的特征基础上使用深度神经网络学习网络流量的内在特征表示，能够更好地表示网络流量，增加了模型预测效果的上限。同时，本申请实施例使用一维卷积、双向LSTM、双向GRU和注意力机制，能够更好的反应数据的内部隐含关系，从而更好地学习到网络流量的特征表示，可以达到更好的分类效果。

附图说明

图1是本申请实施例的网络异常检测方法的流程图；

图2为本申请实施例的原始网络流量转换方式示意图；

图3为本申请实施例采用n-gram模型对标准输入形式的网络流量数据包进行向量转换的流程图；

图4为本申请实施例对每个网络流量数据包的向量矩阵进行一维卷积操作的流程图；

图5为本申请实施例时空特征提取的流程图；

图6是本申请实施例的网络异常检测系统的结构示意图；

图7为本申请实施例的终端结构示意图；

图8为本申请实施例的存储介质的结构示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。

为了解决现有技术的不足，本申请实施例使用n-gram模型建立网络流量的组合表，并对每一个组合学习一个低维空间中的向量表示，每一个网络数据包通过n-gram模型进行拆分并进行向量转换后，送入深度神经网络学习网络流量的向量空间表示，提取时空特

征。同时，为了补充神经网络可能没有学习到的隐含特征，本申请实施例通过加入人工设计的特征表示，进一步提高模型的检测效果。

具体的，请参阅图1，是本申请实施例的网络异常检测方法的流程图。本申请实施例的网络异常检测方法包括以下步骤：

S1：采集原始网络流量，并同时执行S2和S6；

本申请实施例中，网络流量采集方式具体为：使用Wireshark、TCPdump等网络流量捕获技术捕获网络流量数据包，并将捕获到的网络流量数据包保存为pacp文件。

S2：将原始网络流量转换成标准输入形式的网络流量数据包；

本步骤中，请一并参阅图2，为原始网络流量转换方式示意图，其具体包括：

S21：将原始网络流量按照五元组<源IP，目标IP，源端口，目标端口，传输协议>分成m个组，每一组代表一个双向通信流；其中，m值的大小可根据实际应用进行设定；

S22：取每个组中的前p个数据包，得到$m*p$个数据包；其中，如果存在不足p个数据包的组，则对该组进行填充，使其达到p个数据包；p值的大小可根据实际应用进行设定；

S23：取每个数据包的前q个字节，得到$m*p*q$个字节；其中，如果存在不足q个字节的数据包，则对该数据包进行0x00字节的填充，使其达到q个字节；q值的大小可根据实际应用进行设定；

S24：将m个组中前p个数据包的前q字节进行拼接，形成一个$m*p*q$的张量。

S3：采用n-gram模型对标准输入形式的网络流量数据包进行向量转换，得到每个网络流量数据包的向量矩阵；

本步骤中，请一并参阅图3，为采用n-gram模型对标准输入形式的网络流量数据包进行向量转换的流程图，其具体包括：

S31：设置长度为256的1-gram哈希字节表，并设置长度为l_1的2-gram哈希字节表和长度为l_2的3-gram哈希字节表；

S32：将每个2-gram和3-gram的字节组合分别映射到2-gram哈希字节表和3-gram哈希字节表中，相同位置的组合使用共享的嵌入表示；

S33：对1-gram、2-gram、3gram字节表中的每项元素设置一个对应的d维向量，该d维向量的值先随机初始化；

S34：将$m*p*q$的张量中的q个字节分别经过1-gram、2-gram、3gram字节表进行向量转换，得到v_1,v_1,v_3，并将v_1,v_1,v_3进行拼接，得到输出维度为$m*p*n*3d$的张量，其中$n=p+p/2+p/3$。

S4：对$m*p$个网络流量数据包的向量矩阵分别进行一维卷积操作，得到各个网络流量数据包的第一隐状态h_1；

本步骤中，通过使用一维卷积对网络流量数据包的向量矩阵进行纵向扫描计算，并使用最大池化技术压缩数据。具体如图4所示，为对每个网络流量数据包的向量矩阵进行一维卷积操作的流程图，其具体包括：

S41：分别设置尺寸为$3*3d$、$4*3d$和$5*3d$的3种卷积核，每种卷积核使用的数量为r，即卷积核总数为$3r$；

S42：对第i个（$0<i\leq p$）网络流量数据包进行行方向的一维卷积操作，每个卷积核可得到一个特征图，则共得到$3r$个特征图；

S43：对$3r$个特征图分别进行最大池化操作，得到$3r$个值，将$3r$个值进行拼接，得到第i个网络流量数据包的第一隐状态h_{i1}。

S5：对$m*p$个网络流量数据包的第一隐状态h_1分别进行时空特征提取，得到各个网络流量数据包的第二隐状态h_2，并执行S9；

本步骤中，使用双向的LSTM结构、双向的GRU结构以及注意力机制对网络流量数据包进行时空特征提取，具体如图5所示，为时空特征提取的流程图，其具体包括：

S51：将第i个网络流量数据包的第一隐状态h_{i1}送进双向的长短时记忆网络（Bi-LSTM）中学习每一个时间步的第一隐状态s_{i1}；

S52：将所有的第一隐状态s_{i1}送进双向门控循环单元（Bi-GRU）学习每一个时间步的第二隐状态h_{i2}；

S53：根据第二隐状态h_{i2}计算每一个时间步的注意力权重:$e_i=tanh(Wh_{i2}+b)$，$\alpha_i=\frac{exp(e_i)}{i\sum exp(e_i)}$；

S54：对所有第二隐状态h_{i2}进行加权求和，得到第i个网络流量数据包的第二隐状态:$h_2=\sum_i \alpha_i*h_{i2}$。

S6：通过人工特征提取器对原始网络流量进行人工特征提取，得到原始网络流量的人工特征表示；

本步骤中，原始网络流量的人工特征提取方式具体包括：使用流量特征提取工具CICFlowMeter从pcap文件中提取80个手工设计的网络流量特征；将原始网络流量中的每一条网络流分别表示成一个尺寸为1*80的流量向量，每一列代表一个特征值。

S7：将原始网络流量的人工特征表示转换成标准输入形式的人工特征数据包；

本步骤中，人工特征表示的转换方式具体为：

首先，对原始网络流量中每一条网络流的每一个特征分别进行归一化操作，将属性值映射到0-1之间：

$$x = x \cdot \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

然后，设定窗口长度w，将每一条网络流向量与其前$w-1$条网络流向量进行组合，得到尺寸为$w*80$的流量向量表示。

S8：将标准输入形式的人工特征数据包进行时空特征提取，得到每条流量向量的隐状态h'_2；

本步骤中，使用双向的LSTM结构、双向的GRU结构以及注意力机制对人工特征数据包进行时空特征提取，流量向量的隐状态h'_2与网络流量数据的第二隐状态h_2的时空特征提取过程相同，此处将不再赘述。

步骤900：将网络流量数据包的第二隐状态h_2与流量向量的隐状态h'_2进行拼接，得到最终的第三隐状态h_3，将第三隐状态h_3输入深度神经网络进行网络流量的分类预测，根据预测结果判定网络流量数据是否异常；

本步骤中，将h_3送进深度神经网络后，首先计算网络流量不同类别的输出预测值：$u = Wh_3 + b$；然后对预测值u进行Softmax分类，得到网络流量的预测标签：$y = argmax\{\frac{exp\,(u_i)}{\sum \exp\,(u_i)}\}$。

基于上述，本申请实施例的网络异常检测方法通过使用融合的特征进行模型的建模，即在人工设计的特征基础上使用深度神经网络学习网络流量的内在特征表示，从而能够更好地表示网络流量，从而增加了模型预测效果的上限。同时，本申请实施例提出一种新的字节组合嵌入方法，对网络流量学习1-gram、2-gram和3-gram的向量表示，并将其进行横向拼接，从而更好地表示网络流量。另外，本申请实施例使用一维卷积、双向LSTM、双向GRU和注意力机制，能够更好的反应数据的内部隐含关系，从而更好地学习到网络流量的特征表示，以达到更好的分类效果。

请参阅图6，是本申请实施例的网络异常检测系统的结构示意图。本申请实施例的网络异常检测系统包括：

流量采集模块：用于采集原始网络流量；本申请实施例中，网络流量采集方式具体为：使用Wireshark、TCPdump等网络流量捕获技术捕获网络流量数据包，并将捕获到的网络流量数据包保存为pacp文件。

流量转换模块：用于将原始网络流量转换成标准输入形式的网络流量数据包；其中，流量转换方式具体包括：

将原始网络流量按照五元组<源IP，目标IP，源端口，目标端口，传输协议>分成m个组，每一组代表一个双向通信流；其中，m值的大小可根据实际应用进行设定；

取每个组中的前p个数据包，得到$m*p$个数据包；其中，如果存在不足p个数据包的组，则对该组进行填充，使其达到p个数据包；p值的大小可根据实际应用进行设定；

取每个数据包的前q个字节，得到$m*p*q$个字节；其中，如果存在不足q个字节的数据包，则对该数据包进行0x00字节的填充，使其达到q个字节；q值的大小可根据实际应用进行设定；

将m个组中前p个数据包的前q字节进行拼接，形成一个$m*p*q$的张量。

向量转换模块：用于采用n-gram模型对标准输入形式的网络流量数据包进行向量转换，得到每个网络流量数据包的向量矩阵；其中，向量转换方式具体包括：

设置长度为256的1-gram哈希字节表，并设置长度为l_1的2-gram哈希字节表和长度为l_2的3-gram哈希字节表；

将每个2-gram和3-gram的字节组合分别映射到2-gram哈希字节表和3-gram哈希字节表中，相同位置的组合使用共享的嵌入表示；

对1-gram、2-gram、3gram字节表中的每项元素设置一个对应的d维向量，该d维向量的值先随机初始化；

将$m*p*q$的张量中的q个字节分别经过1-gram、2-gram、3gram字节表进行向量转换，得到v_1,v_1,v_3，并将v_1,v_1,v_3进行拼接，得到输出维度为$m*p*n*3d$的张量，其中$n=p+p/2+p/3$。

卷积计算模块：用于对$m*p$个网络流量数据包的向量矩阵分别进行一维卷积操作，得到各个网络流量数据包的第一隐状态h_1；其中，本申请实施例通过使用一维卷积对网

络流量数据包的向量矩阵进行纵向扫描计算，并使用最大池化技术压缩数据。具体包括：

分别设置尺寸为$3*3d$、$4*3d$和$5*3d$的3种卷积核，每种卷积核使用的数量为r，即卷积核总数为$3r$；

对第i个（$0<i\leq p$）网络流量数据包进行行方向的一维卷积操作，每个卷积核可得到一个特征图，则共得到$3r$个特征图；

对$3r$个特征图分别进行最大池化操作，得到$3r$个值，将$3r$个值进行拼接，得到第i个网络流量数据包的第一隐状态h_{i1}。

第一时空特征提取模块：用于对$m*p$个网络流量数据包的第一隐状态h_1分别进行时空特征提取，得到各个网络流量数据包的第二隐状态h_2；其中，本申请实施例使用双向的LSTM结构、双向的GRU结构以及注意力机制对网络流量数据包进行时空特征提取，具体包括：

将第i个网络流量数据包的第一隐状态h_{i1}送进双向的长短时记忆网络（Bi-LSTM）中学习每一个时间步的第一隐状态s_{i1}；

将所有的第一隐状态s_{i1}送进双向门控循环单元（Bi-GRU）学习每一个时间步的第二隐状态h_{i2}；

根据第二隐状态h_{i2}计算每一个时间步的注意力权重:$e_i=tanh(Wh_{i2}+b)$，$\alpha_i=\frac{exp(e_i)}{i\sum exp(e_i)}$;

对所有第二隐状态h_{i2}进行加权求和，得到第i个网络流量数据包的第二隐状态:$h_2=\sum_i \alpha_i*h_{i2}$。

人工特征提取模块：用于通过人工特征提取器对原始网络流量进行人工特征提取，得到原始网络流量的人工特征表示；其中，原始网络流量的人工特征提取方式具体包括：使用流量特征提取工具CICFlowMeter从pcap文件中提取80个手工设计的网络流量特征；将原始网络流量中的每一条网络流分别表示成一个尺寸为1*80的流量向量，每一列代表一个特征值。

人工特征转换模块：用于将原始网络流量的人工特征表示转换成标准输入形式的人工特征数据包；其中，人工特征表示的转换方式具体为：

首先，对原始网络流量中每一条网络流的每一个特征分别进行归一化操作，将属性值映射到0-1之间：

$$x = x \cdot \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

然后，设定窗口长度w，将每一条网络流向量与其前$w-1$条网络流向量进行组合，得到尺寸为$w*80$的流量向量表示。

第二时空特征提取模块：用于将标准输入形式的人工特征数据包进行时空特征提取，得到每条流量向量的隐状态h'_2；其中，流量向量的隐状态h'_2与网络流量数据的第二隐状态h_2的时空特征提取过程相同，此处将不再赘述。

网络流量预测模块：用于将网络流量数据包的第二隐状态h_2与流量向量的隐状态h'_2进行拼接，得到最终的第三隐状态h_3，将隐状态h_3输入深度神经网络进行网络流量的分类预测，根据预测结果判定网络流量是否异常；其中，将h_3送进深度神经网络后，首先计算网络流量不同类别的输出预测值：$u = Wh_3 + b$；然后对预测值u进行Softmax分类，得到网络流量的预测标签：$y = argmax\{\frac{exp\,(u_i)}{\sum \exp\,(u_i)}\}$。

请参阅图7，为本申请实施例的终端结构示意图。该终端50包括处理器51、与处理器51耦接的存储器52。

存储器52存储有用于实现上述网络异常检测方法的程序指令。

处理器51用于执行存储器52存储的程序指令以控制网络异常检测。

其中，处理器51还可以称为CPU（CentralProcessingUnit，中央处理单元）。处理器51可能是一种集成电路芯片，具有信号的处理能力。处理器51还可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现成可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

请参阅图8，为本申请实施例的存储介质的结构示意图。本申请实施例的存储介质存储有能够实现上述所有方法的程序文件61，其中，该程序文件61可以以软件产品的形式存储在上述存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施方式方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-OnlyMemory）、随机存取存储器（RAM，RandomAccessMemory）、磁碟或者光盘等各种可以存储程序代码的介质，或者是计算机、服务器、手机、平板等终端设备。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本申请中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本申请所示的这些实施例，而是要符合与本申请所公开的原理和新颖特点相一致的最宽的范围。

权利要求书

1、一种网络异常检测方法，其特征在于，包括以下步骤：

采用n-gram模型对网络流量进行向量转换，得到所述网络流量的向量矩阵；

采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态；

通过人工特征提取器提取所述网络流量的人工特征，并对所述人工特征进行时空特征提取，得到所述人工特征的隐状态；

将所述网络流量的隐状态与所述人工特征的隐状态进行拼接后，输入深度神经网络进行所述网络流量的分类预测，根据所述预测结果判定所述网络流量是否异常。

2、根据权利要求1所述的网络异常检测方法，其特征在于，所述采用n-gram模型对网络流量数据进行向量转换前还包括：

将所述网络流量转换成标准输入形式的网络流量数据包；具体为：

将所述网络流量按照五元组<源IP，目标IP，源端口，目标端口，传输协议>分成m个组，每一组代表一个双向通信流；

取每个组中的前p个数据包，得到$m*p$个数据包；

取每个数据包的前q个字节，得到$m*p*q$个字节；

将m个组中前p个数据包的前q字节进行拼接，形成一个$m*p*q$的张量。

3、根据权利要求2所述的网络异常检测方法，其特征在于，所述采用n-gram模型对网络流量进行向量转换包括：

设置长度为256的1-gram哈希字节表，并设置长度为l_1的2-gram哈希字节表和长度为l_2的3-gram哈希字节表；

将每个2-gram和3-gram的字节组合分别映射到2-gram哈希字节表和3-gram哈希字节表中，相同位置的组合使用共享的嵌入表示；

对所述1-gram、2-gram、3gram哈希字节表中的每项元素分别设置一个对应的d维向量；

将所述$m*p*q$的张量中的q个字节分别经过所述1-gram、2-gram、3gram哈希字节表进行向量转换，得到v_1,v_1,v_3，并将v_1,v_1,v_3进行拼接，得到输出维度为$m*p*n*3d$的张量，其中$n=p+p/2+p/3$。

4、根据权利要求3所述的网络异常检测方法，其特征在于，所述采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态包括：

对所述$m*p$个网络流量数据包的向量矩阵分别进行一维卷积操作，得到各个网络流量数据包的第一隐状态h_1；

对所述$m*p$个网络流量数据包的第一隐状态h_1分别进行时空特征提取，得到各个网络流量数据包的第二隐状态h_2。

5、根据权利要求4所述的网络异常检测方法，其特征在于，所述对所述$m*p$个网络流量数据包的向量矩阵分别进行一维卷积操作包括：

分别设置尺寸为$3*3d$、$4*3d$和$5*3d$的卷积核，每种卷积核使用的数量为r，所述卷积核总数为$3r$；

对第i个（$0<i\leq p$）网络流量数据包进行行方向的一维卷积操作，得到$3r$个特征图；

对所述$3r$个特征图分别进行最大池化操作，得到$3r$个值，将所述$3r$个值进行拼接，得到第i个网络流量数据包的第一隐状态h_{i1}。

6、根据权利要求5所述的网络异常检测方法，其特征在于，所述对所述$m*p$个网络流量数据包的第一隐状态h_1分别进行时空特征提取包括：

将第i个网络流量数据包的第一隐状态h_{i1}送进双向的长短时记忆网络中学习每一个时间步的第一隐状态s_{i1}；

将所有的第一隐状态s_{i1}送进双向门控循环单元学习每一个时间步的第二隐状态h_{i2}；

根据第二隐状态h_{i2}计算每一个时间步的注意力权重：$e_i=tanh(Wh_{i2}+b)$，$\alpha_i=\frac{exp(e_i)}{i\sum exp(e_i)}$；

对所有第二隐状态h_{i2}进行加权求和，得到第i个网络流量数据包的第二隐状态：$h_2=\sum_i \alpha_i*h_{i2}$。

7、根据权利要求1所述的网络异常检测方法，其特征在于，所述通过人工特征提取器提取所述网络流量的人工特征还包括：

使用流量特征提取工具从所述网络流量中提取80个手工设计的网络流量特征；

将所述网络流量中的每一条网络流分别表示成一个尺寸为1*80的流量向量，每一列代表一个特征值。

8、根据权利要求7所述的网络异常检测方法，其特征在于，所述对所述人工特征进行时空特征提取，得到所述人工特征的隐状态包括：

将所述网络流量的人工特征转换成标准输入形式的人工特征数据包；

将所述标准输入形式的人工特征数据包进行时空特征提取，得到每条流量向量的隐状态h'_2。

9、一种网络异常检测系统，其特征在于，包括：

向量转换模块：用于采用n-gram模型对网络流量进行向量转换，得到所述网络流量的向量矩阵；

第一时空特征提取模块：用于采用长短时记忆网络及双向门控循环单元对所述网络流量的向量矩阵进行时空特征提取，得到所述网络流量的隐状态；

人工特征提取模块：用于通过人工特征提取器提取所述网络流量的人工特征；

第二时空特征提取模块：用于对所述人工特征进行时空特征提取，得到所述人工特征的隐状态；

网络流量预测模块：用于将所述网络流量的隐状态与所述人工特征的隐状态进行拼接后，输入深度神经网络进行所述网络流量的分类预测，根据所述预测结果判定网络流量是否异常。

10、一种终端，其特征在于，所述终端包括处理器、与所述处理器耦接的存储器，其中，

所述存储器存储有用于实现权利要求1-8任一项所述的网络异常检测方法的程序指令；

所述处理器用于执行所述存储器存储的所述程序指令以控制网络异常检测。

11、一种存储介质，其特征在于，存储有处理器可运行的程序指令，所述程序指令用于执行权利要求1至8任一项所述网络异常检测方法。

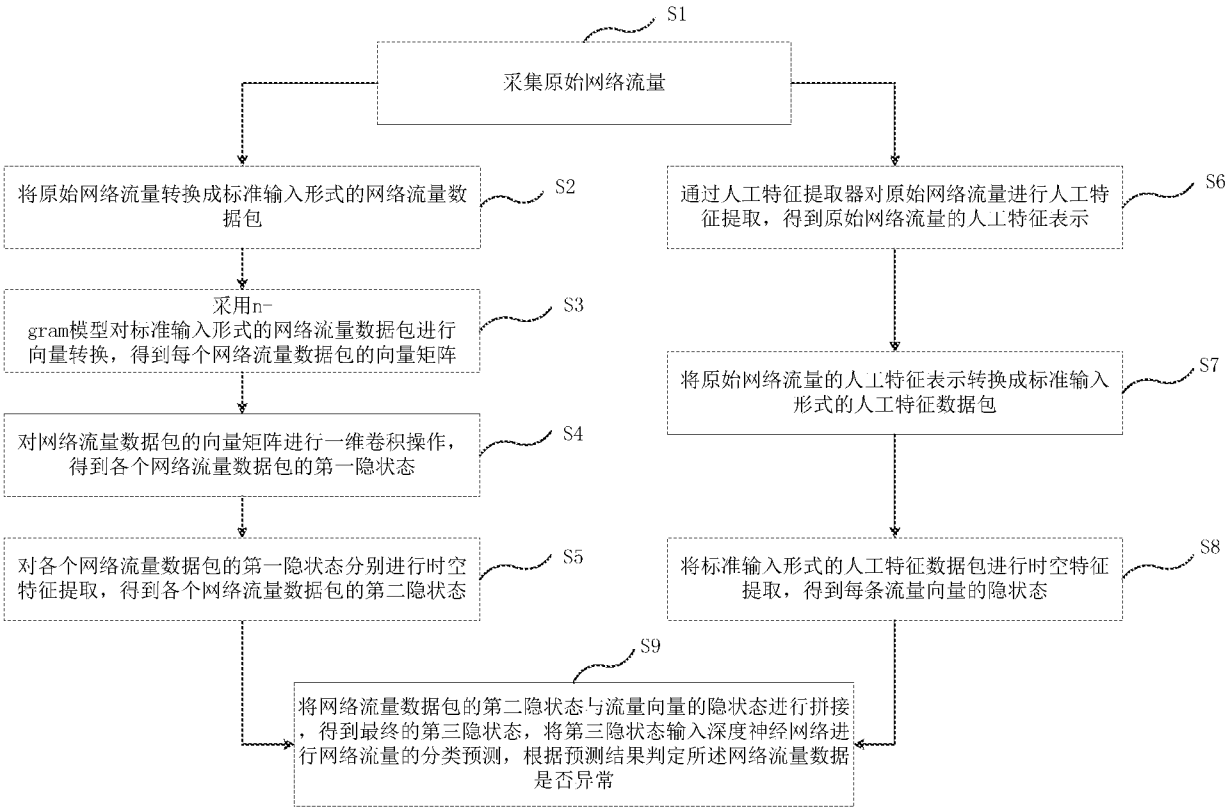
S1
采集原始网络流量
将原始网络流量转换成标准输入形式的网络流量数据包
S2
采用n-gram模型对标准输入形式的网络流量数据包进行向量转换，得到每个网络流量数据包的向量矩阵
S3
对网络流量数据包的向量矩阵进行一维卷积操作，得到各个网络流量数据包的第一隐状态
S4
对各个网络流量数据包的第一隐状态分别进行时空特征提取，得到各个网络流量数据包的第二隐状态
S5
通过人工特征提取器对原始网络流量进行人工特征提取，得到原始网络流量的人工特征表示
S6
将原始网络流量的人工特征表示转换成标准输入形式的人工特征数据包
S7
将标准输入形式的人工特征数据包进行时空特征提取，得到每条流量向量的隐状态
S8
将网络流量数据包的第二隐状态与流量向量的隐状态进行拼接，得到最终的第三隐状态，将第三隐状态输入深度神经网络进行网络流量的分类预测，根据预测结果判定所述网络流量数据是否异常
S9

图1

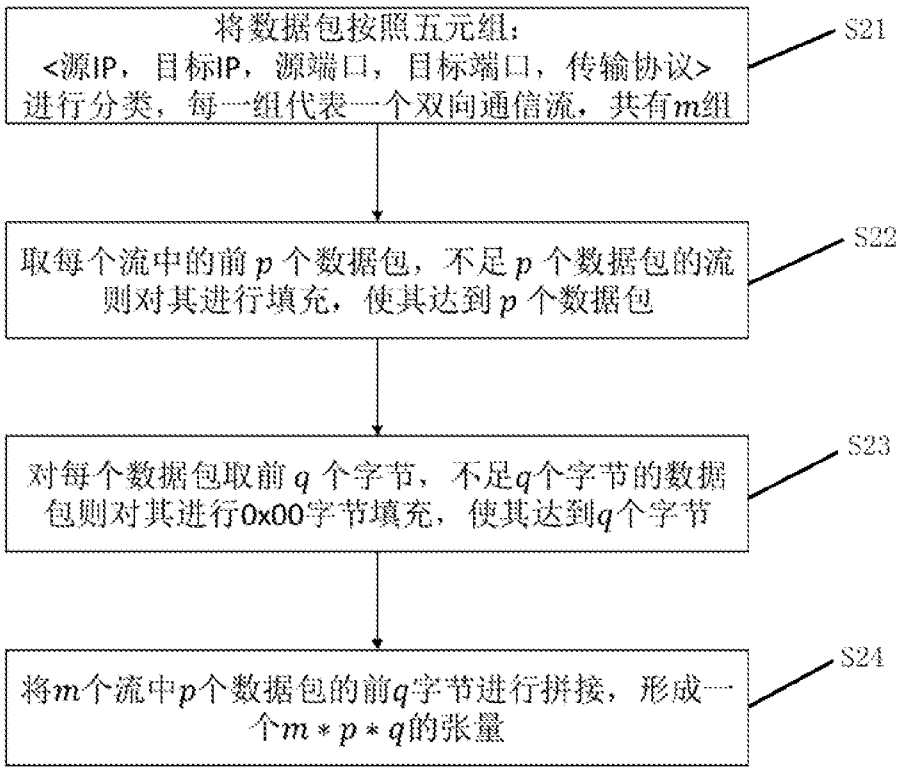
将数据包按照五元组：
<源IP，目标IP，源端口，目标端口，传输协议>
进行分类，每一组代表一个双向通信流，共有m组
S21
取每个流中的前p个数据包，不足p个数据包的流则对其进行填充，使其达到p个数据包
S22
对每个数据包取前q个字节，不足q个字节的数据包则对其进行0x00字节填充，使其达到q个字节
S23
将m个流中p个数据包的前q字节进行拼接，形成一个$m*p*q$的张量
S24

图2

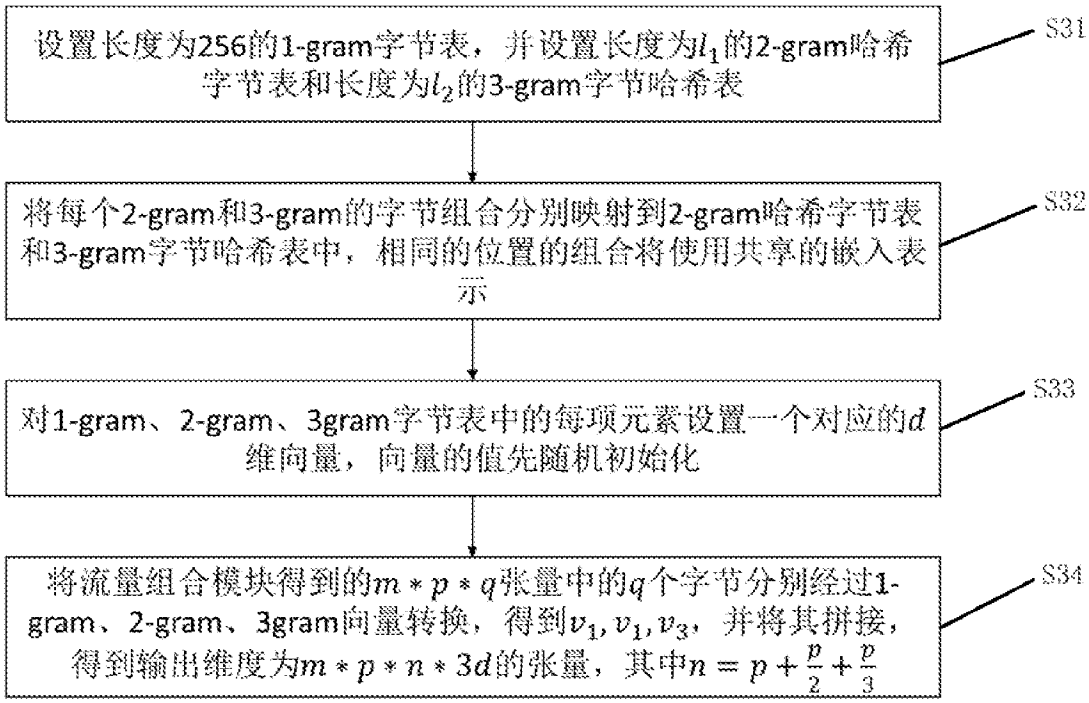
设置长度为256的1-gram字节表，并设置长度为l_1的2-gram哈希字节表和长度为l_2的3-gram字节哈希表
S31
将每个2-gram和3-gram的字节组合分别映射到2-gram哈希字节表和3-gram字节哈希表中，相同的位置的组合将使用共享的嵌入表示
S32
对1-gram、2-gram、3gram字节表中的每项元素设置一个对应的d维向量，向量的值先随机初始化
S33
将流量组合模块得到的$m*p*q$张量中的q个字节分别经过1-gram、2-gram、3gram向量转换，得到v_1, v_1, v_3，并将其拼接，得到输出维度为$m*p*n*3d$的张量，其中$n=p+\frac{p}{2}+\frac{p}{3}$
S34

图3

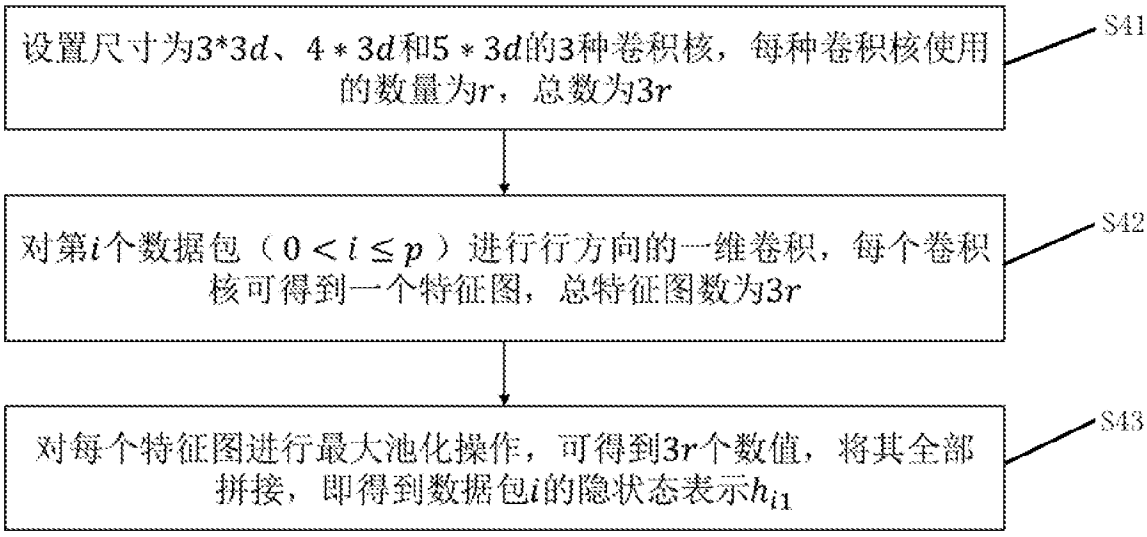
设置尺寸为3*3d、$4*3d$和$5*3d$的3种卷积核，每种卷积核使用的数量为r，总数为$3r$
S41
对第i个数据包（$0<i\leq p$）进行行方向的一维卷积，每个卷积核可得到一个特征图，总特征图数为$3r$
S42
对每个特征图进行最大池化操作，可得到$3r$个数值，将其全部拼接，即得到数据包i的隐状态表示h_{i1}
S43

图4

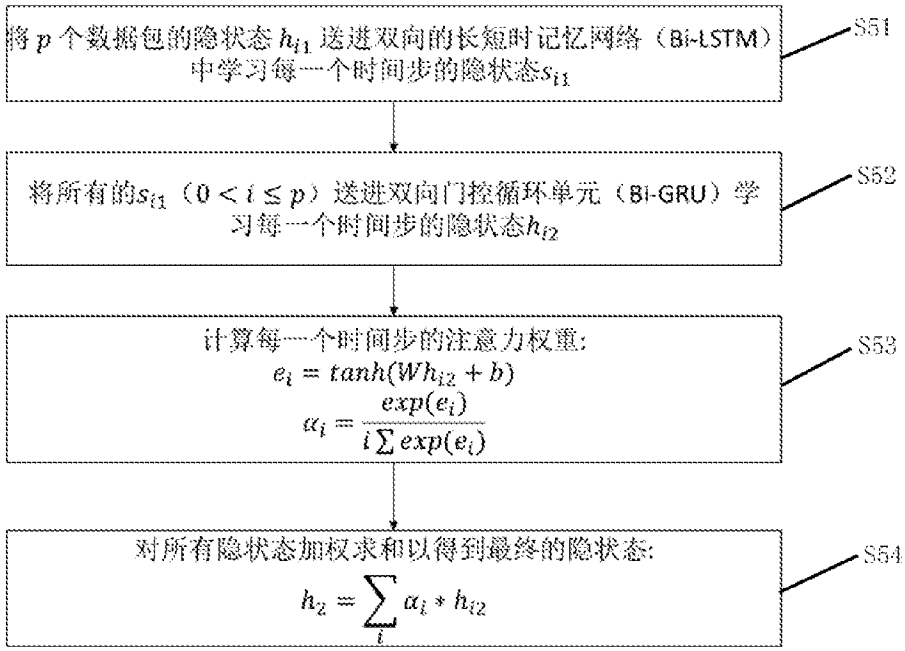
将 p 个数据包的隐状态 h_{i1} 送进双向的长短时记忆网络（Bi-LSTM）中学习每一个时间步的隐状态 s_{i1}
S51
将所有的 s_{i1}（$0 < i \leq p$）送进双向门控循环单元（Bi-GRU）学习每一个时间步的隐状态 h_{i2}
S52
计算每一个时间步的注意力权重：
$e_i = tanh(Wh_{i2} + b)$
$\alpha_i = \frac{exp(e_i)}{i \sum exp(e_i)}$
S53
对所有隐状态加权求和以得到最终的隐状态：
$h_2 = \sum_i \alpha_i * h_{i2}$
S54

图5

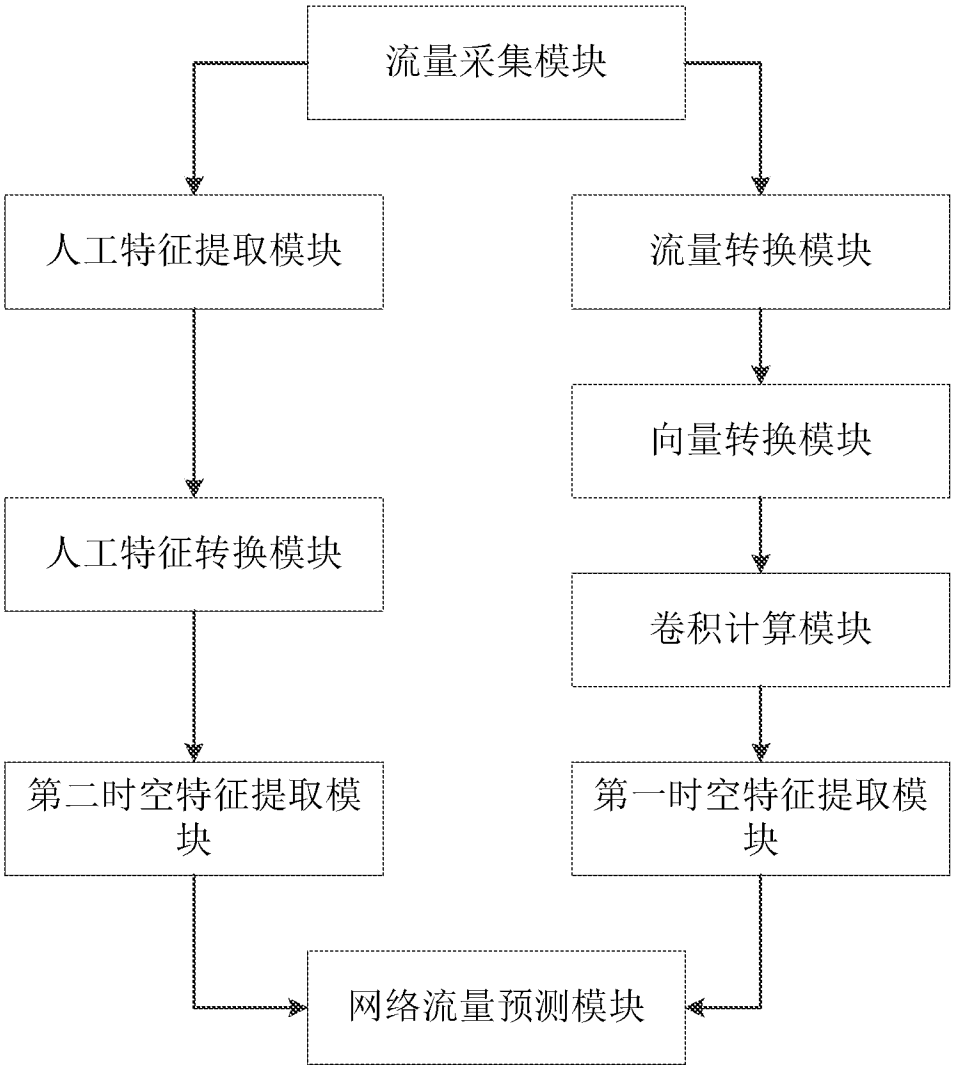
流量采集模块
人工特征提取模块
流量转换模块
向量转换模块
人工特征转换模块
卷积计算模块
第二时空特征提取模块
第一时空特征提取模块
网络流量预测模块

图6

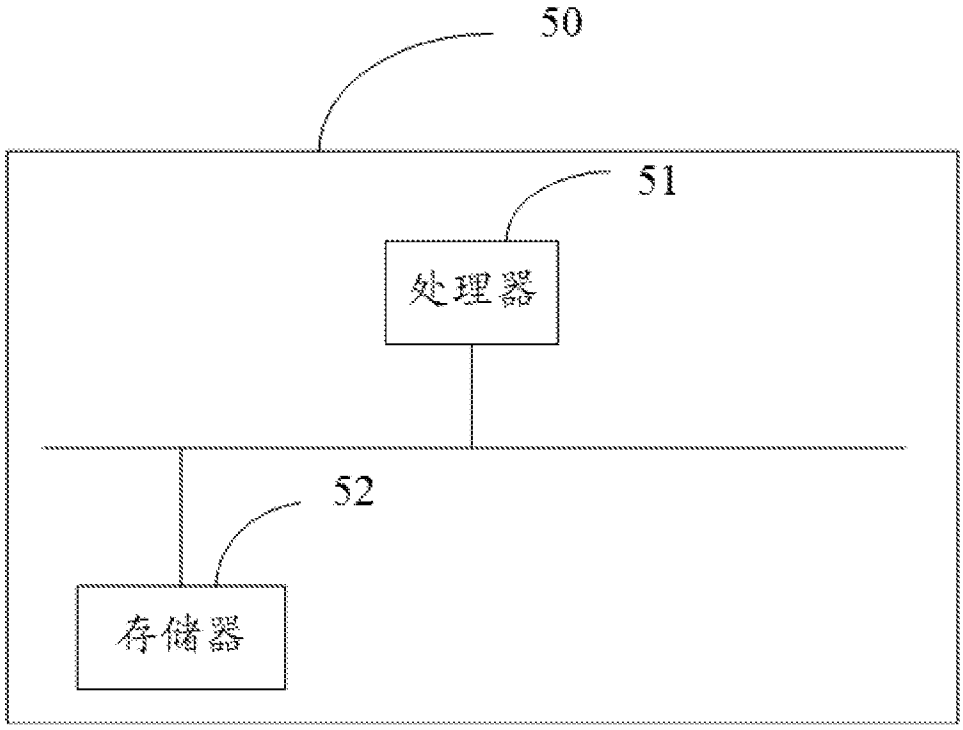

图7

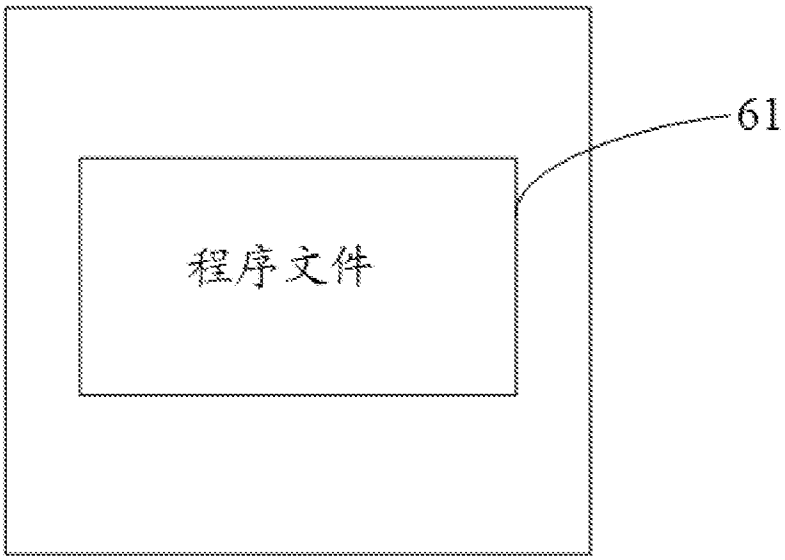

图8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/138820

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; USTXT; WOTXT; EPTXT; CNKI: 网络, 检测, 流量, 异常, 特征, 提取, 向量, n-gram模型, 长短时记忆, 神经网络, 隐, 状态, 分类, 预测, network, detect, flow, abnormal, feature, extract, vector, matrix, n-gram pattern, LSTM, neural network, hide, status, classify, predict

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 110851782 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 28 February 2020 (2020-02-28) entire document	1-11
A	CN 106951783 A (STATE GRID CORPORATION OF CHINA et al.) 14 July 2017 (2017-07-14) entire document	1-11
A	CN 108173708 A (BEIJING TOPSEC NETWORK SECURITY TECHNOLOGY CO., LTD. et al.) 15 June 2018 (2018-06-15) entire document	1-11
A	US 2015205826 A1 (IBM) 23 July 2015 (2015-07-23) entire document	1-11
A	仇媛 等 (QIU, Yuan et al.). "基于长短期记忆网络和滑动窗口的流数据异常检测方法 (Stream Data Anomaly Detection Method Based on Long Short-Term Memory Network and Sliding Window)" *计算机应用 (Journal of Computer Applications)*, Vol. 40, No. 5, 10 May 2020 (2020-05-10), pp. 1-5	1-11

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 March 2021	**30 March 2021**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/138820

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110851782 A	28 February 2020	None	
CN 106951783 A	14 July 2017	None	
CN 108173708 A	15 June 2018	None	
US 2015205826 A1	23 July 2015	CN 104050096 A	17 September 2014
		CN 104050096 B	15 August 2017
		DE 102014103072 A1	11 September 2014
		US 9507767 B2	29 November 2016
		US 2014258314 A1	11 September 2014
		US 2016124938 A1	05 May 2016
		US 9092444 B2	28 July 2015
		US 9275064 B2	01 March 2016

国际检索报告

国际申请号
PCT/CN2020/138820

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;USTXT;WOTXT;EPTXT;CNKI:网络，检测，流量，异常，特征，提取，向量，n-gram模型，长短时记忆，神经网络，隐，状态，分类，预测，network, detect, flow, abnormal, feature, extract, vector, matrix, n-gram pattern, LSTM, neural network, hide, status, classify, predict

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 110851782 A (南京邮电大学) 2020年 2月 28日 (2020-02-28) 全文	1-11
A	CN 106951783 A (国家电网公司等) 2017年 7月 14日 (2017-07-14) 全文	1-11
A	CN 108173708 A (北京天融信网络安全技术有限公司等) 2018年 6月 15日 (2018-06-15) 全文	1-11
A	US 2015205826 A1 (IBM) 2015年 7月 23日 (2015-07-23) 全文	1-11
A	仇媛等. "基于长短期记忆网络和滑动窗口的流数据异常检测方法" 计算机应用, 第40卷，第5期，2020年 5月 10日 (2020-05-10)， 第1-5页	1-11

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 3月 9日	2021年 3月 30日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 鲁秋艳 电话号码 86-010-62411073

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/138820

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110851782	A	2020年 2月 28日	无			
CN	106951783	A	2017年 7月 14日	无			
CN	108173708	A	2018年 6月 15日	无			
US	2015205826	A1	2015年 7月 23日	CN	104050096	A	2014年 9月 17日
				CN	104050096	B	2017年 8月 15日
				DE	102014103072	A1	2014年 9月 11日
				US	9507767	B2	2016年 11月 29日
				US	2014258314	A1	2014年 9月 11日
				US	2016124938	A1	2016年 5月 5日
				US	9092444	B2	2015年 7月 28日
				US	9275064	B2	2016年 3月 1日