

(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
2024 年 10 月 10 日 (10.10.2024)



(10) 国际公布号
WO 2024/207804 A1

- (51) 国际专利分类号:
H04L 9/40 (2022.01)
- (21) 国际申请号: PCT/CN2023/139627
- (22) 国际申请日: 2023 年 12 月 18 日 (18.12.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202310365470.7 2023年4月7日 (07.04.2023) CN
- (71) 申请人: 天翼云科技有限公司(CHINA TELECOM CLOUD TECHNOLOGY CO., LTD.) [CN/CN]; 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。
- (72) 发明人: 方文(FANG, Wen); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007

(CN)。李旭(LI, Xu); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。张卫平(ZHANG, Weiping); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。郑尧展(ZHENG, Yaozhan); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。张刚(ZHANG, Gang); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。林志銮(LIN, Zhiluan); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。刘阳(LIU, Yang); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。景广豫(JING, Guangyu); 中国北京市东城区青龙胡同甲1号、3号2幢2层205-32室, Beijing 100007 (CN)。

(54) Title: NETWORK INTRUSION DETECTION METHOD AND APPARATUS, AND ELECTRONIC DEVICE AND READ-ABLE STORAGE MEDIUM

(54) 发明名称: 网络入侵检测方法、装置、电子设备和可读存储介质

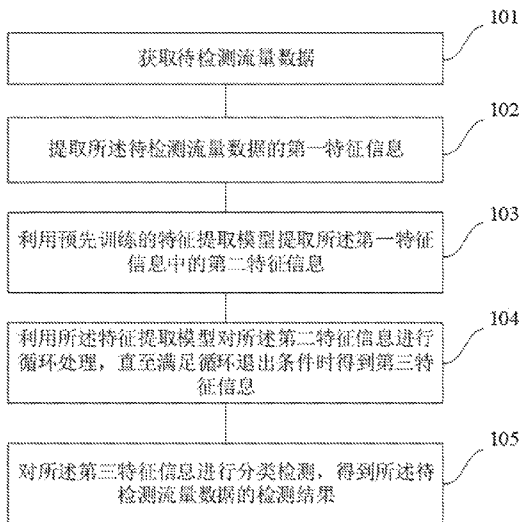


图 1

- 101 Acquire traffic data to be subjected to detection
102 Extract first feature information of said traffic data
103 Extract second feature information from the first feature information by using a pre-trained feature extraction model
104 Perform loop processing on the second feature information by using the feature extraction model until a loop exit condition is met, so as to obtain third feature information
105 Perform classification detection on the third feature information, so as to obtain a detection result of said traffic data

(57) Abstract: The embodiments of the present application relate to the field of system security. Provided are a network intrusion detection method and apparatus, and an electronic device and a readable storage medium. The method comprises: acquiring traffic data to be subjected to detection; extracting first feature information of said traffic data; extracting second feature information from the first feature information by using a pre-trained feature extraction model, wherein the feature extraction model is a multi-head self-attention network model; performing loop processing on the second feature information by using the feature extraction model until a loop exit condition is met, so as to obtain third feature information, wherein in each round of loop, input data of the feature extraction model is output data of the previous round; and performing classification detection on the third feature information, so as to obtain a detection

(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街甲 18 号北京国际 C 座 6 层 606, Beijing 100081 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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)。

根据细则 4.17 的声明:

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

result of said traffic data. By means of the method, the accuracy of traffic data classification can be effectively improved, thereby reducing risks caused by network intrusion.

(57) 摘要: 本申请实施例提供了一种网络入侵检测方法、装置、电子设备和可读存储介质, 涉及系统安全领域, 所述方法包括: 获取待检测流量数据; 提取所述待检测流量数据的第一特征信息; 利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息, 所述特征提取模型为多头自注意力网络模型; 利用所述特征提取模型对所述第二特征信息进行循环处理, 直至满足循环退出条件时得到第三特征信息; 在每一轮循环中, 所述特征提取模型的输入数据为上一轮的输出数据; 对所述第三特征信息进行分类检测, 得到所述待检测流量数据的检测结果。通过上述方法, 可以有效提高流量数据分类的准确性, 降低网络入侵带来的风险。

网络入侵检测方法、装置、电子设备和可读存储介质

相关申请的交叉引用

本申请要求于 2023 年 04 月 27 日提交中国专利局, 申请号为 202310365470.7, 申请名称为“网络入侵检测方法、装置、电子设备和可读存储介质”的中国专利申请优先权, 其全部内容通过引用结合在本申请中。

技术领域

本申请涉及系统安全领域, 尤其涉及一种网络入侵检测方法、装置、电子设备和可读存储介质。

背景技术

随着信息化、数字化的迅猛发展, 以云计算为代表的新兴技术产业正备受关注, 尽管云计算有着诸多优势, 但其一直面临着网络安全问题带来的重大挑战, 尤其是异常的流量数据更会导致网络入侵的风险大大提高。

在相关技术中, 通常利用卷积神经网络(Convolutional Neural Network, CNN)对网络上的流量数据进行特征提取, 进而通过分类识别流量数据是否存在异常。

但是, 与其他数据如图像、语音数据不同, 由于流量数据的特征比较稀疏, 在流量数据序列较长的情况下, 基于 CNN 的流量数据特征在学习流量序列间的依赖关系方面有所欠缺, 因此基于 CNN 的网络检测方法在对检测网络中的流量数据进行分类检测时准确率较低, 导致异常流量数据所带来的网络入侵风险较高。

发明内容

本申请实施例提供一种网络入侵检测方法、装置、电子设备和可读存储介质, 可以提高对异常流量数据分类的准确性, 降低网络入侵带来的风险。

本申请实施例提供了一种网络入侵检测方法, 方法包括:

获取待检测流量数据;

提取待检测流量数据的第一特征信息;

利用预先训练的特征提取模型提取第一特征信息中的第二特征信息, 特征提取模型为多头自注意力网络模型;

利用特征提取模型对第二特征信息进行循环处理, 直至满足循环退出条件时得到第三特征信息; 在每一轮循环中, 特征提取模型的输入数据为上一轮的输出数据;

对第三特征信息进行分类检测, 得到待检测流量数据的检测结果。

可选地, 第一特征信息中包括至少一个第一特征矩阵;

利用预先训练的特征提取模型提取第一特征信息中的第二特征信息, 包括: 计算第一特征矩阵的稀疏度;

基于第一特征矩阵的稀疏度, 按照预设的稀疏度阈值从至少一个第一特征矩阵中筛选出 N 个连续的第一特征矩阵;

利用预先训练的特征提取模型提取 N 个连续的第一特征矩阵中的第二特征信息;

其中, 稀疏度表示为:

$$M(q_i, K) = \ln \sum_{j=1}^{L_K} e^{\frac{q_i k_j^T}{\sqrt{d}}} - \frac{1}{L_K} \sum_{j=1}^{L_K} \frac{q_i k_j^T}{\sqrt{d}},$$

其中， M 表示第一特征信息中第 i 个第一特征矩阵 q_i 的稀疏度， L_K 表示第一特征信息中第一特征矩阵的个数， k_j 表示第一特征信息中第 j 个第一特征矩阵， $\sqrt{d}$ 表示比例因子系数， T 表示矩阵转置。

可选地，利用特征提取模型对第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息，包括：

对第二特征信息进行特征提取，得到待检测流量数据的第四特征信息；

利用特征提取模型对第四特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；

其中，第四特征信息表示为：

$$F = \text{MaxPool}(\text{ELU}(\text{Conv1d}(S)))$$

F 表示第四特征信息， S 表示第二特征信息； Conv1d 表示一维卷积处理， ELU 表示激活函数， MaxPool 表示最大池化处理。

可选地，利用预先训练的特征提取模型提取第一特征信息中的第二特征信息之前，方法还包括：

获取初始样本集，初始样本集包括多数类样本和少数类样本，少数类样本构成平衡样本集；

从少数类样本中抽取一个第一样本；

从少数类样本中确定与第一样本的欧氏距离最近的第二样本；

根据第一样本和第二样本构成的超球面中包含的多数类样本的样本数量调整平衡样本集；

若平衡样本集中的样本数与多数类样本的样本数满足预设比例，则基于平衡样本集和多数类样本生成最终样本集；

基于最终样本集对多头自注意力网络模型进行迭代训练，得到待检测数据的特征提取模型。

可选地，方法还包括：

若平衡样本集中的样本数与多数类样本的样本数不满足预设比例，则从少数类样本中重新抽取第一样本，并基于重新抽取的第一样本重新调整平衡样本集，其中，每个少数类样本只能被抽取一次。

可选地，根据第一样本和第二样本构成的超球面中包含的多数类样本的样本数量调整平衡样本集，包括：

基于第一样本和第二样本构建第一超球面；

将位于第一超球面所构成的空间中的多数类样本添加到第一样本集中；

若第一样本集为空集，则在第一超球面所构成的空间中生成一个第三样本，并将第三样本添加到平衡样本集中。

可选地，方法还包括：

若第一样本集不为空集，则从第一样本集中确定与第一样本的欧氏距离最近

的第四样本；

基于第一样本和第四样本构建第二超球面；

根据位于第二超球面所构成的空间中的多数类样本重新确定第一样本集中。

可选地，第三样本满足以下条件：

$$x_m = \frac{x_i + x_k}{2}$$

$$x_{syn} = x_m + r \cdot v,$$

其中， x_{syn} 表示第三样本在欧式空间中的坐标， x_i 表示第一样本在欧式空间中的坐标， x_k 表示第二样本在欧式空间中的坐标； r 表示第一超球面的半径；

$$v = \{v^1, \dots, v^i, \dots, v^d\}, v^1 \in (-1, 1), v^i \in (-1, 1), v^d \in (-1, 1),$$

$$1 < i < d, \text{ 且 } \|v\|^2 < 1.$$

可选地，若平衡样本集中的样本数与多数类样本的样本数满足预设比例，则基于平衡样本集和多数类样本生成最终样本集，包括：

若平衡样本集中的样本数与多数类样本的样本数满足预设比例，确定每个多数类样本所分别对应的第二样本集，第二样本集中包括在初始样本集中距离单个多数类样本最近的 B 个样本，其中， B 为预设的整数；

根据第二样本集，从多数类样本中筛选安全样本，其中，安全样本所对应的 B 个样本中没有少数类样本；

基于安全样本和平衡样本集生成最终样本集。

本申请实施例提供了一种网络入侵检测装置，装置包括：

流量数据获取模块，用于获取待检测流量数据；

第一特征信息提取模块，用于提取待检测流量数据的第一特征信息；

第二特征信息提取模块，用于利用预先训练的特征提取模型提取第一特征信息中的第二特征信息，特征提取模型为多头自注意力网络模型；

第三特征信息提取模块，用于利用特征提取模型对第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；在每一轮循环中，特征提取模型的输入数据为上一轮的输出数据；

分类模块，用于对第三特征信息进行分类检测，得到待检测流量数据的检测结果。

本申请实施例提供一种电子设备，包括：处理器和存储器，处理器执行存储在存储器中的计算机程序，实现如第一方面的网络入侵检测方法。

本申请实施例提供一种可读存储介质，可读存储介质中存储有计算机指令，计算机指令被处理器执行时实现如第一方面的网络入侵检测方法。

本申请实施例包括以下优点：

综上，本申请实施例提供了一种网络入侵检测方法。在获取待检测流量数据之后，提取待检测流量数据的第一特征信息，利用预先训练的基于多头自注意力网络的特征提取模型提取第一特征信息中的第二特征信息，利用特征提取模型对

第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；在每一轮循环中，特征提取模型的输入数据为上一轮的输出数据；对第三特征信息进行分类检测，得到待检测流量数据的检测结果。在利用卷积神经网络提取流量数据局部特征的基础上，利用基于多头自注意力网络的特征提取模型可以有效学习到流量数据的依赖关系特征，而进一步基于该特征提取模型对第二特征信息的循环处理更可以提高依赖关系特征提取的准确性，从而可以有效提高流量数据分类检测的准确性，进而精确识别出网络流量数据中的异常流量，降低网络入侵带来的风险。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例的描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1示出了本申请实施例提供的一种网络入侵检测方法的流程图；

图2示出了本申请实施例提供的一种局部特征提取模型的架构图；

图3示出了本申请实施例提供的一种特征提取模型的架构图；

图4示出了本申请实施例提供的一种循环处理架构图；

图5示出了本申请实施例提供的一种样本处理方法的流程图；

图6示出了本申请实施例提供的一种特征提取模型的训练流程图；

图7示出了本申请实施例提供的另一种数据处理方法的流程图；

图8示出了本申请实施例提供的一种网络入侵检测装置的结构框图；

图9示出了本申请实施例提供的电子设备的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。并且，需要说明的是，本申请实施例中获取各种数据相关过程，都是在遵照所在地国家相应的数据保护政策法规的前提下，并获得由相应装置所有者给予授权的情况下进行的。

参照图1所示的本申请实施例提供的一种网络入侵检测方法的流程图，具体可以包括如下步骤：

步骤101、获取待检测流量数据。

流量数据是指网络中用于交互的传输数据。数据在交互过程中，异常的数据往往会导致网络入侵的风险大大提高，因此在进行数据交互过程中，首先需要对传输的数据进行检测，防止获取到异常的数据对本地网络的造成损害，对于获取流量数据的具体方式本申请不作限定。

步骤102、提取所述待检测流量数据的第一特征信息。

其中，第一特征信息是指待检测流量数据的局部特征信息。卷积神经网络、先检测后描述（detect-then-describe）等方法均可以用于提取局部特征，本申请对此不做限定。在本申请实施例中，利用基于卷积神经网络的局部特征提取模型提取第一特征信息。

考虑到流量数据的特征比较稀疏，为了便于后续模型的检测，可以对其进行

编码。在本申请实施例中使用嵌入 (embedding) 技术来对流量数据进行编码, 可以对流量数据进行向量化表示。通过嵌入, 待检测流量数据可以被表示为:

$$E = [e_1, e_2, \dots, e_i] \in R^{i \times n}, \quad (1)$$

其中, i 表示待检测流量数据所包含的字节数, n 表示嵌入向量的维度, e_i 表示第 i 个字节数据被编码后形成的向量。

参照图 2 所示的本申请实施例提供的一种局部特征提取模型的架构图, 在本申请实施例中, 局部特征提取模型包含两个卷积层和两个池化层, 以及一个全连接层。卷积层的输入是待检测流量数据编码后的矩阵, 其经过卷积层处理后可以得到以下结果:

$$h_j = f(h_{j-1} \otimes w_j + b_j), \quad (2)$$

其中, h_j 是第 j 层的特征图, $j=1,2,3\dots n$ 。 b_j 是第 j 层的偏置系数, $\otimes$ 是卷积运算操作, $f(x)$ 是激活函数, 本模型采用线性整流单元 (ReLU)。为了缩小特征图的大小以及避免过拟合问题, 因此在卷积层输出后, 紧接着将其输入到池化层, 表示为:

$$h_j = \text{pool}(h_{j-1}), \quad (3)$$

基于 CNN 的局部特征提取模型可以准确地提取待检测流量数据的局部特征, 可以为后续学习流量序列的依赖关系提供良好的数据基础。

步骤 103、利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息, 所述特征提取模型为多头自注意力网络模型。

参照图 3 所示的本申请实施例提供的一种特征提取模型的架构图, 在本申请实施例中, 采用基于多头自注意力机制的特征提取模型学习待检测流量数据的依赖关系特征即第二特征信息, 具体可以通过点积注意力机制计算注意力, 其中, 多头即 heads 用于表示自注意力计算的多个注意力头, Q (Query), K (Key), V (Value) 分别代表查询, 键, 值, 归一化指数函数是指 softmax 函数。在本申请实施例中, 特征提取模型的输入 Q 、 K 、 V 可以均为步骤 102 得到的待检测数据的第一特征信息, 也可以对第一特征信息进行特征增强、卷积等处理后再分别作为 Q 、 K 、 V , 本申请对此不作限定。

在将第一特征信息输入多头自注意力网络后, 可以按照如下公式计算多头自注意力网络的 Multi-head Attention :

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d}}\right) V, \quad (4)$$

$$H_i = \text{Attention}(QW_i^Q, KW_i^K, VW_i^V), \quad (5)$$

$$\text{Multihead}(Q, K, V) = \text{Concat}(H_1, \dots, H_i)W^O, \quad (6)$$

其中, $\sqrt{d}$ 表示通过点积自注意力 (Scaled Dot-Product Attention) 方式计算

注意力分数时的比例因子系数； H_i 代表多头注意力中第*i*个头的注意力计算结果， W_i^Q, W_i^K 和 W_i^V 则分别为对应于Q、K、V的转换矩阵，可以进行预先设置或通过预先训练得到；Concat（）表示多个注意力头之间的连接函数， W^O 表示计算Multihead(Q, K, V)的参数矩阵；Multihead(Q, K, V)表示多头自注意力网络的注意力计算结果，即第二特征信息。

利用在自注意力网络基础上利用多头自注意力网络构建特征提取模型，不仅可以充分学习流量序列的依赖关系特征，还可以改善常规的单头注意力单一计算的局限性，多头注意力的计算结果相互佐证，可以有效提高提取流量数据序列的依赖关系特征的准确率，从而提高对于异常流量数据识别的准确性，增强网络安全。

步骤104、利用所述特征提取模型对所述第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；在每一轮循环中，所述特征提取模型的输入数据为上一轮的输出数据。

考虑到流量数据间的复杂关系以及流量数据特征的稀疏性，为了提取流量数据更深层的序列特征，在本申请实施例中，通过堆叠自注意力块（self-attention blocks）基于第二特征信息进行进一步提取待检测流浪数据的第三特征信息。

参照图4所示的本申请实施例提供的一种循环处理架构图，其中，自注意力模型用于表示步骤103基于多头自注意力的特征提取模型，残差相加归一化表示add&norm的处理过程，用于防止由于深度所导致的模型退化问题，保证循环处理的效率不受影响。

在本申请实施例中，利用步骤103的特征提取模型对第二特征信息进行循环处理，即将第二特征信息继续输入特征提取模型进行循环处理，在每一轮循环中，特征提取模型的输入数据为上一轮的输出数据，直到满足循环退出条件时停止输入特征提取模型，最后将Z个自注意力块输出的特征信息经过前馈神经网络处理后，输出第三特征信息。

其中，Z为整数；循环退出条件可以为预先设定的Z次特征提取模型循环，即Z个自注意力块，也可以指第三特征信息达到了某种条件，本申请对此不作限定。

步骤105、对所述第三特征信息进行分类检测，得到所述待检测流量数据的检测结果。

在本申请中，可以利用softmax函数来输出流量类别的概率：

$$P = \sigma(F), \quad (7)$$

其中，F表示第三特征信息， σ 为softmax函数，它可以将前面第三特征信息转换为0-1之间的概率值；P是输出的概率矩阵，用于表示待检测流量数据被识别为对应类型流量的概率，例如当 $P=[0.6, 0.2, 0.1, 0.05, 0.05]$ ，对应的流量类型列表为[Normal, Dos, R2L, Probe, U2R]时，则表示输入的流量被识别为Normal的概率为0.6，Dos的概率为0.2，R2L的概率为0.1，Probe的概率为0.05，U2R的概率为0.05。当P中元素数据越大时，被识别为该类型流量的可能性就越大，例如上述P中最大的是0.6，对应的流量类型是Normal，那么可以认为待检测流量数据是正常的流量；若Dos的概率为0.7，则说明待检测流量数据为拒绝服务攻击流量数据，为异常流量数据。

通过上述方法,在利用卷积神经网络提取流量数据局部特征的基础上,利用基于多头自注意力网络的特征提取模型可以有效学习到流量数据的依赖关系特征,而基于该特征提取模型对第二特征信息的循环处理更可以提高依赖关系特征提取的准确性,从而可以有效提高流量数据分类的准确性,进而精确识别出网络流量数据中的异常流量,降低网络入侵带来的风险。

可选地,第一特征信息中包括至少一个第一特征矩阵;

步骤 103 所述利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息,包括:

步骤 S11、计算第一特征矩阵的稀疏度;

步骤 S12、基于第一特征矩阵的稀疏度,按照预设的稀疏度阈值从至少一个第一特征矩阵中筛选出 N 个连续的第一特征矩阵;

步骤 S13、利用预先训练的特征提取模型提取 N 个连续的第一特征矩阵中的第二特征信息;

其中,稀疏度表示为:

$$M(q_i, K) = \ln \sum_{j=1}^{L_K} e^{\frac{q_i k_j^T}{\sqrt{d}}} - \frac{1}{L_K} \sum_{j=1}^{L_K} \frac{q_i k_j^T}{\sqrt{d}}, \quad (8)$$

其中, M 表示第一特征信息中第 i 个第一特征矩阵 q_i 的稀疏度, L_K 表示第一特征信息中第一特征矩阵的个数, k_j 表示第一特征信息中第 j 个第一特征矩阵, $\sqrt{d}$ 表示比例因子系数, T 表示矩阵转置。

考虑到 Self-attention 的概率分布具有潜在的稀疏性,可以基于 KL 散度量第一特征信息中特征矩阵的稀疏性,再基于预设的稀疏度阈值筛选 N 个连续的第一特征矩阵作为步骤 103 的输入,即改进后的 Self-attention 的计算公式可以为:

$$Attention(Q, K, V) = \text{softmax}\left(\frac{\bar{Q}K^T}{\sqrt{d}}\right)V, \quad (9)$$

其中, $\bar{Q}$ 为经过评估函数 $M(q_i, K)$ 计算出来的 N 个连续的第一特征矩阵。

在保证了能够充分学习到待检测流量数据的依赖关系特征的基础上,改进后的 Self-attention 机制降低了时间复杂度和内存开销,提高了特征提取效率。

可选地,步骤 104 利用特征提取模型对第二特征信息进行循环处理,直至满足循环退出条件时得到第三特征信息,包括:

步骤 S21、对第二特征信息进行特征提取,得到待检测流量数据的第四特征信息;

步骤 S22、利用特征提取模型对第四特征信息进行循环处理,直至满足循环退出条件时得到第三特征信息;

其中,第四特征信息表示为:

$$F = \text{MaxPool}(\text{ELU}(\text{Conv1d}(S))) \quad (10)$$

F 表示第四特征信息, S 表示第二特征信息; Conv1d 表示一维卷积处理, ELU 表示激活函数, MaxPool 表示最大池化处理。

在本申请实施例中，将第二特征信息进行了“蒸馏”操作，即对第二特征信息一维卷积、激活处理和最大池化操作，有助于提取流量数据更深层的序列特征，并减少内存的使用。

可选地，步骤 103 所述利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息之前，所述方法还包括：

步骤 S31、获取初始样本集，所述初始样本集包括多数类样本和少数类样本，所述少数类样本构成平衡样本集；

步骤 S32、从所述少数类样本中抽取一个第一样本；

步骤 S33、从所述少数类样本中确定与所述第一样本的欧氏距离最近的第二样本；

步骤 S34、根据所述第一样本和所述第二样本构成的超球面中包含的多数类样本的样本数量调整所述平衡样本集；

步骤 S35、若所述平衡样本集中的样本数与所述多数类样本的样本数满足预设比例，则基于所述平衡样本集和所述多数类样本生成最终样本集；

步骤 S36、基于所述最终样本集对多头自注意力网络模型进行迭代训练，得到待检测数据的特征提取模型。

网络流量数据通常是由多数的正常流量和少数的异常流量组成，因此在通过标签过的流量数据训练特征提取模型时，多数类流量数据的预测精度可以得到提高，但少数类的预测精度会很低。

其中，多数类是指样本量大于其他类别的类别，少数类是相较于多数类样本数较少的类别，多数类样本和少数类样本用于描述不同类别之间样本量不平衡的问题。

参照如图 5 所示的本申请实施例提供的一种样本处理方法的流程图，为了平衡多数类和少数类流量数据通过插值生成新的样本，首先将初始样本集中的样本映射到欧氏空间中，并从少数类样本抽取第一样本，考虑到噪声样本的影响，在本申请实施例中，从少数类样本中确定与第一样本的欧氏距离最近的第二样本，然后以第一样本和第二样本构建第一超球面，具体地，可以以第一样本与第二样本之间的欧氏距离为直径，以第一样本和第二样本连线的中心为圆心构建第一超球面。再在第一超球面构成的空间内进行插值，从而生成新的属于少数类的样本即第三样本。

本申请通过将第三样本添加到包括初始的少数类样本的平衡样本集中，在平衡样本集中的样本数与多数类样本的样本数满足预设比例的情况下，基于平衡样本集和多数类样本生成最终样本集，最后基于最终样本集对多头自注意力网络模型进行迭代训练，得到待检测数据的特征提取模型。其中，预设比例可以根据实际情况确定，本申请不作限定。

参照如图 6 所示的本申请实施例提供的一种特征提取模型的训练流程图，在对初始样本集进行如图 5 所示的样本平衡处理后，将最终样本集进行编码、归一化进而得到矩阵形式的最终样本集，可以按照一定比例将样本集划分为训练集和测试集，考虑到在步骤 102 中，可以利用基于卷积神经网络的局部特征提取模型提取第一特征信息，因此可以利用训练集中的训练样本对步骤 102 的局部特征提取模型和步骤 103 基于自注意力网络的特征提取模型进行统一训练，然后利用测试集中的测试样本对训练好的模型进行测试。

可选地，所述方法还包括：

步骤 S37、若所述平衡样本集中的样本数与所述多数类样本的样本数不满足

所述预设比例, 则从所述少数类样本中重新抽取第一样本, 并基于重新抽取的第一样本重新调整所述平衡样本集, 其中, 每个少数类样本只能被抽取一次。

为了保证新生成的样本分布均匀, 在一个超球面内不适合生成过多的新样本即第三样本, 因此在本申请实施例中, 通过从少数类样本中反复抽取不同的第一样本来构建不同的第一超球面, 并在不同的第一超球面内插值生成第三样本, 直到平衡样本集中的样本数与多数类样本的样本数满足预设比例。

可选地, 步骤 S34 所述根据所述第一样本和所述第二样本构成的超球面中包含的多数类样本的样本数量调整所述平衡样本集, 包括:

步骤 S41、基于第一样本和第二样本构建第一超球面;

步骤 S42、将位于第一超球面所构成的空间中的多数类样本添加到第一样本集中;

步骤 S43、若第一样本集为空集, 则在第一超球面所构成的空间中生成一个第三样本, 并将第三样本添加到平衡样本集中。

参照如图 7 所示的本申请实施例提供的另一种数据处理方法的流程图, 其中, D 表示初始样本集, D⁻表示少数类样本, D⁺表示多数类样本, x_i 表示第一样本, x_k 表示第二样本, CS 表示第一样本集, C 表示第一超球面。

为了保证训练样本的平衡性, 确保新生成的第三样本的类别为少数类, 那么第一超球面构成的空间中不能落入多数类样本, 因此只有在第一超球面所构成的空间中无多数类样本即第一样本集为空集的情况下, 可以在第一超球面所构成的空间中生成一个第三样本, 并将第三样本添加到平衡样本集中。

可选地, 方法还包括:

步骤 S51、若第一样本集不为空集, 则从第一样本集中确定与第一样本的欧氏距离最近的第四样本;

步骤 S52、基于第一样本和第四样本构建第二超球面;

步骤 S53、根据位于第二超球面所构成的空间中的多数类样本重新确定第一样本集中。

参照如图 7 所示的本申请实施例提供的另一种数据处理方法的流程图, 其中, y_p 表示第四样本, C_n 表示第 n 个第二超球面, n 为整数。

若是第一超球面所构成的空间中存在多数类样本, 即第一样本集不为空集, 则需要从第一样本集中确定与第一样本的欧氏距离最近的多数类样本即第四样本, 再根据第一样本和第四样本构建第二超球面, 然后根据第二超球面所构成的空间中的多数类样本重新确定第一样本集, 若第一样本集仍然不为空集则继续执行步骤 S51-S53, 直到第一样本集为空集, 从而确保多数类样本不会对新生成的第三样本产生干扰。

可选地, 第三样本满足以下条件:

$$x_m = \frac{x_i + x_k}{2}$$

$$x_{syn} = x_m + r \cdot v, \quad (11)$$

其中, x_{syn} 表示第三样本在欧式空间中的坐标, x_i 表示第一样本在欧式空间中的坐标, x_k 表示第二样本在欧式空间中的坐标; r 表示第一超球面的半径;

$$v = \{v^1, \dots, v^i, \dots, v^d\}, v^1 \in (-1, 1), v^i \in (-1, 1), v^d \in (-1, 1),$$

$$1 < i < d, \text{ 且 } \|v\|^2 < 1.$$

当然，在如步骤 S51-S53 所示的情况下，公式 (10) 中的 x_k 可以替换为内部空间中无多数类样本的第二超球面所对应的第四样本点 y_p 。

为了新生成的第三样本的随机性，在确定了超球面后，可以在超球面内的任意位置生成第三样本，因此， v^1, v^i, v^d 均可以为 -1 到 1 之间的随机数。

可选地，若平衡样本集中的样本数与多数类样本的样本数满足预设比例，则基于平衡样本集和多数类样本生成最终样本集，包括：

步骤 S61、若平衡样本集中的样本数与多数类样本的样本数满足预设比例，确定每个多数类样本所分别对应的第二样本集，第二样本集中包括在初始样本集中距离单个多数类样本最近的 B 个样本，其中， B 为预设的整数；

步骤 S62、根据第二样本集，从多数类样本中筛选安全样本，其中，安全样本所对应的 B 个样本中没有少数类样本；

步骤 S63、基于安全样本和平衡样本集生成最终样本集。

参照如图 7 所示的本申请实施例提供的另一种数据处理方法的流程图，考虑到多数类样本可能存在噪声样本会对模型训练产生影响，因此，可以利用聚类计算每个多数类样本与初始样本集中其他样本的欧氏距离，并从中确定每个多数类样本所对应的第二样本集，即单个多数类样本所对应的欧氏距离最近的 B 个样本。

可以根据 B 个样本的类别构成确定 B 个样本所对应的多数类样本的属性。具体地，以多数类样本 A 为例，若 A 对应的 B 个样本均属于多数类，则可以确定 A 为安全样本，可以用于模型训练；若 A 对应的 B 个样本均属于少数类，则可以确定 A 为噪声样本；若 A 对应的 B 个样本中既有多数类样本也有少数类样本，那么可以确定 A 为边界样本。

考虑到边界样本和噪声样本均可能对模型训练造成干扰，所以仅保留安全样本与平衡样本集构成最终样本集，以保证训练样本的可靠性。在本实施例中，平衡样本集的生成方法不限于如图 7 所示的方法。

综上，本申请实施例提供了一种网络入侵检测方法。在获取待检测流量数据之后，提取待检测流量数据的第一特征信息，利用预先训练的基于多头自注意力网络的特征提取模型提取第一特征信息中的第二特征信息，利用特征提取模型对第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；在每一轮循环中，特征提取模型的输入数据为上一轮的输出数据；对第三特征信息进行分类检测，得到待检测流量数据的检测结果。在利用卷积神经网络提取流量数据局部特征的基础上，利用基于多头自注意力网络的特征提取模型可以有效学习到流量数据的依赖关系特征，而进一步基于该特征提取模型对第二特征信息的循环处理更可以提高依赖关系特征提取的准确性，从而可以有效提高流量数据分类的准确性，进而精确识别出网络流量数据中的异常流量，降低网络入侵带来的风险。

参照图 8，所示的本申请实施例提供的一种网络入侵检测装置的结构框图，装置 200 可以包括：

流量数据获取模块 201，用于获取待检测流量数据；

第一特征信息提取模块 202, 用于提取待检测流量数据的第一特征信息;

第二特征信息提取模块 203, 用于利用预先训练的特征提取模型提取第一特征信息中的第二特征信息, 特征提取模型为多头自注意力网络模型;

第三特征信息提取模块 204, 用于利用特征提取模型对第二特征信息进行循环处理, 直至满足循环退出条件时得到第三特征信息; 在每一轮循环中, 特征提取模型的输入数据为上一轮的输出数据;

分类模块 205, 用于对第三特征信息进行分类检测, 得到待检测流量数据的检测结果。

可选地, 第一特征信息中包括至少一个第一特征矩阵;

第二特征信息提取模块包括:

稀疏度计算子模块, 用于计算第一特征矩阵的稀疏度;

筛选子模块, 用于基于第一特征矩阵的稀疏度, 按照预设的稀疏度阈值从至少一个第一特征矩阵中筛选出 N 个连续的第一特征矩阵;

第二特征信息提取子模块, 用于利用预先训练的特征提取模型提取 N 个连续的第一特征矩阵中的第二特征信息;

其中, 稀疏度表示为:

$$M(q_i, K) = \ln \sum_{j=1}^{L_K} e^{\frac{q_i k_j^T}{\sqrt{d}}} - \frac{1}{L_K} \sum_{j=1}^{L_K} \frac{q_i k_j^T}{\sqrt{d}},$$

其中, M 表示第一特征信息中第 i 个第一特征矩阵 q_i 的稀疏度, L_K 表示第一特征信息中第一特征矩阵的个数, k_j 表示第一特征信息中第 j 个第一特征矩阵, $\sqrt{d}$ 表示比例因子系数, T 表示矩阵转置。

可选地, 第三特征信息提取模块, 包括:

第四特征信息提取子模块, 用于对第二特征信息进行特征提取, 得到待检测流量数据的第四特征信息;

第三特征信息提取子模块, 用于利用特征提取模型对第四特征信息进行循环处理, 直至满足循环退出条件时得到第三特征信息;

其中, 第四特征信息表示为:

$$F = \text{MaxPool}(\text{ELU}(\text{Conv1d}(S)))$$

F 表示第四特征信息, S 表示第二特征信息; Conv1d 表示一维卷积处理, ELU 表示激活函数, MaxPool 表示最大池化处理。

可选地, 装置还可以包括:

初始样本集获取模块, 用于在利用预先训练的特征提取模型提取第一特征信息中的第二特征信息之前, 获取初始样本集, 初始样本集包括多数类样本和少数类样本, 少数类样本构成平衡样本集;

样本抽取模块, 用于从少数类样本中抽取一个第一样本;

第二样本确定模块, 用于从少数类样本中确定与第一样本的欧氏距离最近的第二样本;

平衡样本集调整模块, 用于根据第一样本和第二样本构成的超球面中包含的多数类样本的样本数量调整平衡样本集;

最终样本集生成模块,用于若平衡样本集中的样本数与多数类样本的样本数满足预设比例,则基于平衡样本集和多数类样本生成最终样本集;

训练模块,用于基于最终样本集对多头自注意力网络模型进行迭代训练,得到待检测数据的特征提取模型。

可选地,装置还可以包括:

第一循环模块,用于若平衡样本集中的样本数与多数类样本的样本数不满足预设比例,则从少数类样本中重新抽取第一样本,并基于重新抽取的第一样本重新调整平衡样本集,其中,每个少数类样本只能被抽取一次。

可选地,平衡样本集调整模块,可以包括:

第一超球面构建子模块,用于基于第一样本和第二样本构建第一超球面;

第一样本集更新子模块,用于将位于第一超球面所构成的空间中的多数类样本添加到第一样本集中;

第三样本生成子模块,用于若第一样本集为空集,则在第一超球面所构成的空间中生成一个第三样本,并将第三样本添加到平衡样本集中。

可选地,平衡样本集调整模块,还可以包括

第四样本确定子模块,用于若第一样本集不为空集,则从第一样本集中确定与第一样本的欧氏距离最近的第四样本;

第二超球面构建子模块,用于基于第一样本和第四样本构建第二超球面;

第二循环子模块,用于根据位于第二超球面所构成的空间中的多数类样本重新确定第一样本集中。

可选地,第三样本满足以下条件:

$$x_m = \frac{x_i + x_k}{2}$$

$$x_{syn} = x_m + r \cdot v,$$

其中, x_{syn} 表示第三样本在欧式空间中的坐标, x_i 表示第一样本在欧式空间中的坐标, x_k 表示第二样本在欧式空间中的坐标; r 表示第一超球面的半径;

$$v = \{v^1, \dots, v^i, \dots, v^d\}, v^1 \in (-1, 1), v^i \in (-1, 1), v^d \in (-1, 1),$$

$$1 < i < d, \text{ 且 } \|v\|^2 < 1。$$

可选地,最终样本集生成模块,可以包括:

第二样本集确定子模块,用于若平衡样本集中的样本数与多数类样本的样本数满足预设比例,确定每个多数类样本所分别对应的第二样本集,第二样本集中包括在初始样本集中距离单个多数类样本最近的 B 个样本,其中, B 为预设的整数;

安全样本筛选子模块,用于根据第二样本集,从多数类样本中筛选安全样本,其中,安全样本所对应的 B 个样本中没有少数类样本;

最终样本集生成子模块,用于基于安全样本和平衡样本集生成最终样本集。

参照图 9,电子设备 700 可以包括以下一个或多个组件:处理组件 702,存储器 704,电源组件 706,多媒体组件 708,音频组件 710,输入/输出(I/O),

Input/Output, 输入/输出) 的接口 712, 传感器组件 714, 以及通信组件 716。

处理组件 702 通常控制电子设备 700 的整体操作, 诸如与显示, 电话呼叫, 数据通信, 相机操作和记录操作相关联的操作。处理元件 702 可以包括一个或多个处理器 720 来执行指令, 以完成上述的网络入侵检测方法的全部或部分步骤。此外, 处理组件 702 可以包括一个或多个模块, 便于处理组件 702 和其他组件之间的交互。例如, 处理组件 702 可以包括多媒体模块, 以方便多媒体组件 708 和处理组件 702 之间的交互。

存储器 704 被配置为存储各种类型的数据以支持在电子设备 700 的操作。这些数据的示例包括用于在电子设备 700 上操作的任何应用程序或方法的指令, 联系人数据, 电话簿数据, 消息, 图片, 视频等。存储器 704 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现, 如静态随机存取存储器 (Static RAM, 简称 SRAM), 电可擦除可编程只读存储器 (Electrically Erasable Programmable read only memory, 简称 EEPROM), 可擦除可编程只读存储器 (Erasable Programmable Read Only Memory, 简称 EPROM), 可编程只读存储器 (Programmable Read Only Memory, 简称 PROM), 只读存储器 (Read Only Memory, 简称 ROM), 磁存储器, 快闪存储器, 磁盘或光盘。

电源组件 706 为电子设备 700 的各种组件提供电力。电源组件 706 可以包括电源管理系统, 一个或多个电源, 及其他与为电子设备 700 生成、管理和分配电力相关联的组件。

多媒体组件 708 包括在电子设备 700 和用户之间的提供一个输出接口的屏幕。在一些实施例中, 屏幕可以包括液晶显示器 (Liquid Crystal Display, 简称 LCD) 和触摸面板 (Touch Panel, 简称 TP)。如果屏幕包括触摸面板, 屏幕可以被实现为触摸屏, 以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。触摸传感器可以不仅感测触摸或滑动动作的边界, 而且还检测与触摸或滑动操作相关的持续时间和压力。在一些实施例中, 多媒体组件 708 包括一个前置摄像头和/或后置摄像头。当电子设备 700 处于操作模式, 如拍摄模式或视频模式时, 前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

音频组件 710 被配置为输出和/或输入音频信号。例如, 音频组件 710 包括一个麦克风 (Microphone, 简称 MIC), 当电子设备 700 处于操作模式, 如呼叫模式、记录模式和语音信息处理模式时, 麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 704 或经由通信组件 716 发送。在一些实施例中, 音频组件 710 还包括一个扬声器, 用于输出音频信号。

I/O 接口 712 为处理组件 702 和外围接口模块之间提供接口, 上述外围接口模块可以是键盘, 点击轮, 按钮等。这些按钮可包括但不限于: 主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 714 包括一个或多个传感器, 用于为电子设备 700 提供各个方面的状态评估。例如, 传感器组件 714 可以检测到电子设备 700 的打开/关闭状态, 组件的相对定位, 例如组件为装置 700 的显示器和小键盘, 传感器组件 714 还可以检测电子设备 700 或电子设备 700 一个组件的位置改变, 用户与电子设备 700 接触的存在或不存在, 电子设备 700 方位或加速/减速和电子设备 700 的温度变化。传感器组件 714 可以包括接近传感器, 被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 714 还可以包括光传感器, 如 CMOS

(Complementary Metal Oxide Semiconductor, 互补金属氧化物半导体) 或 CCD (Charge-coupled Device, 电荷耦合元件) 图像传感器, 用于在成像应用中使用。在一些实施例中, 该传感器组件 714 还可以包括加速度传感器, 陀螺仪传感器, 磁传感器, 压力传感器或温度传感器。

通信组件 716 被配置为便于电子设备 700 和其他设备之间有线或无线方式的通信。电子设备 700 可以接入基于通信标准的无线网络, 如 WiFi, 2G 或 3G, 或它们的组合。在一个示例性实施例中, 通信组件 716 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中, 通信组件 716 还包括近场通信 (Near Field Communication, 简称 NFC) 模块, 以促进短程通信。例如, 在 NFC 模块可基于射频信息处理 (Radio Frequency Identification, 简称 RFID) 技术, 红外数据协会 (Infrared Data Association, 简称 IrDA) 技术, 超宽带 (Ultra Wide Band, 简称 UWB) 技术, 蓝牙 (BlueTooth, 简称 BT) 技术和其他技术来实现。

在示例性实施例中, 电子设备 700 可以被一个或多个应用专用集成电路 (Application Specific Integrated Circuit, 简称 ASIC)、数字信号处理器 (Digital Signal Processing, 简称 DSP)、数字信号处理设备 (Digital Signal Processing Device, 简称 DSPD)、可编程逻辑器件 (Programmable Logic Device, 简称 PLD)、现场可编程门阵列 (Field Programmable Gate Array, 简称 FPGA)、控制器、微控制器、微处理器或其他电子元件实现, 用于执行上述网络入侵检测方法。

在示例性实施例中, 还提供了一种包括指令的非临时性计算机可读存储介质, 例如包括指令的存储器 704, 上述指令可由电子设备 700 的处理器 720 执行以完成上述网络入侵检测方法。例如, 非临时性计算机可读存储介质可以是 ROM、随机存取存储器 (Random Access Memory, 简称 RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

一种非临时性计算机可读存储介质, 当存储介质中的指令由电子设备 (服务器或者终端) 的处理器执行时, 使得处理器能够执行前文的网络入侵检测方法。

本说明书中各个实施例采用递进的方式描述, 每个实施例重点说明的都是与其它实施例的不同之处, 各个实施例之间相同或相似部分互相参见即可。对于实施例公开的装置而言, 由于其与实施例公开的方法相对应, 所以描述的比较简单, 相关之处参见方法部分说明即可。

最后, 还需要说明的是, 在本文中, 诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来, 而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且, 术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性地包含, 从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素, 而且还包括没有明确列出的其他要素, 或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下, 由语句“包括一个……”限定的要素, 并不排除在包括要素的过程、方法、物品或者设备中还存在另外的相同要素。

以上对本申请所提供的一种网络入侵检测方法、装置、电子设备和可读存储介质进行了详细介绍, 本文中应用了具体个例对本申请的原理及实施方式进行了阐述, 以上实施例的说明只是用于帮助理解本申请的方法及其核心思想; 同时, 对于本领域的一般技术人员, 依据本申请的思想, 在具体实施方式及应用范围上均会有改变之处, 综上, 本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1、一种网络入侵检测方法，其特征在于，所述方法包括：

获取待检测流量数据；

提取所述待检测流量数据的第一特征信息；

利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息，所述特征提取模型为多头自注意力网络模型；

利用所述特征提取模型对所述第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；在每一轮循环中，所述特征提取模型的输入数据为上一轮的输出数据；

对所述第三特征信息进行分类检测，得到所述待检测流量数据的检测结果。

2、根据权利要求1所述的方法，其特征在于，所述第一特征信息中包括至少一个第一特征矩阵；

所述利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息，包括：

计算所述第一特征矩阵的稀疏度；

基于所述第一特征矩阵的稀疏度，按照预设的稀疏度阈值从所述至少一个第一特征矩阵中筛选出N个连续的第一特征矩阵；

利用预先训练的特征提取模型提取所述N个连续的第一特征矩阵中的第二特征信息；

其中，所述稀疏度表示为：

$$M(q_i, K) = \ln \sum_{j=1}^{L_K} e^{\frac{q_i k_j^T}{\sqrt{d}}} - \frac{1}{L_K} \sum_{j=1}^{L_K} \frac{q_i k_j^T}{\sqrt{d}},$$

其中，M表示所述第一特征信息中第i个第一特征矩阵 q_i 的稀疏度， L_K 表示所述第一特征信息中第一特征矩阵的个数， k_j 表示所述第一特征信息中第j个第一特征矩阵， $\sqrt{d}$ 表示比例因子系数，T表示矩阵转置。

3、根据权利要求1所述的方法，其特征在于，所述利用所述特征提取模型对所述第二特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息，包括：

对所述第二特征信息进行特征提取，得到所述待检测流量数据的第四特征信息；

利用所述特征提取模型对所述第四特征信息进行循环处理，直至满足循环退出条件时得到第三特征信息；

其中，所述第四特征信息表示为：

$$F = \text{MaxPool}(\text{ELU}(\text{Conv1d}(S)))$$

F表示所述第四特征信息，S表示所述第二特征信息；Conv1d表示一维卷积处理，ELU表示激活函数，MaxPool表示最大池化处理。

4、根据权利要求1所述的方法，其特征在于，所述利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息之前，所述方法还包括：

获取初始样本集，所述初始样本集包括多数类样本和少数类样本，所述少数

类样本构成平衡样本集；

从所述少数类样本中抽取一个第一样本；

从所述少数类样本中确定与所述第一样本的欧氏距离最近的第二样本；

根据所述第一样本和所述第二样本构成的超球面中包含的多数类样本的样本数量调整所述平衡样本集；

若所述平衡样本集中的样本数与所述多数类样本的样本数满足预设比例，则基于所述平衡样本集和所述多数类样本生成最终样本集；

基于所述最终样本集对多头自注意力网络模型进行迭代训练，得到待检测数据的特征提取模型。

5、根据权利要求4所述方法，其特征在于，所述方法还包括：

若所述平衡样本集中的样本数与所述多数类样本的样本数不满足所述预设比例，则从所述少数类样本中重新抽取第一样本，并基于重新抽取的第一样本重新调整所述平衡样本集，其中，每个少数类样本只能被抽取一次。

6、根据权利要求4所述的方法，其特征在于，所述根据所述第一样本和所述第二样本构成的超球面中包含的多数类样本的样本数量调整所述平衡样本集，包括：

基于所述第一样本和所述第二样本构建第一超球面；

将位于所述第一超球面所构成的空间中的多数类样本添加到第一样本集中；

若所述第一样本集为空集，则在所述第一超球面所构成的空间中生成一个第三样本，并将所述第三样本添加到所述平衡样本集中。

7、根据权利要求6所述的方法，其特征在于，所述方法还包括：

若所述第一样本集不为空集，则从所述第一样本集中确定与所述第一样本的欧氏距离最近的第四样本；

基于所述第一样本和所述第四样本构建第二超球面；

根据位于所述第二超球面所构成的空间中的多数类样本重新确定第一样本集中。

8、根据权利要求6所述的方法，其特征在于，所述第三样本满足以下条件：

$$x_m = \frac{x_i + x_k}{2}$$

$$x_{syn} = x_m + r \cdot v$$

其中， x_{syn} 表示第三样本在欧式空间中的坐标， x_i 表示第一样本在欧式空间中的坐标， x_k 表示第二样本在欧式空间中的坐标； r 表示所述第一超球面的半径；

$$v = \{v^1, \dots, v^i, \dots, v^d\}, v^1 \in (-1, 1), v^i \in (-1, 1), v^d \in (-1, 1),$$

$$1 < i < d, \text{ 且 } \|v\|^2 < 1。$$

9、根据权利要求4所述的方法，其特征在于，所述若所述平衡样本集中的样本数与所述多数类样本的样本数满足预设比例，则基于所述平衡样本集和所述多数类样本生成最终样本集，包括：

若所述平衡样本集中的样本数与所述多数类样本的样本数满足预设比例，确

定每个多数类样本所分别对应的第二样本集,所述第二样本集中包括在所述初始样本集中距离单个多数类样本最近的 B 个样本,其中, B 为预设的整数;

根据所述第二样本集,从所述多数类样本中筛选安全样本,其中,所述安全样本所对应的 B 个样本中没有少数类样本;

基于所述安全样本和所述平衡样本集生成最终样本集。

10、一种网络入侵检测装置,其特征在于,所述装置包括:

流量数据获取模块,用于获取待检测流量数据;

第一特征信息提取模块,用于提取所述待检测流量数据的第一特征信息;

第二特征信息提取模块,用于利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息,所述特征提取模型为多头自注意力网络模型;

第三特征信息提取模块,用于利用所述特征提取模型对所述第二特征信息进行循环处理,直至满足循环退出条件时得到第三特征信息;在每一轮循环中,所述特征提取模型的输入数据为上一轮的输出数据;

分类模块,用于对所述第三特征信息进行分类检测,得到所述待检测流量数据的检测结果。

11、根据权利要求 10 所述的装置,其特征在于,所述第一特征信息中包括至少一个第一特征矩阵;

所述第二特征信息提取模块包括:

稀疏度计算子模块,用于计算所述第一特征矩阵的稀疏度;

筛选子模块,用于基于所述第一特征矩阵的稀疏度,按照预设的稀疏度阈值从所述至少一个第一特征矩阵中筛选出 N 个连续的第一特征矩阵;

第二特征信息提取子模块,用于利用预先训练的特征提取模型提取所述 N 个连续的第一特征矩阵中的第二特征信息;

其中,所述稀疏度表示为:

$$M(q_i, K) = \ln \sum_{j=1}^{L_K} e^{\frac{q_i k_j^T}{\sqrt{d}}} - \frac{1}{L_K} \sum_{j=1}^{L_K} \frac{q_i k_j^T}{\sqrt{d}},$$

其中, M 表示所述第一特征信息中第 i 个第一特征矩阵 q_i 的稀疏度, L_K 表示所述第一特征信息中第一特征矩阵的个数, k_j 表示所述第一特征信息中第 j 个第一特征矩阵, $\sqrt{d}$ 表示比例因子系数, T 表示矩阵转置。

12、根据权利要求 10 所述的装置,其特征在于,所述装置还包括:

初始样本集获取模块,用于在利用预先训练的特征提取模型提取所述第一特征信息中的第二特征信息之前,获取初始样本集,所述初始样本集包括多数类样本和少数类样本,所述少数类样本构成平衡样本集;

样本抽取模块,用于从所述少数类样本中抽取一个第一样本;

第二样本确定模块,用于从所述少数类样本中确定与所述第一样本的欧式距离最近的第二样本;

平衡样本集调整模块,用于根据所述第一样本和所述第二样本构成的超球面中包含的多数类样本的样本数量调整所述平衡样本集;

最终样本集生成模块,用于若所述平衡样本集中的样本数与所述多数类样本的样本数满足预设比例,则基于所述平衡样本集和所述多数类样本生成最终样本

集；

训练模块，用于基于所述最终样本集对多头自注意力网络模型进行迭代训练，得到待检测数据的特征提取模型。

13、根据权利要求 12 所述的装置，其特征在于，所述最终样本集生成模块，包括：

第二样本集确定子模块，用于若所述平衡样本集中的样本数与所述多数类样本的样本数满足预设比例，确定每个多数类样本所分别对应的第二样本集，所述第二样本集中包括在所述初始样本集中距离单个多数类样本最近的 B 个样本，其中， B 为预设的整数；

安全样本筛选子模块，用于根据所述第二样本集，从所述多数类样本中筛选安全样本，其中，所述安全样本所对应的 B 个样本中没有少数类样本；

最终样本集生成子模块，用于基于所述安全样本和所述平衡样本集生成最终样本集。

14、一种电子设备，其特征在于，包括：处理器和存储器，所述处理器执行存储在所述存储器中的计算机程序，实现权利要求 1 至 9 中任一项所述的网络入侵检测方法。

15、一种可读存储介质，其特征在于，当所述存储介质中的指令由装置的处理器的执行时，使得装置能够执行如方法权利要求 1 至 9 中任一所述的网络入侵检测方法。

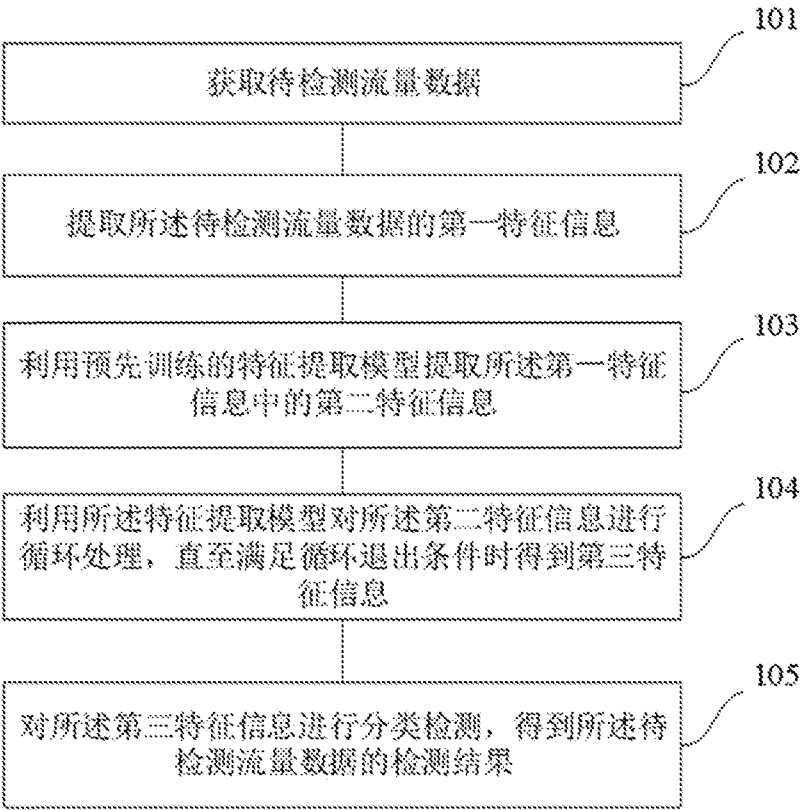


图 1

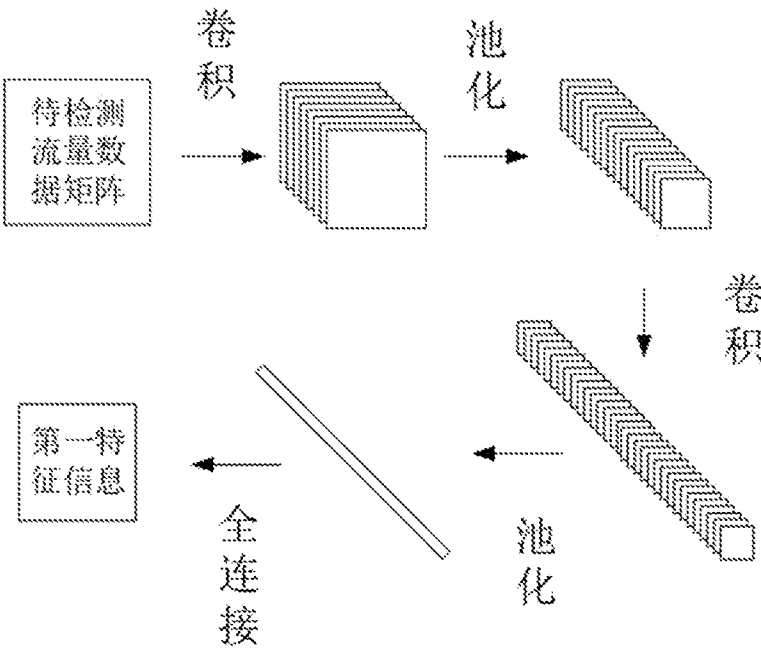


图 2

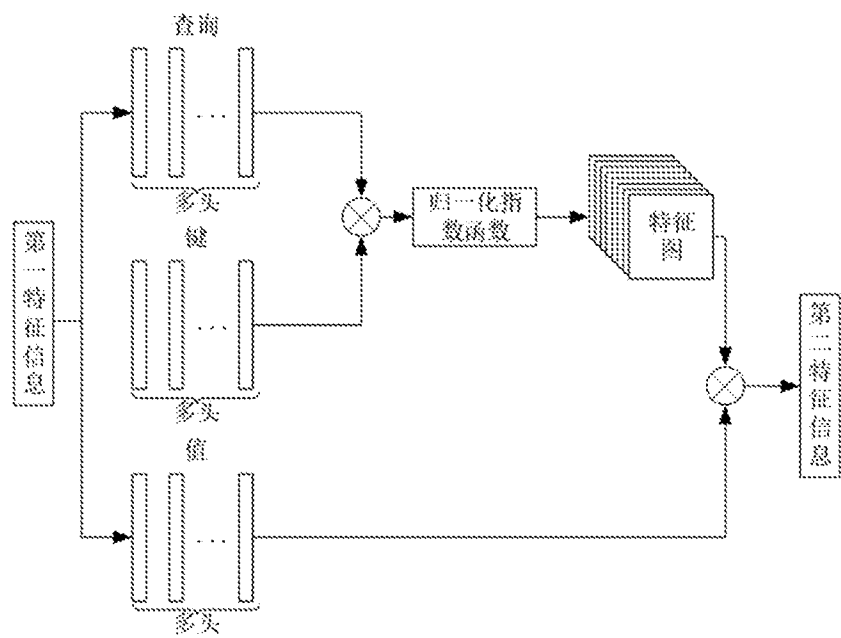


图 3

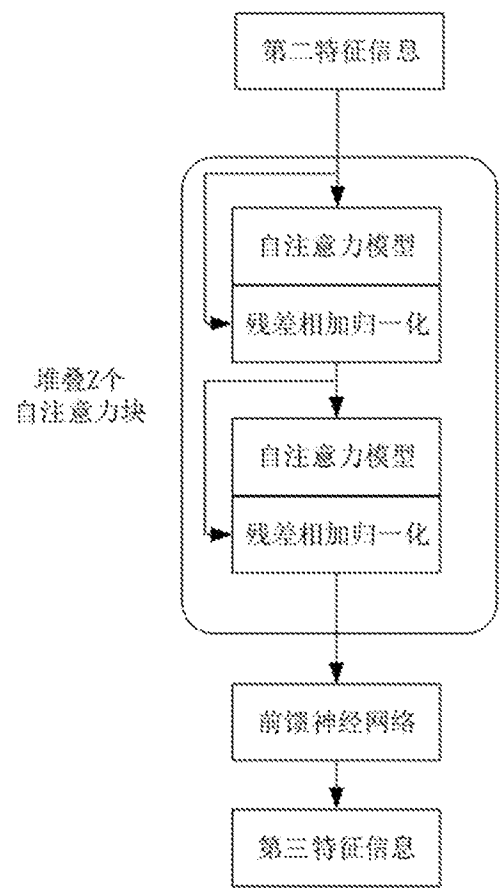


图 4

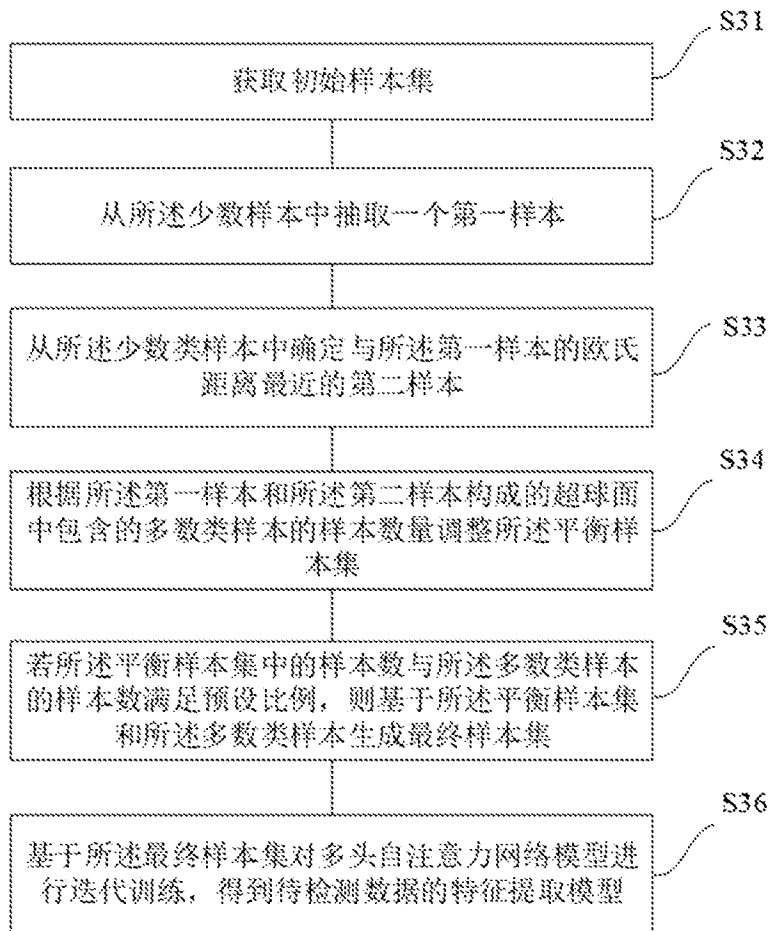


图 5

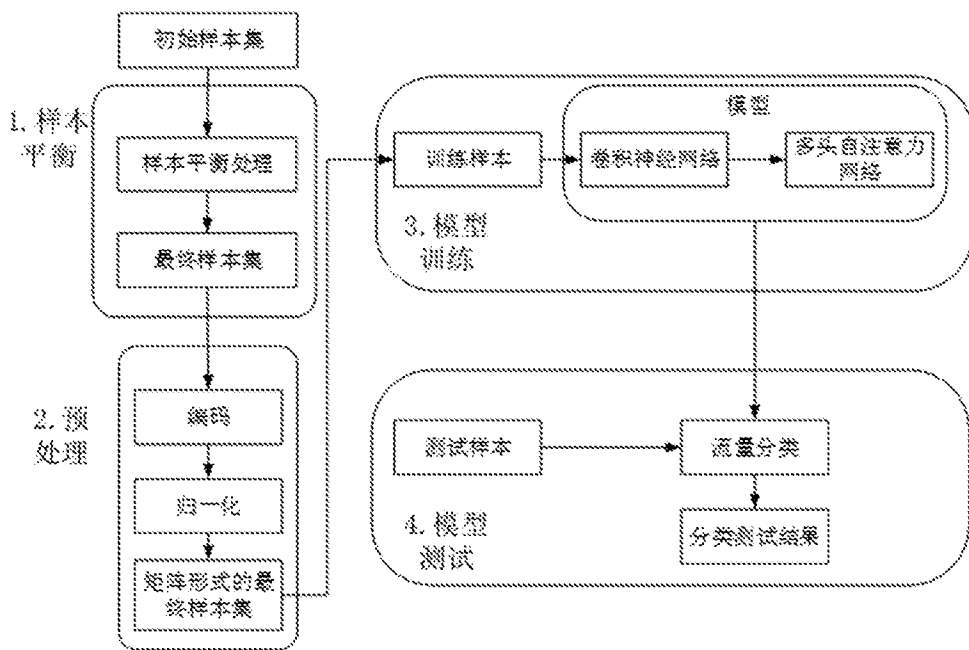


图 6

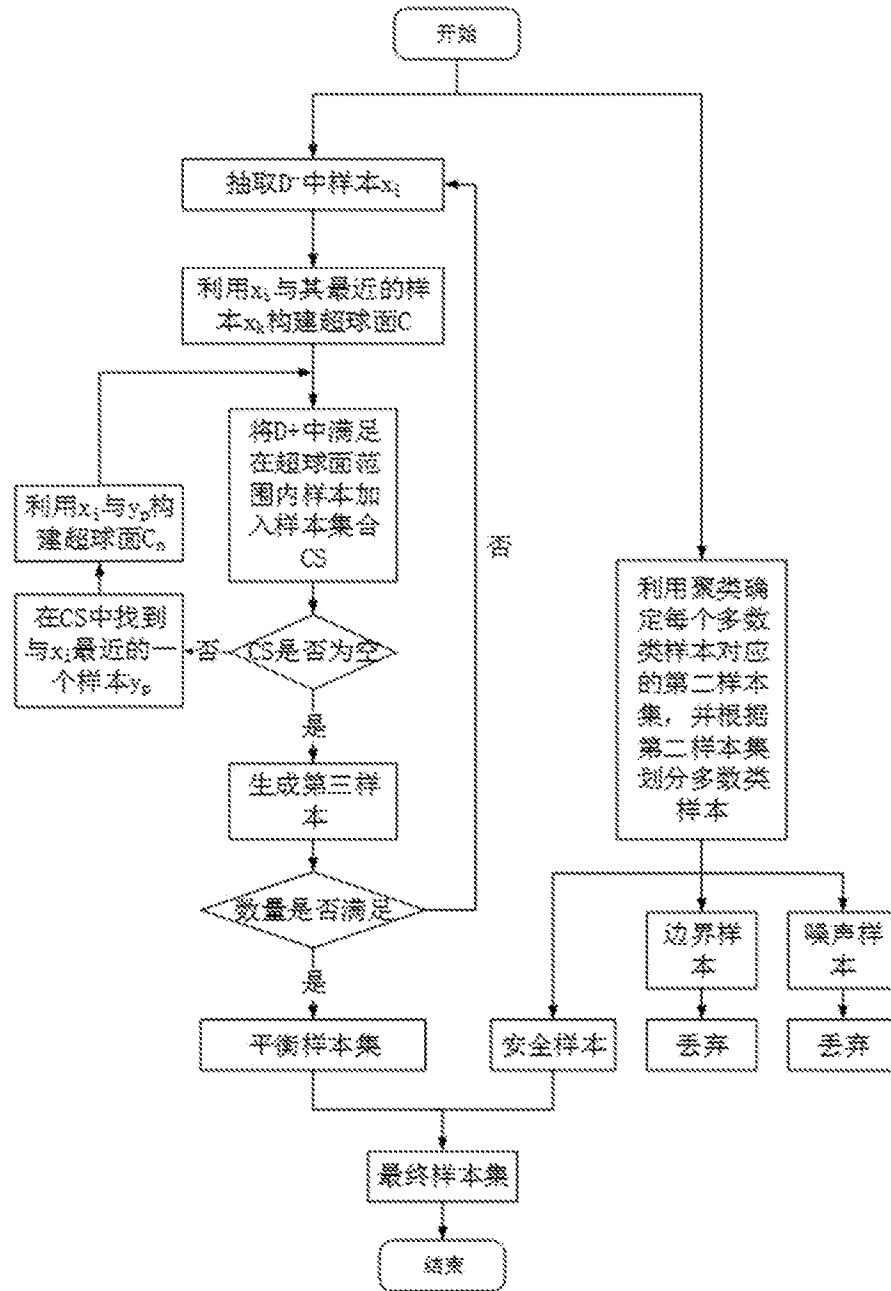


图 7

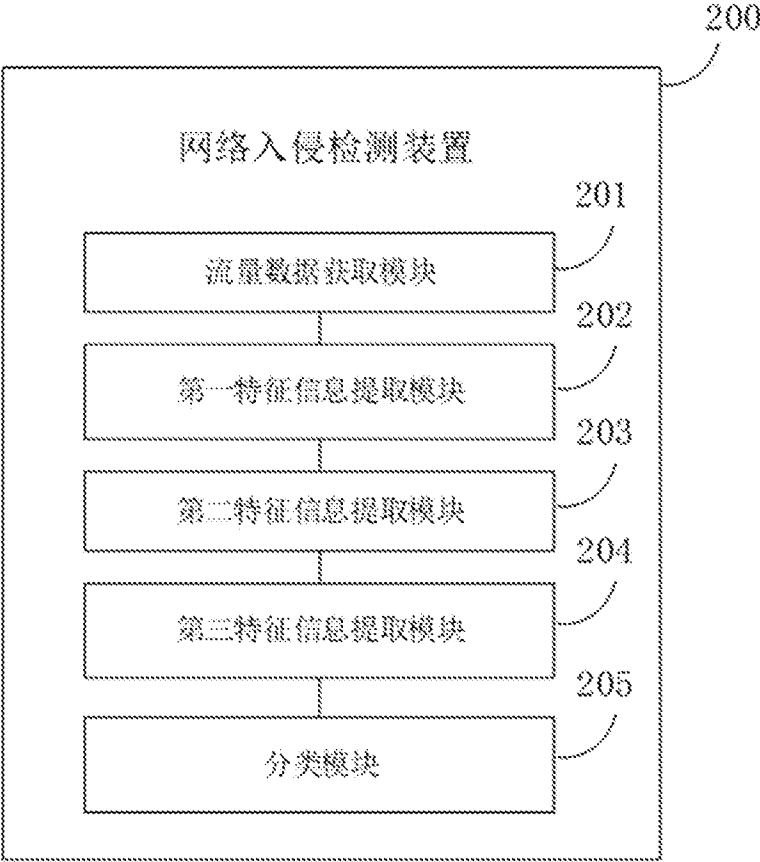


图 8

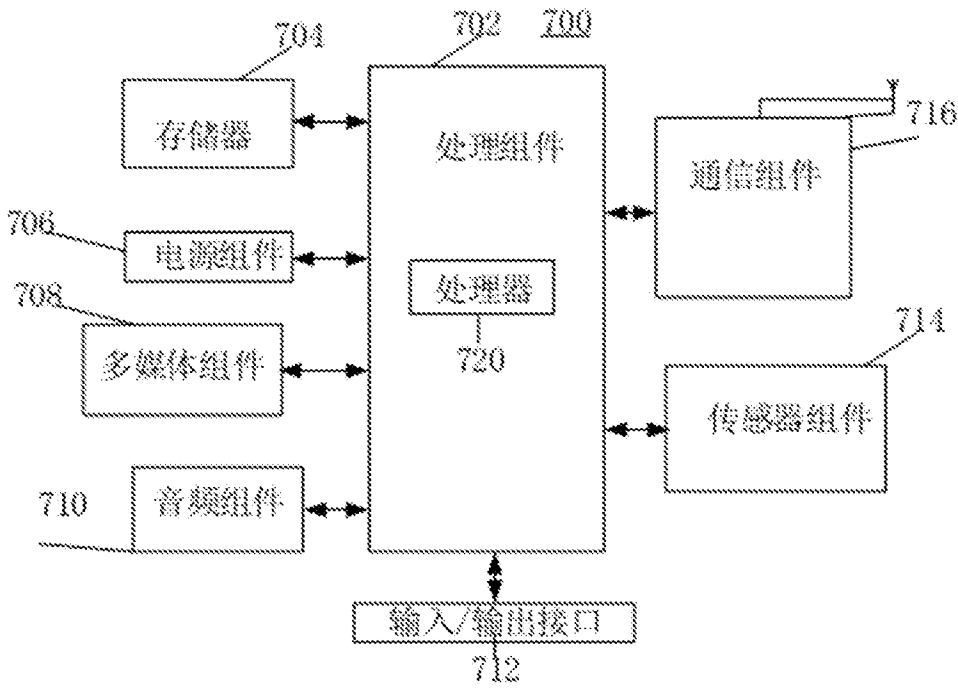


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/139627

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)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)

IPC:H04L

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)

CNTXT, ENTXT, DWPI: 网络, 入侵, 检测, 特征, 分类, 自注意力, 多头, 稀疏, intrusion, detect, model, feature, self-attention

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116112288 A (TIANYI CLOUD TECHNOLOGY CO., LTD.) 12 May 2023 (2023-05-12) claims 1-15	1-15
Y	CN 114048468 A (BEIJING TOPSEC NETWORK SECURITY TECHNOLOGY CO., LTD. et al.) 15 February 2022 (2022-02-15) description, paragraphs 36-122 and 132-144	1-3, 10-11, 14-15
Y	CN 113723440 A (BEIJING UNIVERSITY OF TECHNOLOGY et al.) 30 November 2021 (2021-11-30) description, paragraphs 32-103	1-3, 10-11, 14-15
Y	CN 113823264 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 21 December 2021 (2021-12-21) description, paragraph 46	2, 11
A	CN 111160343 A (SOUTH CHINA UNIVERSITY OF TECHNOLOGY) 15 May 2020 (2020-05-15) entire document	1-15
A	CN 109871901 A (CENTRAL SOUTH UNIVERSITY) 11 June 2019 (2019-06-11) entire document	1-15



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

“D” document cited by the applicant in the international application

“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

01 March 2024

Date of mailing of the international search report

06 March 2024

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/139627

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2020322362 A1 (HOSEO UNIVERSITY ACADEMIC COOPERATION FOUNDATION) 08 October 2020 (2020-10-08) entire document	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/139627

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	116112288	A	12 May 2023	None			
CN	114048468	A	15 February 2022	None			
CN	113723440	A	30 November 2021	None			
CN	113823264	A	21 December 2021	None			
CN	111160343	A	15 May 2020	None			
CN	109871901	A	11 June 2019	None			
US	2020322362	A1	08 October 2020	KR	102046789	B1	20 November 2019

A. 主题的分类

H04L 9/40(2022.01)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)

IPC:H04L

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))

CNTEXT,ENTXT,DWPI:网络, 入侵, 检测, 特征, 分类, 自注意力, 多头, 稀疏, intrusion, detect, model, feature, self-attention

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
PX	CN 116112288 A (天翼云科技有限公司) 2023年5月12日 (2023 - 05 - 12) 权利要求1-15	1-15
Y	CN 114048468 A (北京天融信网络安全技术有限公司 等) 2022年2月15日 (2022 - 02 - 15) 说明书第36-122, 132-144段	1-3,10-11,14-15
Y	CN 113723440 A (北京工业大学 等) 2021年11月30日 (2021 - 11 - 30) 说明书第32-103段	1-3,10-11,14-15
Y	CN 113823264 A (腾讯科技(深圳)有限公司) 2021年12月21日 (2021 - 12 - 21) 说明书第46段	2,11
A	CN 111160343 A (华南理工大学) 2020年5月15日 (2020 - 05 - 15) 全文	1-15
A	CN 109871901 A (中南大学) 2019年6月11日 (2019 - 06 - 11) 全文	1-15
A	US 2020322362 A1 (HOSEO UNIVERSITY ACADEMIC COOPORATION FOUNDATION) 2020年10月8日 (2020 - 10 - 08) 全文	1-15

☐ 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

“D” 申请人在国际申请中引证的文件

“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

2024年3月1日

国际检索报告邮寄日期

2024年3月6日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

徐泉

电话号码 (+86) 010-53961794

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/139627

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	116112288	A	2023年5月12日	无	
CN	114048468	A	2022年2月15日	无	
CN	113723440	A	2021年11月30日	无	
CN	113823264	A	2021年12月21日	无	
CN	111160343	A	2020年5月15日	无	
CN	109871901	A	2019年6月11日	无	
US	2020322362	A1	2020年10月8日	KR 102046789 B1	2019年11月20日