(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 106953862 A
(43)申请公布日 2017.07.14

(21)申请号 201710178579.4

(22)申请日 2017.03.23

(71)申请人 国家电网公司
地址 100033 北京市西城区西长安街86号
申请人 全球能源互联网研究院

(72)发明人 张姗 毛澍 李彦庆 张晶晶

(74)专利代理机构 北京三聚阳光知识产权代理有限公司 11250
代理人 吴黎

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

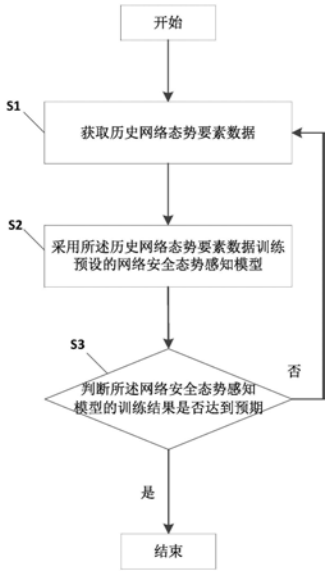
权利要求书1页 说明书6页 附图2页

(54)发明名称

网络安全态势的感知方法和装置及感知模型训练方法和装置

(57)摘要

本发明公开了一种基于Tensorflow和Docker的网络安全态势的感知方法和装置及感知模型训练方法和装置，该感知模型训练方法包括：获取历史网络态势要素数据；采用所述历史网络态势要素数据训练预设的网络安全态势感知模型，所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型；判断所述网络安全态势感知模型的训练结果是否达到预期；当未达到预期时，重复执行所述获取历史网络态势要素数据的步骤至所述采用所述历史网络态势要素数据训练预设的网络安全态势感知模型的步骤，直至所述网络安全态势感知模型的训练结果达到预期。由此，能够高效的处理海量网络数据，从而有效地进行网络安全态势的感知。



CN 106953862 A

1.一种基于Tensorflow和Docker的网络安全态势的感知模型训练方法,其特征在于,包括:

获取历史网络态势要素数据;

采用所述历史网络态势要素数据训练预设的网络安全态势感知模型,所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型;

判断所述网络安全态势感知模型的训练结果是否达到预期;

当未达到预期时,重复执行所述获取历史网络态势要素数据的步骤至所述采用所述历史网络态势要素数据训练预设的网络安全态势感知模型的步骤,直至所述网络安全态势感知模型的训练结果达到预期。

2.根据权利要求1所述的方法,其特征在于,所述获取历史网络态势要素数据包括:采用管道通讯机制获取所述历史网络态势要素数据。

3.根据权利要求1所述的方法,其特征在于,所述网络安全态势感知模型还包括分布式集群子模型。

4.根据权利要求1所述的方法,其特征在于,所述Tensorflow宽度和深度学习子模型中包括PReLU激活函数和Softmax损失函数。

5.一种基于Tensorflow和Docker的网络安全态势的感知方法,其特征在于,包括:

获取当前网络态势要素数据;

根据所述当前网络态势要素数据,通过预设的网络安全态势感知模型获取当前网络态势,其中所述网络安全态势感知模型是使用权利要求1-4中任一项所述的网络安全态势的感知模型训练方法训练并达到预期训练结果的模型。

6.一种基于Tensorflow和Docker的网络安全态势的感知模型训练装置,其特征在于,包括:

历史网络态势要素数据获取单元,用于获取所述历史网络态势要素数据;

模型训练单元,用于采用所述历史网络态势要素数据训练预设的网络安全态势感知模型,所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型;

训练结果判断单元,用于判断所述网络安全态势感知模型的训练结果是否达到预期,以及当所述训练结果未达到预期时,跳转到所述历史网络态势要素数据获取单元。

7.根据权利要求6所述的装置,其特征在于,所述历史网络态势要素数据获取单元还用于:采用管道通讯机制获取所述历史网络态势要素数据。

8.根据权利要求6所述的装置,其特征在于,所述网络安全态势感知模型还包括分布式集群子模型。

9.根据权利要求6所述的装置,其特征在于,所述Tensorflow宽度和深度学习子模型中包括PReLU激活函数和Softmax损失函数。

10.一种基于Tensorflow和Docker的网络安全态势的感知装置,其特征在于,包括:

当前网络态势要素数据获取单元,用于获取所述当前网络态势要素数据;

当前网络态势获取单元,用于根据所述当前网络态势要素数据,通过预设的网络安全态势感知模型获取所述当前网络态势,其中所述网络安全态势感知模型是采用权利要求6-9中任一项所述的网络安全态势的感知模型训练装置训练并达到预期训练结果的模型。

网络安全态势的感知方法和装置及感知模型训练方法和装置

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Tensorflow和Docker的网络安全态势的感知方法和装置及感知模型训练方法和装置。

背景技术

[0002] 随着信息技术和网络的快速发展，计算机网络的资源共享愈发开放普及，随之而来的是信息安全问题日益突出。网络安全威胁的范围和内容不断扩大和演化，网络安全形势与挑战日益严峻复杂，感知网络安全态势成为十分迫切的需要。然而由于网络数据的数量十分庞大，如何根据海量数据来感知网络安全态势，成为困扰技术人员的难题。

发明内容

[0003] 本发明要解决的技术问题在于，由于网络数据的数量十分庞大，难以根据海量的网络数据来感知网络安全态势。

[0004] 为此，本发明实施例提供了一种基于Tensorflow和Docker的网络安全态势的感知模型训练方法，包括：获取历史网络态势要素数据；采用所述历史网络态势要素数据训练预设的网络安全态势感知模型，所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型；判断所述网络安全态势感知模型的训练结果是否达到预期；当未达到预期时，重复执行所述获取历史网络态势要素数据的步骤至所述采用所述历史网络态势要素数据训练预设的网络安全态势感知模型的步骤，直至所述网络安全态势感知模型的训练结果达到预期。

[0005] 优选的，所述获取历史网络态势要素数据包括：采用管道通讯机制获取所述历史网络态势要素数据。

[0006] 优选的，所述网络安全态势感知模型还包括分布式集群子模型。

[0007] 优选的，所述Tensorflow宽度和深度学习子模型中包括PReLU激活函数和Softmax损失函数。

[0008] 本发明实施例还提供了一种基于Tensorflow和Docker的网络安全态势感知方法，包括：获取当前网络态势要素数据；根据所述当前网络态势要素数据，通过预设的网络安全态势感知模型获取当前网络态势，其中所述网络安全态势感知模型是使用上述任一种网络安全态势感知模型训练方法训练并达到预期训练结果的模型。

[0009] 本发明实施例还提供了一种基于Tensorflow和Docker的网络安全态势感知模型训练装置，包括：历史网络态势要素数据获取单元，用于获取所述历史网络态势要素数据；模型训练单元，用于采用所述历史网络态势要素数据训练预设的网络安全态势感知模型，所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型；训练结果判断单元，用于判断所述网络安全态势感知模型的训练结果是否达到预期，以及当所述训练结果未达到预期时，跳转到所述历史网络态势要素数据获取单元。

[0010] 优选的，所述历史网络态势要素数据获取单元还用于：采用管道通讯机制获取所

述历史网络态势要素数据。

[0011] 优选的，所述网络安全态势感知模型还包括分布式集群子模型。

[0012] 优选的，所述Tensorflow宽度和深度学习子模型中包括PReLU激活函数和Softmax损失函数。

[0013] 本发明实施例还提供了一种基于Tensorflow和Docker的网络安全态势感知装置，包括：当前网络态势要素数据获取单元，用于获取所述当前网络态势要素数据；当前网络态势获取单元，用于根据所述当前网络态势要素数据，通过预设的网络安全态势感知模型获取所述当前网络态势，其中所述网络安全态势感知模型是采用上述任一种网络安全态势感知模型训练装置训练并达到预期训练结果的模型。

[0014] 本发明实施例的基于Tensorflow和Docker的网络安全态势的感知方法和装置及感知模型训练方法和装置，通过Tensorflow宽度和深度学习子模型能高效的处理海量网络数据；通过将Tensorflow宽度和深度学习子模型运行在Docker容器内提高了模型的通用性。

附图说明

[0015] 通过参考附图会更加清楚的理解本发明的特征和优点，附图是示意性的而不应理解为对本发明进行任何限制，在附图中：

[0016] 图1示出了本发明实施例的基于Tensorflow和Docker的网络安全态势的感知模型训练方法的流程图；

[0017] 图2示出了本发明实施例的基于Tensorflow和Docker的网络安全态势的感知模型训练装置的结构示意图。

具体实施方式

[0018] 下面将结合附图对本发明的实施例进行详细描述。

[0019] 实施例1

[0020] 如图1所示，本发明实施例提供的基于Tensorflow和Docker的网络安全态势的感知模型训练方法，适用于分布式系统，例如互相连接以进行并行计算的多台linux服务器，包括：

[0021] S1.获取历史网络态势要素数据；

[0022] 具体地，网络态势要素可以分为生存性指标、威胁性指标和脆弱性指标三类，其中，生存性指标包括网络拓扑、网络带宽、安全设备的类型和数等等，威胁性指标包括恶意代码类型和数量、报警数量和类型、数据流入量、网络流量变化率等等，脆弱性指标包括存活主机数量、安全设备存在漏洞的数量危害等级、存活主机存在漏洞的数量危害等级等等。

[0023] S2.采用所述历史网络态势要素数据训练预设的网络安全态势感知模型；

[0024] 具体的，所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型，TensorFlow是一种将复杂的数据结构传输至人工智能神经网中进行分析和处理过程的系统框架，表达了高层次的机器学习计算，支持CPU/GPU异构设备分布式计算，具备优秀的灵活性和可延展性；Docker是一个应用容器引擎，可以轻松的为任何应用创建一个轻量级的、可移植的、自给自足的容器，开发者在笔记本上编译测试通过的容器可以

批量地在生产环境中部署，包括裸机部署(windows服务器、linux服务器)、虚拟机(vmware)、OpenStack集群和其他的基础应用平台。

[0025] 基于Tensorflow，本发明实施例将传统的线性学习(宽度学习组件)与深度前馈神经网络(深度学习组件)进行联合训练，结合这两种学习组件，形成宽度&深度学习模型。其中，宽度模型组件具有稀疏矩阵和交叉特征向量的线性模型，具有高维特征和特征组合等特点，并基于L1规范化的分类器。宽度模型组件形如y＝wx+b，使用宽度模型组件中的交叉特征转换能够记忆所有稀疏的特定规则，这对于带有稀疏输入的一般大规模态势模型分类效果明显；深度模型组件训练一个深度前馈神经网络，前馈神经网络在每一层都有感知机，会将输入的信息传递到下一层，网络的最后一层是输出。在给定的一层，节点之间不会直接相连。没有原始输入也没有输出的层就是隐藏层。前馈神经网络的目标与使用反向传播的其他监督神经网络很类似，让输入有理想的、经过训练的输出。深度模型组件是解决一些分类问题最简单有效的神经方法，能够通过嵌入归纳出类似的项目。本发明实施例中的宽度&深度学习模型的可以表达为：

[0026] $P(Y=1/x)=\sigma(w^{T}wide[x,\phi(x)]+w^{T}deepa(^{l}f)+b)$ (1)

[0027] 其中，Y是分类标签，σ是阈值函数，φ(x)是原始特征x的交叉乘积变换，W_{wide}是宽度模型权重的向量，W_{deep}是应用于最终激活$a(^{l}f)$的权重，b是偏置项。

[0028] 本发明实施例中的宽度和深度学习模型，以传统的基于逻辑回归并且用大量的交叉向量作为特征，用深度神经网络把大量分类转换成为深度向量列表，态势模型不仅减少特征工程，同时既有记忆也有泛化功能。

[0029] 利用Docker进行集群部署可以包括：

[0030] 服务端利用Docker命令启动名称为“tf-serving”容器作为TF Serving服务器。命令为docker run-d--name tf-serving enterprise/tf-serving；

[0031] 客户端利用Docker命令以交互式方式启动“tf-client”镜像作为客户端，并定义容器link，设置在容器内部通过“serving”别名访问“tf-serving”容器。命令为docker run-it--name client--link tf-serving:serving enterprise/tf-client。

[0032] S3.判断所述网络安全态势感知模型的训练结果是否达到预期；

[0033] 当未达到预期时，重复执行所述获取历史网络态势要素数据的步骤至所述采用所述历史网络态势要素数据训练预设的网络安全态势感知模型的步骤，直至所述网络安全态势感知模型的训练结果达到预期。

[0034] 本发明实施例的网络安全态势感知模型训练方法，通过Tensorflow宽度和深度学习子模型能高效的处理海量网络数据；通过将Tensorflow宽度和深度学习子模型运行在Docker容器内提高了模型的通用性。

[0035] 优选的，所述获取历史网络态势要素数据包括：采用管道通讯机制获取所述历史网络态势要素数据，管道(pipe)通信主要用于大批量的信息传递，管道可用于同一用户的同祖先的进程间通信。

[0036] 优选的，所述网络安全态势感知模型还包括分布式集群子模型，该分布式集群子模型包括客户端、主节点、从节点和参数服务器等，其中，主节点仅仅需要对每个图的执行给出一个执行请求，以及连接那些包含图中任意节点的从节点，主节点不会对每个跨设备通信或所有节点都进行调度。从节点是计算模型梯度的节点，得到的梯度向量会交付给参

数服务器更新模型，即从节点只负责处理梯度计算的参数服务器。参数服务器是多台机器组成的集群，保存模型变量、更新参数操作，以提供执行服务。Tensorflow的分布式有图内拷贝和图间拷贝两种架构模式，本实施例采用但不限于图间拷贝，在此模式中，每个从节点独立构建同一图，然后每个从节点独立运行该图，只和参数服务器共享梯度。集群可以拆分成一个或多个作业，每个作业可以包含一个或多个任务。分布式集群模型支持对客户端、主节点和从节点可以在不同的机器的不同的进程上运行的场景。一个集群中多个从节点可以创建多个图，但由于从节点运行的代码相同因此构建的图也相同，并且参数都保存到相同的参数服务器中保证训练同一个模型，这样多个从节点都可以构建图和读取训练数据，适合企业态势感知大数据场景。创建集群的必要条件是为每个参数服务器启动一个服务。这些参数服务器可以运行在不同的机器上，或者在同一台机器不同GPU上启动多个参数服务。每个参数服务器会做如下的工作：创建tf.train.ClusterSpec用于对集群中的所有任务进行描述，该描述内容对于所有任务应该是相同的。创建tf.train.Server并将tf.train.ClusterSpec中的参数传入构造函数，并将作业的名称和当前任务的编号写入本地任务中。集群中包含的参数均通过参数服务器作业进行声明并使用tf.train.replica_device_setter()方法将参数映射到不同的参数服务器中。模型中每一个独立的计算单元都会映射到参数服务器<->从节点的本地的任务中。学习者在Tensorflow参数服务器根据输入数据进行模型训练。等模型训练完成、验证之后，模型会被发布到Tensorflow系统服务器。客户端提交请求，由服务端返回预测结果。

[0037] 优选的，所述Tensorflow深度学习子模型中包括PReLU激活函数以适应宽度&深度学习模型数据的稀疏性；还可以通过引入Softmax损失函数，实现网络安全态势预测的多分类。具体地，由于Relu(Rectified Linear Units)修正线性单元激活函数在训练中较为脆弱，本实施例采用PReLU(Parametric Rectified Linear Unit，即带参数的ReLU)激活函数来拟合模型，PRelu的表达式为f(x)＝max(ax,x)，其中a是控制函数负半部分的斜率，a<0。PReLU使用后向传播训练，a用链式法则求导并用动量方法更新。PRelu需要像更新权重W一样使用神经网络更新一个额外的参数，但是相较于W的数量来说，PRelu需要更新的参数总数可以忽略不计，所以不会加重过拟合的影响。softmax回归模型是logistic回归模型在多分类问题上的扩展(logistic回归解决的是二分类问题)。态势预测的目标是分解成多类别，机器学习算法优化又依赖于损失函数，因此本实施例引入损失函数Softmax并加入函数权重衰减项，利用Softmax重新定义了宽度&深度学习模型的输出层，对类标记的k个可能值进行了累加，进而实现网络安全态势预测的多分类。修改后的Softmax损失函数为：

[0038] $$loss(X,Y)=-\frac{1}{N}\sum_i\sum_j 1\{j=y^{(i)}\}\log(Pi,j) \quad (2)$$

[0039] 其中，X指的是神经网络的输出，Y代表的是0-1矩阵，N代表输入的数据的个数；当第i个样本的类别为j，则设置y_{ij}＝1，且第i行的其余列的值都为0，表示为.1{j＝$y^{(i)}$}；

[0040] $P_{i,j}=\frac{\exp(x_{i,j})}{\sum_j\exp(x_{i,j})}$其含义为第i个输入的类别为j的概率为$p_{i,j}$。

[0041] 实施例2

[0042] 本发明实施例提供了一种基于Tensorflow和Docker的网络安全态势感知方法，包括：

[0043] 获取当前网络态势要素数据；

[0044] 根据所述当前网络态势要素数据，通过预设的网络安全态势感知模型获取当前网络态势，其中所述网络安全态势感知模型是使用实施例1所述的网络安全态势感知模型训练方法训练并达到预期训练结果的模型。

[0045] 实施例3

[0046] 如图2所示，本发明实施例提供了一种基于Tensorflow和Docker的网络安全态势感知模型训练装置，适用于分布式系统，包括：

[0047] 历史网络态势要素数据获取单元1，用于获取所述历史网络态势要素数据；

[0048] 模型训练单元2，用于采用所述历史网络态势要素数据训练预设的网络安全态势感知模型，所述网络安全态势感知模型包括运行在Docker容器内的Tensorflow宽度和深度学习子模型；

[0049] 训练结果判断单元3，用于判断所述网络安全态势感知模型的训练结果是否达到预期，以及当所述训练结果未达到预期时，跳转到所述历史网络态势要素数据获取单元。

[0050] 本发明实施例的网络安全态势感知模型训练方法，通过Tensorflow宽度和深度学习子模型能高效的处理海量数据；此外，还通过将Tensorflow宽度和深度学习子模型运行在Docker容器内提高了通用性。

[0051] 优选的，所述历史网络态势要素数据获取单元还用于：采用管道通讯机制获取所述历史网络态势要素数据。

[0052] 优选的，所述网络安全态势感知模型还包括分布式集群子模型。

[0053] 实施例4

[0054] 本发明实施例提供了一种基于Tensorflow和Docker的网络安全态势感知装置，包括：

[0055] 当前网络态势要素数据获取单元，用于获取所述当前网络态势要素数据；

[0056] 当前网络态势获取单元，用于根据所述当前网络态势要素数据，通过预设的网络安全态势感知模型获取所述当前网络态势，其中所述网络安全态势感知模型是采用实施例3所述的网络安全态势感知模型训练装置训练并达到预期训练结果的模型。

[0057] 本领域内的技术人员还应理解，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM)上实施的计算机程序产品的形式。

[0058] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的，应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0059] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0060] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0061] 虽然结合附图描述了本发明的实施方式，但是本领域技术人员可以在不脱离本发明的精神和范围的情况下作出各种修改和变型，这样的修改和变型均落入由所附权利要求所限定的范围之内。

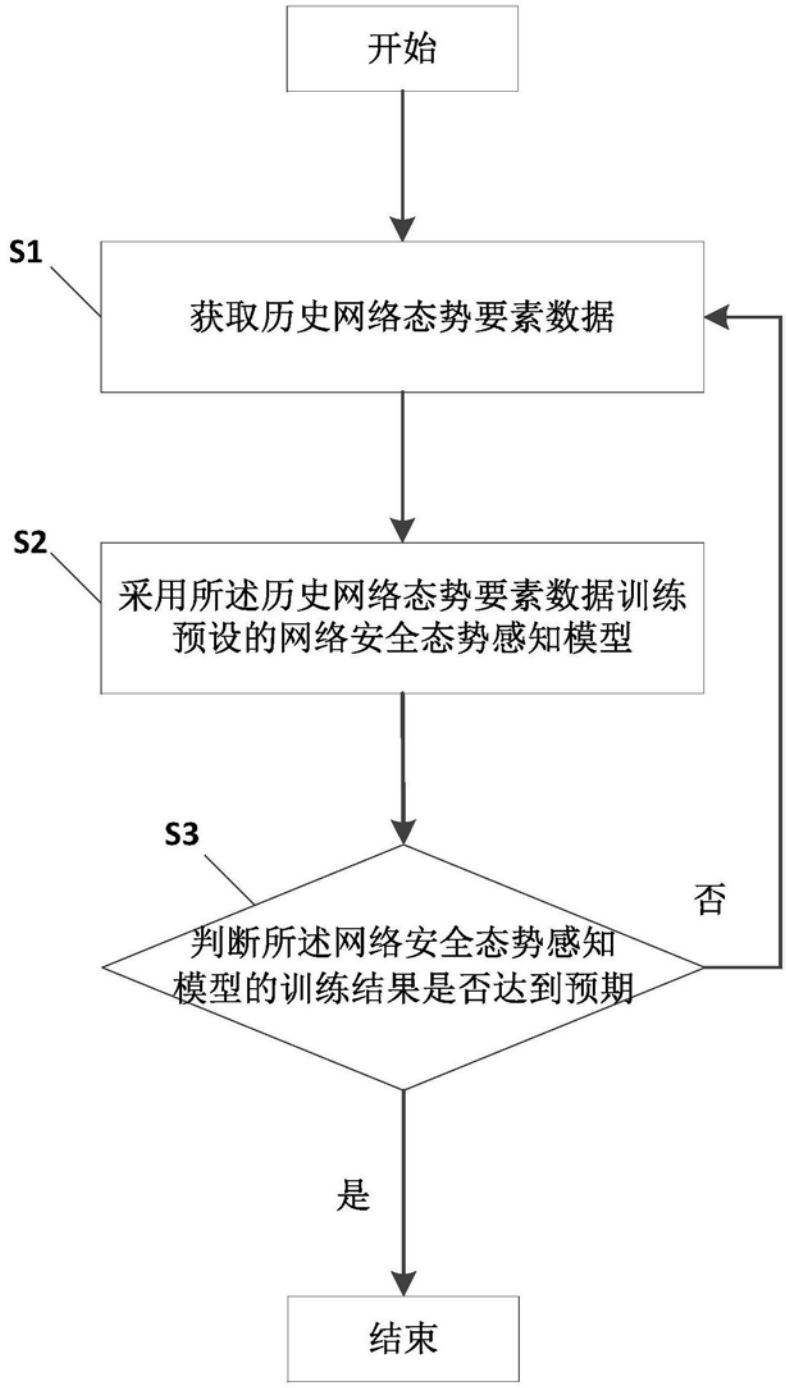

开始
S1
获取历史网络态势要素数据
S2
采用所述历史网络态势要素数据训练预设的网络安全态势感知模型
S3
判断所述网络安全态势感知模型的训练结果是否达到预期
否
是
结束

图1

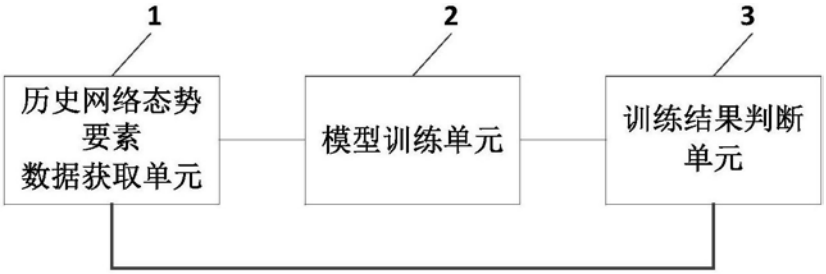


图2