(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 105491013 A
(43)申请公布日 2016.04.13

(21)申请号 201510815368.8

(22)申请日 2015.11.20

(71)申请人 电子科技大学
地址 611731 四川省成都市高新区(西区)西源大道2006号

(72)发明人 唐勇 王卫振 汪文勇

(74)专利代理机构 成都天嘉专利事务所(普通合伙) 51211
代理人 冉鹏程

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)

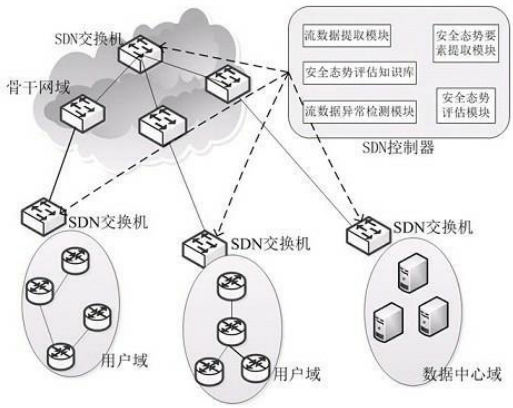
权利要求书2页 说明书7页 附图2页

(54)发明名称

一种基于SDN的多域网络安全态势感知模型及方法

(57)摘要

本发明公开了一种基于SDN的多域网络安全态势感知模型及感知方法,其包括:流数据提取模块,流数据异常检测模块,安全态势要素提取模块,安全态势评估模块和网络安全态势评估知识库。本发明利用OpenFlow中流表机制,控制器能更加实时高效的获取这些网络流量信息,并且不增加额外网络负载。这相比传统网络内基于数据包或者数据包整合流的流量信息来说,既不需要路由器对NetFlow的软件支持,也不需要交换机中额外配置硬件芯片对sFlow的支持,使得该系统既节约成本又部署方便。



CN 105491013 A

1.一种基于SDN的多域网络安全态势感知模型，其特征在于包括：流数据提取模块，流数据异常检测模块，安全态势要素提取模块，安全态势评估模块和网络安全态势评估知识库；

所述流数据提取模块，用来针对主干网和各网络域分别提取其网络流信息，完成数据采集和特征提取工作；

所述流数据异常检测模块，根据流数据提取模块所得到的数据特征，对主干网和各网络域的流数据分别使用不同粒度的检测模型进行检测，检测有无网络安全事件发生并判断其类别和具体安全事件；

所述安全态势要素提取模块，用来从流数据异常检测模块的检测结果中，提取出安全威胁和安全防御两方面的态势要素；

所述安全态势评估模块，用来把表示网络安全状态的要素信息转换为安全态势知识，通过指标的定量描述来实现系统态势感知的目标；

所述网络安全态势评估知识库，首先是实时地存储由异常检测模块得到的检测结果并为各安全态势要素和安全态势指标的计算提供数据，其次也是整个评估系统的历史知识的积累，从而使系统能够更加准确和及时地对检测到的安全威胁进行分析判断并且对出现的新情况更快做出响应。

2.采用如权利要求1所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于步骤如下：

步骤1).在当前时间窗口结束时刻，控制器从主干网交换机和各安全域出口处的SDN交换机中提取出现成的所有网络流实体；

步骤2).流数据提取模块分别对主干网和各安全域的流数据进行各自的流的统计，统计依据为按需定义；对流的概率统计；然后计算这些概率的香农熵值并且进行标准化，最后以向量的形式组合这些统计信息形成流数据的特征向量；

步骤3).流数据异常检测模块采用贝叶斯网络分类算法对主干网流数据的特征向量进行网络安全事件检测并判别种类；检测结果是安全事件所属类别；记录每个时间窗口内主干网数据流量的检测结果到安全态势感知数据库；

步骤4).流数据异常检测模块采用基于决策树C4.5分类算法对各安全域流数据的特征向量进行网络安全事件的检测；检测结果是具体的安全事件；记录每个时间窗口内各个安全域数据流量的检测结果到安全态势感知数据库；

步骤5).根据步骤3)和步骤4)中主干网络流量和各安全域网络流量的异常安全事件检测结果，按态势要素计算方法计算出各要素值；

步骤6).基于确立的安全态势指标体系，根据安全态势要素值和安全态势指标值的历史信息，分别计算安全威胁和安全防御两大方面的指标值，表征整个网络的安全态势。

3.根据权利要求2所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤1)中，所述的网络流实体是指流表项和流表项对数据包的匹配信息，比如匹配的次数和字节数。

4.根据权利要求2所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤2)中，所述的统计依据为按需定义，如各协议流量在该处网络流量的各自比例、流平均包数。

5.根据权利要求4所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤2)中，所述的对流的概率统计，如按照目的IP统计各流的概率分布，抑或目的端口流的概率分布。

6.根据权利要求2所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤1)进一步包括：

控制器向所有交换机发出流表查询请求，交换机回复所有流表项和流表项的匹配数据给控制器，控制器通过与上一时间窗口的流信息的比较，存储该时间窗口内活跃的流数据。

7.根据权利要求2所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤2)进一步包括：

控制器根据与各交换机的连接来区分该时间窗口内流表项的网络出处，并按照主干网和各安全域来组织这些流数据，流数据提取模块对各安全域的流数据进行特征计算，特征有目的IP流概率分布的熵、目的端口流概率分布的熵和各协议流数据占该总流量的比例，并根据特征出现次数做标准化处理，最后以向量的形式组合这些统计信息形成流数据的特征向量。

8.根据权利要求2所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤3)进一步包括：

利用贝叶斯网络分类算法实现对主干网络流量的异常检测过程分三步：选择训练样本、学习训练样本得分类器、利用分类器对待检测数据进行分类；具体实现时，学习样本不能直接使用动态的网络流量数据，这是因为动态的网络数据流是分类器的检测对象，也是分类器的直接输入数据；但是在分类器学习的过程中，学习样本却是动态网络流加上它的所属类别，该类别的添加完全是人为操作，所以动态的网络流量必须慢下节奏，变成静态的信息记录的形式，然后添加其类别，最后才能被分类器学习；学习过程是基于贝叶斯分类算法的；最后使用学习好的分类器对主干网络数据按时间窗口进行安全事件检测。

9.根据权利要求2所述的基于SDN的多域网络安全态势感知模型的感知方法，其特征在于：步骤6)进一步包括：

由安全态势要素值，按照安全态势指标体系的设计和各指标的计算公式来计算各指标值，以这些指标值来反应多域网络的安全态势；指标体系分两大方面：安全威胁态势评估指标和安全防御态势评估指标；安全威胁态势评估指标主要有理论安全威胁指标，用以表示主干网和各安全域整体发生安全事件的可能性；实际安全威胁指标，用以表示在各安全域所检测到的安全事件对网络造成的影响；安全威胁范围指数以及安全威胁可控指数；安全防御态势评估指标主要有安全设备总体防御指数和网络主机综合安全防御指数；同要素计算模块，各指标值的计算也需要用到安全态势评估知识库所存储的历史知识和当前时间窗口网络流异常检测结果并且把计算结果动态更新到知识库。

一种基于SDN的多域网络安全态势感知模型及方法

技术领域

[0001] 本发明涉及网络安全和网络管理领域，确切地说涉及一种基于SDN的多域网络中网络安全态势感知模型及方法。

背景技术

[0002] 网络安全问题一直存在，应对安全威胁的软硬件措施也已经广泛应用。然而网络管理人员却在面对大量的威胁检测数据的时候，不能快速准确的提取出有用信息进行网络安全管理决策。为此研究人员将最先出现在航空领域的态势感知技术应用于网络，提出了网络安全态势感知，其主要目的就是从多元的安全信息中提取、精炼、融合生成宏观层面的网络安全信息，帮助管理人员及时处理网络中出现的各类安全问题。

[0003] 公开号为 103581186A，公开日为2014年2月12日的中国专利文献公开了一种网络安全态势感知方法及系统，其包括：提取可用于描述网络安全态势的关键要素，包括网络流量稳定性、威胁性、脆弱性、用户行为；对提取的该关键要素，进行二级指标分值和一级指标分值计算，该一级指标分值包括网络流量稳定性指标分值SS、威胁性指标分值TS、脆弱性指标分值VS、用户行为指标分值US；最后，利用加权求和计算整个网络安全态势值。该发明的目的在于，力求建立全面的网络安全态势感知指标，提高网络安全态势感知的有效性和实时性。

[0004] SDN最早起源于斯坦福大学的clean state项目，它是一种创新的网络体系架构，其核心思想是把转发平面和控制平面解耦，通过集中式的控制器并使用标准的接口对各种不同的网络设备进行管理。目前，OpenFlow作为标准的接口已经得到广泛使用，中心控制器通过OpenFlow协议实现对物理交换机的精细化监测和管理。同时，SDN具有天然的网络虚拟化的优势，特别是对于数据中心的网络虚拟化应用。出于部署的要求，虚拟化要求具有集中式控制的网络架构，而SDN网络恰恰就是一种集中式管理的网络架构。

[0005] 通过上述背景技术的描述，可知现有的网络安全态势感知模型，并未与SDN技术相结合，针对以公开号为 103581186A专利文献为代表的传统网络内是基于数据包或者数据包整合流的流量信息来说，既需要路由器对NetFlow的软件支持，还需要交换机中额外配置硬件芯片对sFlow的支持，成本高而又布置不方便。

发明内容

[0006] 本发明旨在针对上述现有技术所存在的缺陷和不足，提供一种基于SDN的多域网络安全态势感知模型，本发明利用OpenFlow中流表机制，控制器能更加实时高效的获取这些网络流量信息，并且不增加额外网络负载。这相比传统网络内基于数据包或者数据包整合流的流量信息来说，既不需要路由器对NetFlow的软件支持，也不需要交换机中额外配置硬件芯片对sFlow的支持，使得该系统既节约成本又部署方便。

[0007] 同时，本发明提供了该多域网络安全态势感知模型的感知方法。

[0008] 本发明是通过采用下述技术方案实现的：

一种基于SDN的多域网络安全态势感知模型，其特征在于包括：流数据提取模块，流数据异常检测模块，安全态势要素提取模块，安全态势评估模块和网络安全态势评估知识库。

[0009] 所述流数据提取模块，用来针对主干网和各网络域分别提取其网络流信息，完成数据采集和特征提取工作。

[0010] 网络流是指在网络流量中具有相同属性的数据包集合，例如具有相同目的IP地址属性的网络流，具体情况中属性可以按需要指定甚至进行属性组合；网络流的概念在SDN网络中有很具体的实体对应——流表(项)；控制器只要查看该交换机上的所有流表项以及它们匹配数据包的次数，很容易就能获得并整理出通过该交换机的网络流信息，完成数据采集工作；为系统的检测需要，具体实现时，该模块分别从主干网交换机和各网络域出口处的交换机中提取出网络流数据信息，并且以这些主干网和各网络域为数据组织单元，统计它们的流的概率分布并计算这些概率的香农熵以及标准化，完成特征提取工作。香农熵的计算公式为 $H(X) \equiv -\sum P(x)\log_2[P(x)]$ 。把主干网络流和各网络域流量分开来提取特征是为了在下面的流量异常检测模块中对它们进行有针对性的检测。该数据采集模块按时间窗口周期采集数据并以此来驱动整个系统的运行。

[0011] 所述流数据异常检测模块，根据流数据提取模块所得到的数据特征，对主干网和各网络域的流数据分别使用不同粒度的检测模型进行检测，检测有无网络安全事件发生并判断其类别和具体安全事件。

[0012] 利用贝叶斯网络分类算法对主干网流数据的特征向量进行网络安全事件检测，检测结果为安全事件的类别，比如RemotFilAccess、Dos或正常等；利用决策树C4.5分类算法对各安全域流数据的特征向量进行网络安全事件的检测，检测结果是具体的安全事件本身，比如Land、PS、FtpWrite等。

[0013] 所述安全态势要素提取模块，用来从流数据异常检测模块的检测结果中，提取出安全威胁和安全防御两方面的态势要素。

[0014] 由流数据异常检测结果，按照安全态势要素的设计和计算公式计算各要素值，为下面的安全态势评估指标的计算提供数据。该模块从主干网流量检测结果与各安全域流量检测结果的对比中以及各安全域入流量与出流量的检测结果对比中，提取态势要素，并计算该要素值。

[0015] 所述安全态势评估模块，主要用来把表示网络安全状态的要素信息转换为安全态势知识，通过指标的定量描述来实现系统态势感知的目标。

[0016] 具体过程是按照所制定的安全态势评估指标体系，对态势要素信息进行分析、统计、融合、计算，最终得到安全威胁与安全防御两个方面安全态势评估指标的数据值。这些数据值从全局视角近实时地反映网络的安全状态和变化趋势，从而为网络安全管理提供决策依据。该模块也包括所选择的安全态势评估指标体系。

[0017] 所述网络安全态势评估知识库，首先是实时地存储由异常检测模块得到的检测结果并为各安全态势要素和安全态势指标的计算提供数据，其次也是整个评估系统的历史知识的积累，从而使系统能够更加准确和及时地对检测到的安全威胁进行分析判断并且对出现的新情况更快做出响应。

[0018] 知识库的数据会在旧时间窗口结束后根据流异常检测结果而动态更新，并且基于

态势要素提取以及态势指标计算时所需访问的信息进行设计，具体也以数据库的形式存在。数据库中的信息表分别从全局网络、安全域网络、攻击事件等角度存储网络安全态势的基本信息，其中主要的表：全网基本信息表，主要记录所管理的整个网络在每个时间窗口的一些统计信息；各个网络域信息表，主要记录该网络域在一个时间窗口的流量检测结果；攻击信息表，主要以每一次攻击为主键记录网络域层面的攻击的原始信息。

[0019] 一种基于SDN的多域网络安全态势感知模型的感知方法，其特征在于步骤如下：

步骤1).在当前时间窗口结束时刻，控制器从主干网交换机和各安全域出口处的SDN交换机中提取出现成的所有网络流实体；

步骤2).流数据提取模块分别对主干网和各安全域的流数据进行各自的流的统计，统计依据为按需定义；对流的概率统计；然后计算这些概率的香农熵值并且进行标准化，最后以向量的形式组合这些统计信息形成流数据的特征向量。

[0020] 步骤3).流数据异常检测模块采用贝叶斯网络分类算法对主干网流数据的特征向量进行网络安全事件检测并判别种类；检测结果是安全事件所属类别；记录每个时间窗口内主干网数据流量的检测结果到安全态势感知数据库；

步骤4).流数据异常检测模块采用基于决策树C4.5分类算法对各安全域流数据的特征向量进行网络安全事件的检测；检测结果是具体的安全事件；记录每个时间窗口内各个安全域数据流量的检测结果到安全态势感知数据库；

步骤5).根据步骤3)和步骤4)中主干网络流量和各安全域网络流量的异常安全事件检测结果，按态势要素计算方法计算出各要素值；

步骤6).基于确立的安全态势指标体系，根据安全态势要素值和安全态势指标值的历史信息，分别计算安全威胁和安全防御两大方面的指标值，表征整个网络的安全态势。

[0021] 步骤1)中，所述的网络流实体是指流表项和流表项对数据包的匹配信息，比如匹配的次数和字节数。

[0022] 步骤2)中，所述的统计依据为按需定义，如各协议流量在该处网络流量的各自比例、流平均包数等；

步骤2)中，所述的对流的概率统计，如按照目的IP统计各流的概率分布，抑或目的端口流的概率分布。

[0023] 步骤1)进一步包括：

控制器向所有交换机发出流表查询请求，交换机回复所有流表项和流表项的匹配数据给控制器，控制器通过与上一时间窗口的流信息的比较，存储该时间窗口内活跃的流数据。

[0024] 步骤2)进一步包括：

控制器根据与各交换机的连接来区分该时间窗口内流表项的网络出处，并按照主干网和各安全域来组织这些流数据，流数据提取模块对各安全域的流数据进行特征计算，特征有目的IP流概率分布的熵、目的端口流概率分布的熵和各协议流数据占该总流量的比例等，并根据特征出现次数做标准化处理，最后以向量的形式组合这些统计信息形成流数据的特征向量。

[0025] 步骤3)进一步包括：

同机器学习的一般步骤，利用贝叶斯网络分类算法实现对主干网络流量的异常检测过程分三步：选择训练样本、学习训练样本得分类器、利用分类器对待检测数据进行分类。具

体实现时，学习样本不能直接使用动态的网络流量数据，这是因为动态的网络数据流是分类器的检测对象，也是分类器的直接输入数据；但是在分类器学习的过程中，学习样本却是动态网络流加上它的所属类别，该类别的添加完全是人为操作，所以动态的网络流量必须慢下节奏，变成静态的信息记录的形式，然后添加其类别，最后才能被分类器学习；学习过程是基于贝叶斯分类算法的；最后使用学习好的分类器对主干网络数据按时间窗口进行安全事件检测。

[0026] 步骤4)进一步包括：

步骤4)和步骤3)大致相同，都是对网络流量的异常检测，但是检测对象、检测精度不同；还有就是在检测之前的分类器学习过程中，学习样本的数据来源不同，使用的学习算法不同；具体来说，对于各安全域数据流的异常检测，其检测对象是相对主干网来说流量较少的子网数据流量，检测的结果也需要精确到具体的某种安全事件；其用于异常检测的分类器也是基于子网的数据流量采用决策树C4.5的学习算法来学习得来的；各安全域的网络流量不需独立学习，既是该由子网数据流量训练学习而得的分类器适用于各个安全域。

[0027] 步骤5)进一步包括：

态势要素主要有表征整个网络在一个时间窗口中面临的安全威胁，表征各安全域在一个时间窗口中面临的安全威胁，以及这些理论上的安全威胁产生实际影响的可能性和对这些安全威胁的防御成功率；这些要素的计算涉及到存储在安全态势评估知识库中的当前时间窗口网络流异常检测的结果和各要素本身的历史值，并且随时间窗口动态更新其值到知识库中。

[0028] 步骤6)进一步包括：

由安全态势要素值，按照安全态势指标体系的设计和各指标的计算公式来计算各指标值，以这些指标值来反应多域网络的安全态势；指标体系分两大方面：安全威胁态势评估指标和安全防御态势评估指标；安全威胁态势评估指标主要有理论安全威胁指标，用以表示主干网和各安全域整体发生安全事件的可能性；实际安全威胁指标，用以表示在各安全域所检测到的安全事件对网络造成的影响；安全威胁范围指数以及安全威胁可控指数；安全防御态势评估指标主要有安全设备总体防御指数和网络主机综合安全防御指数；同要素计算模块，各指标值的计算也需要用到安全态势评估知识库所存储的历史知识和当前时间窗口网络流异常检测结果并且把计算结果动态更新到知识库。

[0029] 与现有技术相比，本发明所达到的有益效果如下：

1.本发明提出基于流的安全态势感知，即安全态势的数据源头从传统研究中的众多安全设备变成了网络中的网络流，从而避免了主流研究中数据融合难度大、系统响应慢的弊端，使系统更加胜任大规模网络的安全态势感知。

[0030] 2.本发明在全局网络和各安全域网络两个层次上从安全威胁和安全防御两个角度，并合理添加历史知识，从而制定了全方位多角度高汇聚度的安全态势指标体系，最终能为网络管理人员提供全面准确的网络管理决策依据。

[0031] 3.本发明在SDN网络中来实现基于流的安全态势感知系统。OpenFlow是一种流行的SDN网络架构的实现技术。利用OpenFlow中流表机制，控制器能更加实时高效的获取这些网络流量信息，并且不增加额外网络负载。这相比传统网络内基于数据包或者数据包整合流的流量信息来说，既不需要路由器对NetFlow的软件支持，也不需要交换机中额外配置硬

件芯片对sFlow的支持，使得该系统既节约成本又部署方便。

附图说明

[0032] 下面将结合说明书附图和具体实施方式对本发明作进一步的详细说明，其中：

图1为本发明基于SDN的多域网络及安全感知模块图。

[0033] 图2为本发明实施例基于SDN的多域网络安全态势感知流程图。

具体实施方式

[0034] 实施例1

基于SDN的多域网络安全态势感知，其主要包含：流数据提取模块，流数据异常检测模块，安全态势要素提取模块，安全态势评估模块，网络安全态势评估知识库。

[0035] 所述流数据提取模块，用来针对主干网和各安全域分别提取其网络流信息，完成数据采集和特征提取工作。网络流是指在网络流量中具有相同属性的数据包集合，例如具有相同目的IP地址属性的网络流，具体情况中属性可以按需要指定甚至进行属性组合。网络流的概念在SDN网络中有很具体的实体对应——流表(项)。控制器只要查看该交换机上的所有流表项以及它们匹配数据包的次数，很容易就能获得并整理出通过该交换机的网络流信息，完成数据采集工作。为系统的检测需要，具体实现时，该模块分别从主干网交换机和各安全域出口处的交换机中提取出网络流数据信息，并且以这些主干网和各安全域为数据组织单元，统计它们的流的概率分布并计算这些概率的香农熵以及标准化，完成特征提取工作。香农熵的计算公式为 $H(X) \equiv -\sum P(x)\log_2[P(x)]$ 。把主干网络流和各安全域流量分开来提取特征是为了在下面的流量异常检测模块中对它们进行有针对性的检测。该数据采集模块按时间窗口周期采集数据并以此来驱动整个系统的运行。

[0036] 所述流数据异常检测模块，根据流数据提取模块所得到的数据特征，对主干网和各安全域的流数据分别使用不同粒度的检测模型进行检测，检测有无网络安全事件发生并判断其类别和具体安全事件。利用贝叶斯网络分类算法对主干网流数据的特征向量进行网络安全事件检测，检测结果为安全事件的类别，比如RemotFilAccess、Dos或正常等；利用决策树C4.5分类算法对各安全域流数据的特征向量进行网络安全事件的检测，检测结果是具体的安全事件本身，比如Land、PS、FtpWrite等。

[0037] 所述安全态势要素提取模块，用来从流数据异常检测模块的检测结果中，提取出安全威胁和安全防御两方面的态势要素。由流数据异常检测结果，按照安全态势要素的设计和计算公式计算各要素值，为下面的安全态势评估指标的计算提供数据。该模块从主干网流量检测结果与各安全域流量检测结果的对比中以及各安全域入流量与出流量的检测结果对比中，提取态势要素，并计算该要素值。

[0038] 所述安全态势评估模块，主要用来把表示网络安全状态的要素信息转换为安全态势知识，通过指标的定量描述来实现系统态势感知的目标。具体过程是按照所制定的安全态势评估指标体系，对态势要素信息进行分析、统计、融合、计算，最终得到安全威胁与安全防御两个方面安全态势评估指标的数据值。这些数据值从全局视角近实时地反映网络的安全状态和变化趋势，从而为网络安全管理提供决策依据。该模块也包括所选择的安全态势

评估指标体系。

[0039] 所述网络安全态势评估知识库，首先是实时地存储由异常检测模块得到的检测结果并为各安全态势要素和安全态势指标的计算提供数据，其次也是整个评估系统的历史知识的积累，从而使系统能够更加准确和及时地对检测到的安全威胁进行分析判断并且对出现的新情况更快做出响应。知识库的数据会在旧时间窗口结束后根据流异常检测结果而动态更新，并且基于态势要素提取以及态势指标计算时所需访问的信息进行设计，具体也以数据库的形式存在。数据库中的信息表分别从全局网络、安全域网络、攻击事件等角度存储网络安全态势的基本信息，其中主要的表：全网基本信息表，主要记录所管理的整个网络在每个时间窗口的一些统计信息；各个安全域信息表，主要记录该安全域在一个时间窗口的流量检测结果；攻击信息表，主要以每一次攻击为主键记录安全域层面的攻击的原始信息；

实施例2

作为本发明的最佳实施方式，其包括如下步骤：

步骤1).在当前时间窗口结束时刻，控制器从主干网交换机和各安全域出口处的SDN交换机中提取出现成的所有网络流实体——流表项和它们对数据包的匹配信息，比如匹配的次数和字节数。

[0040] 步骤2).流数据提取模块继续分别对主干网和各安全域的流数据进行各自的流的统计，统计依据为按需定义，比如各协议流量在该处网络流量的各自比例、流平均包数等，还有就是对流的概率统计，比如按照目的IP统计各流的概率分布，抑或目的端口流的概率分布，然后计算这些概率的香农熵值并且进行标准化。最后以向量的形式组合这些统计信息形成流数据的特征向量。

[0041] 步骤3).流数据异常检测模块采用贝叶斯网络分类算法对主干网流数据的特征向量进行网络安全事件检测并判别种类。检测结果是安全事件所属类别。记录每个时间窗口内主干网数据流量的检测结果到安全态势感知数据库。

[0042] 步骤4).流数据异常检测模块采用基于决策树C4.5分类算法对各安全域流数据的特征向量进行网络安全事件的检测。检测结果是具体的安全事件。记录每个时间窗口内各个安全域数据流量的检测结果到安全态势感知数据库。

[0043] 步骤5).根据步骤3)和步骤4)中主干网络流量和各安全域网络流量的异常安全事件检测结果，按态势要素计算方法计算出各要素值。

[0044] 步骤6).基于确立的安全态势指标体系，根据安全态势要素值和安全态势指标值得历史信息，分别计算安全威胁和安全防御两大方面的指标值，表征整个网络的安全态势。

[0045] 步骤1)进一步包括：

控制器向所有交换机发出流表查询请求，交换机回复所有流表项和它们的匹配数据给控制器。控制器通过与上一时间窗口的流信息的比较，存储下该时间窗口内活跃的流数据。

[0046] 步骤2)进一步包括：

控制器根据与各交换机的连接来区分该时间窗口内流表项的网络出处，并按照主干网和各安全域来组织这些流数据。流数据提取模块对各安全域的流数据进行特征计算，特征有目的IP流概率分布的熵、目的端口流概率分布的熵、各协议流数据占该总流量的比例等，并根据特征出现次数做标准化处理，最后以向量的形式组合这些统计信息形成流数据的特征向量。

[0047] 步骤3)进一步包括：

同机器学习的一般步骤，利用贝叶斯网络分类算法实现对主干网络流量的异常检测过程大体上需要三步：选择训练样本、学习训练样本得分类器、利用分类器对待检测数据进行分类。具体实现时，学习样本不能直接使用动态的网络流量数据，这是因为动态的网络数据流是分类器的检测对象，也是分类器的直接输入数据。但是在分类器学习的过程中，学习样本却是动态网络流加上它的所属类别，该类别的添加完全是人为操作，所以动态的网络流量必须慢下节奏，变成静态的信息记录的形式，然后添加其类别，最后才能被分类器学习。学习过程是基于贝叶斯分类算法的。最后使用学习好的分类器对主干网络数据按时间窗口进行安全事件检测。

[0048] 步骤4)进一步包括：

步骤4)和步骤3)大致相同，都是对网络流量的异常检测，但是检测对象、检测精度不同；还有就是在检测之前的分类器学习过程中，学习样本的数据来源不同，使用的学习算法不同。具体来说，对于各安全域数据流的异常检测，其检测对象是相对主干网来说流量较少的子网数据流量，检测的结果也需要精确到具体的某种安全事件。其用于异常检测的分类器也是基于子网的数据流量采用决策树C4.5的学习算法来学习得来的。各安全域的网络流量不需独立学习，既是该由子网数据流量训练学习而得的分类器适用于各个安全域。

[0049] 步骤5)进一步包括：

态势要素主要有表征整个网络在一个时间窗口中面临的安全威胁，表征各安全域在一个时间窗口中面临的安全威胁，以及这些理论上的安全威胁产生实际影响的可能性和对这些安全威胁的防御成功率。这些要素的计算涉及到存储在安全态势评估知识库中的当前时间窗口网络流异常检测的结果和各要素本身的历史值，并且随时间窗口动态更新其值到知识库中。

[0050] 步骤6)进一步包括：

由安全态势要素值，按照安全态势指标体系的设计和各指标的计算公式来计算各指标值，以这些指标值来反应多域网络的安全态势。指标体系分两大方面：安全威胁态势评估指标和安全防御态势评估指标。安全威胁态势评估指标主要有理论安全威胁指标，用以表示主干网和各安全域整体发生安全事件的可能性；实际安全威胁指标，用以表示在各安全域所检测到的安全事件对网络造成的影响；安全威胁范围指数以及安全威胁可控指数。安全防御态势评估指标主要有安全设备总体防御指数和网络主机综合安全防御指数。同要素计算模块，各指标值的计算也需要用到安全态势评估知识库所存储的历史知识和当前时间窗口网络流异常检测结果并且把计算结果动态更新到知识库。

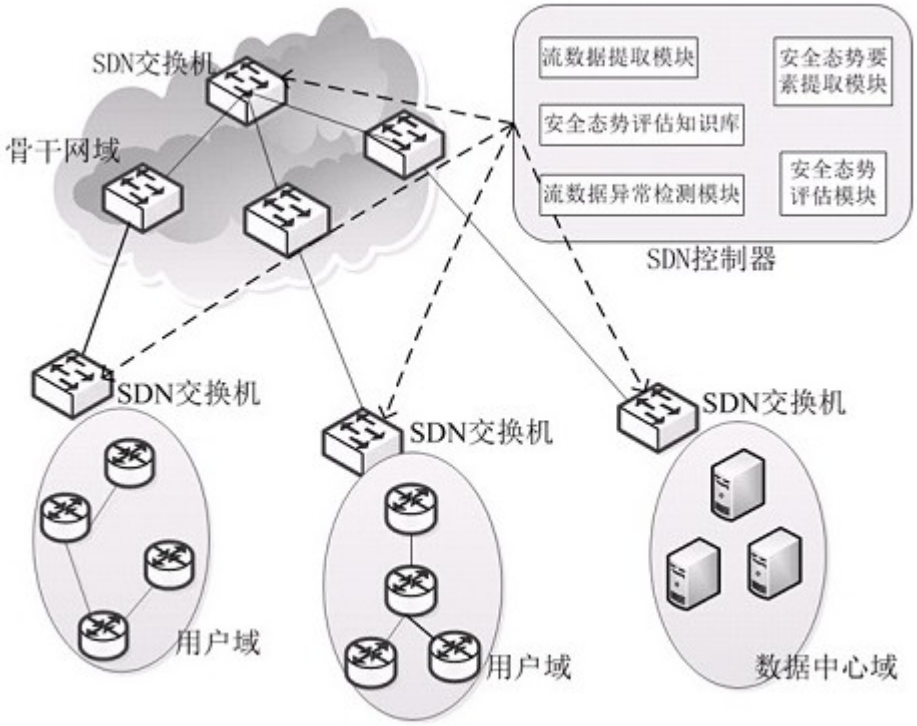

SDN交换机
骨干网域
流数据提取模块
安全态势要素提取模块
安全态势评估知识库
流数据异常检测模块
安全态势评估模块
SDN控制器
SDN交换机
SDN交换机
SDN交换机
用户域
用户域
数据中心域

图1

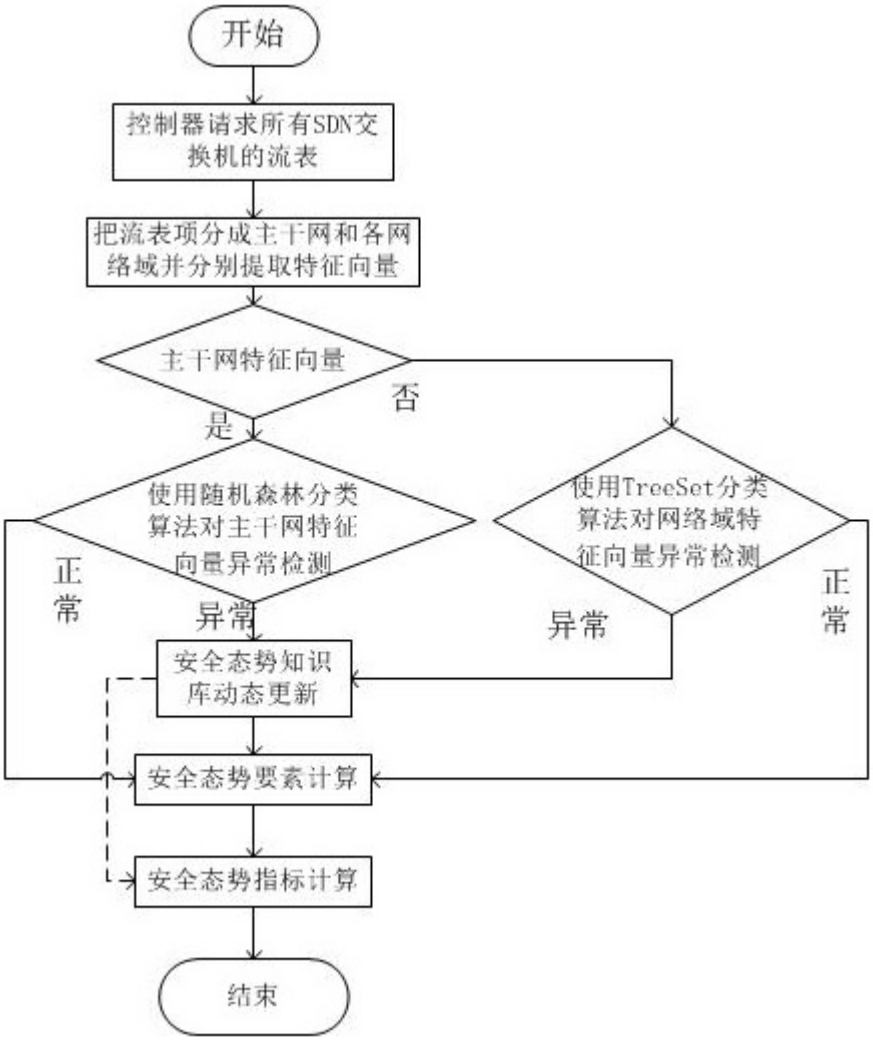

开始
控制器请求所有SDN交换机的流表
把流表项分成主干网和各网络域并分别提取特征向量
主干网特征向量
否
是
使用随机森林分类算法对主干网特征向量异常检测
使用TreeSet分类算法对网络域特征向量异常检测
正常
异常
异常
正常
安全态势知识库动态更新
安全态势要素计算
安全态势指标计算
结束

图2