(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 104378350 A
(43)申请公布日 2015.02.25

(21)申请号 201410549654.X

(22)申请日 2014.10.16

(71)申请人 江苏博智软件科技有限公司
地址 210000 江苏省南京市雨花台区西春路1号创智软件园808室

(72)发明人 傅涛 傅德胜 经正俊 孙文静

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

权利要求书1页 说明书2页

(54)发明名称

一种基于隐Markow模型的网络安全态势感知的方法

(57)摘要

一种基于隐Markow模型的网络安全态势感知的方法，它涉及网络技术领域；它具体包括以下步骤：步骤一：构建虚拟的网络安全态势感知仿真系统和真实的网络安全态势感知实物系统，网络安全态势感知仿真系统和网络安全态势感知实物系统通过数据转换通道连接；步骤二：提取可用于描述网络安全态势的关键要素；步骤三：从安全防护软件和硬件中采集数据，对数据进行预处理，并将预处理后的数据作为数据样本；得到数据样本的输出值；步骤四：收集数据，利用历史数据和当前网络安全态势，来设定时长内的网络安全态势；步骤五：根据所得数据进行检测与对比，确定网络是否安全；它通过建立网络安全态势模型，提高了网络安全态势感知的实时性和准确性，稳定性高。

CN 104378350 A

1. 一种基于隐 Markow 模型的网络安全态势感知的方法，其特征在于它具体包括以下步骤：

步骤一：构建虚拟的网络安全态势感知仿真系统和真实的网络安全态势感知实物系统，网络安全态势感知仿真系统和网络安全态势感知实物系统通过数据转换通道连接；网络安全态势感知实物系统包括网络攻击设备和网络安全设备；

步骤二：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，该一级指标分值的计算；

步骤三：从安全防护软件和硬件中采集数据，对数据进行预处理，并将预处理后的数据作为数据样本；利用流形学习对数据样本进行特征提取和降维，得到数据样本的输出值；

步骤四：收集数据，利用历史数据和当前网络安全态势，来设定时长内的网络安全态势；

步骤五：根据所得数据进行检测与对比，确定网络是否安全。

一种基于隐 Markow 模型的网络安全态势感知的方法

技术领域：

[0001] 本发明涉及网络技术领域，具体涉及一种基于隐 Markow 模型的网络安全态势感知的方法。

背景技术：

[0002] 网络原指用一个巨大的虚拟画面，把所有东西连接起来，也可以作为动词使用。在计算机领域中，网络就是用物理链路将各个孤立的工作站或主机相连在一起，组成数据链路，从而达到资源共享和通信的目的。凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路而连接起来，且以功能完善的网络软件（网络协议、信息交换方式及网络操作系统等）实现网络资源共享的系统，可称为计算机网络。

[0003] 网络是信息传输、接收、共享的虚拟平台，通过它把各个点、面、体的信息联系到一起，从而实现这些资源的共享。它是人们信息交流使用的一个工具。作为工具，它一定会越来越好用。功能会越来越多，内容也会越来越丰富。网络会借助文字阅读、图片查看、影音播放、下载传输、游戏聊天等软件工具从文字、图片、声音、视频，等方面给人们带来极其丰富和美好的使用和享受。网络也是一个资源共享的通道，但它毕竟是人类的一个工具。

[0004] 而目前要想网络安全态势感知效果好，其主要是要解决三个方面的问题：第一是研究怎样能从海量数据中挖掘出有用的特征数据，不仅反映数据的基本信息，同时也减少处理数据的维数，从而提高网络安全态势感知的实时性；第二是研究怎样使网络安全态势评估和威胁评估更加合理、有效；第三是研究怎样建立准确的网络安全态势预测模型。

发明内容：

[0005] 本发明的目的是提供一种基于隐 Markow 模型的网络安全态势感知的方法，它通过建立网络安全态势模型，提高了网络安全态势感知的实时性和准确性，稳定性高。

[0006] 为了解决背景技术所存在的问题，本发明是采用如下技术方案：它具体包括以下步骤：

[0007] 步骤一：构建虚拟的网络安全态势感知仿真系统和真实的网络安全态势感知实物系统，网络安全态势感知仿真系统和网络安全态势感知实物系统通过数据转换通道连接；网络安全态势感知实物系统包括网络攻击设备和网络安全设备；

[0008] 步骤二：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，该一级指标分值的计算；

[0009] 步骤三：从安全防护软件和硬件中采集数据，对数据进行预处理，并将预处理后的数据作为数据样本；利用流形学习对数据样本进行特征提取和降维，得到数据样本的输出值；

[0010] 步骤四：收集数据，利用历史数据和当前网络安全态势，来设定时长内的网络安全态势；

[0011] 步骤五：根据所得数据进行检测与对比，确定网络是否安全。

[0012] 本发明具有如下有益效果：通过建立网络安全态势模型，提高了网络安全态势感知的实时性和准确性，稳定性高。

具体实施方式：

[0013] 本具体实施方式采用如下技术方案：它具体包括以下步骤：

[0014] 步骤一：构建虚拟的网络安全态势感知仿真系统和真实的网络安全态势感知实物系统，网络安全态势感知仿真系统和网络安全态势感知实物系统通过数据转换通道连接；网络安全态势感知实物系统包括网络攻击设备和网络安全设备；

[0015] 步骤二：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，该一级指标分值的计算；

[0016] 步骤三：从安全防护软件和硬件中采集数据，对数据进行预处理，并将预处理后的数据作为数据样本；利用流形学习对数据样本进行特征提取和降维，得到数据样本的输出值；

[0017] 步骤四：收集数据，利用历史数据和当前网络安全态势，来设定时长内的网络安全态势；

[0018] 步骤五：根据所得数据进行检测与对比，确定网络是否安全。

[0019] 本具体实施方式具有如下有益效果：通过建立网络安全态势模型，提高了网络安全态势感知的实时性和准确性，稳定性高。

[0020] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。