(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 104506385 A
(43)申请公布日 2015.04.08

(21)申请号 201410826302.4

(22)申请日 2014.12.25

(71)申请人 西安电子科技大学
地址 710071 陕西省西安市太白南路 2 号西安电子科技大学

(72)发明人 李兴华 何龚敏 郭佳 刘海 张俊伟 马建峰 姜奇

(74)专利代理机构 北京科亿知识产权代理事务所（普通合伙）11350
代理人 汤东凤

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 29/06(2006.01)

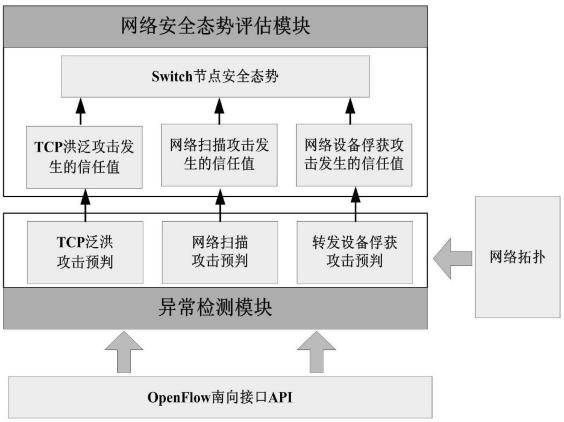
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种软件定义网络安全态势评估方法

(57)摘要

本发明公开了一种软件定义网络安全态势评估方法，结合 SDN 集中控制和收集信息直接、快速的优势，针对 SDN 转发面典型的三类攻击提出了一个开放的 SDN 安全态势评估框架，该安全框架与 SDN 控制器的架构紧密契合，其中异常检测模块根据 SDN 和各类攻击特性提取特征指标，并且选取支持向量分类算法 (SVM) 进行识别，给出攻击的预判。而安全态势评估模块根据异常检测模块收集的信息对网络安全态势进行量化评估，并通过阈值的设置来调节评估系统对攻击的敏感程度和抗噪声能力。最后本发明对不同的攻击基于层次分析法 (AHP) 分配不同的权值，从而拟合出网络的综合安全态势值。本发明灵活、简单，能准确地检测到攻击行为并给出网络的安全态势量化评估，以较小的代价实现对 SDN 转发面安全状况的监测和评估。



CN 104506385 A

1.一种软件定义网络安全态势评估方法，其特征在于：首先由异常检测模块给出各类攻击的预判，然后安全态势评估模块在预判的基础上建立针对各类攻击的网络安全态势，具体包括如下步骤：

步骤1，控制器周期性地对各个转发节点的网络指标参数进行采集，异常检测模块根据各类攻击的特点从采集到的样本数据中提取具体的特征指标；

步骤2，在一段时间内收集各类攻击的特征指标 $Y=(y_1, y_2, \ldots y_n)$，将这些特征指标作为训练集，通过支持向量机(SVM)分类器进行训练：首先确定分类个数为2，即正常或异常，分类器将所有样本集的特征分类，计算SVM分类器中每个特征向量的相关值，并根据这些相关值计算协方差矩阵空间，然后计算特征系数，获得模型参数；最后对步骤1中的样本数据进行测试分类；

步骤3，进行M次采样后，统计出在该M次采样中，转发节点在各类攻击下的正常次数和异常次数；

步骤4，安全态势评估模块接收到所述异常检测模块的统计数据后，根据贝叶斯理论计算出转发节点在各类攻击下的当前信任值，以评估在各类攻击下转发节点的安全状况；

步骤5，安全态势评估模块在步骤4中计算得出的各个信任值和不同攻击类型对网络的不同危害程度的基础上，为各类攻击对网络安全态势的影响分配相应的权值，并通过拟合得到网络的综合安全态势值。

2.根据权利要求1所述的一种软件定义网络安全态势评估方法，其特征在于，所述攻击类型包括TCP洪泛攻击、网络扫描攻击以及转发设备俘获攻击。

3.根据权利要求2所述的一种软件定义网络安全态势评估方法，其特征在于，所述TCP洪泛攻击的特征指标包括流平均数据包数以及流平均字节数，其中流平均数据包数以及流平均字节数均采用下式进行计算：

$$mid(X)=\begin{cases} x_{(n+1)/2} & n\text{为奇数} \\ \dfrac{x_{n/2}+x_{(n+2)/2}}{2} & \text{其他} \end{cases};$$

其中 $X=(x_1, x_2 \ldots x_n)$ 是各流的数据包数目或者字节数目组成的序列，并且按从小到大排列，即 $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n$。

4.根据权利要求2所述的一种软件定义网络安全态势评估方法，其特征在于，所述网络扫描攻击的特征指标包括端口号变化率和大于空闲超时流表项比例，其中端口号变化率GDP采用如下公式进行计算：

$$GDP=\frac{Num\_ports_{t_2}-Num\_ports_{t_1}}{t_2-t_1};$$

其中 $Num\_ports_{t_2}$ 和 $Num\_ports_{t_1}$ 分别为 t_2 和 t_1 时刻的端口号数目；

另外，所述大于空闲超时流表项比例为超过空闲超时的流表项数站总流表项数的比例，所述空闲超时是指一个流表项没有数据流的时间超过设定的值后流表项会被删除。

5.根据权利要求2所述的一种软件定义网络安全态势评估方法，其特征在于，所述转发设备俘获特征指标包括转发节点端口流量变化率和流表一致性检查，其中端口号流量变

化率的计算方法如下：

$R_{tra}=(S_{tra2}-S_{tra1})/(t_2-t_1)$；

其中 S_{tra2}, S_{tra1}分别为 t_2和 t_1时刻的端口数据流速率；

流表一致性检查是指检查控制器和交换机流表状态是否出现流表不一致。

6.根据权利要求 1 所述的一种软件定义网络安全态势评估方法，其特征在于，步骤 4 中，根据贝叶斯理论，二元事件服从 Beta 分布，则转发节点收集 M 次预判值后，在每个攻击类型下的当前信任值计算方法如下：

$$T_0=\frac{m'+1}{m'+m+1}$$

其中，m’ 和 m 分别为在该类攻击下的正常次数和异常次数，m’+m ＝ M。

7.根据权利要求 6 所述的一种软件定义网络安全态势评估方法，其特征在于，样本数据进行实时更新，大小为 M 的样本组成一个长度为 M 的窗口，若当前的信任值 T_0计算完成后，样本中的数据整体右移一位，原来的第 M 个样本数据即离当前时间最远、最陈旧数据的从窗口中淘汰，然后把刚计算出来的 T_0放入原来 T_1的位置，即第一个位置，参与下一次信任值的计算，同时保证样本实时更新。

8.根据权利要求 1 所述的一种软件定义网络安全态势评估方法，其特征在于，步骤 5 中，不同攻击类型的权值是基于层次分析法进行分配的，并且当遭受某类攻击超过一定程度后将对得到的权值进行修正；所述综合安全态势值的计算方法具体如下：

5.1 初始化要拟合的元素个数 n、某时刻转发节点在各类攻击下的信任值 $T=\{T_{Attack1}, T_{Attack2}, \ldots T_{Attackn}\}$、n×n 判断矩阵 A 以及各类攻击的惩罚阈值 $C=\{c_1, c_2, \ldots, c_n\}$；

5.2 将判断矩阵 A 的每一列归一化：$\bar{b}_{ij}=b_{ij}/\sum_{k=1}^{n}b_{kj},(i=1,2,...n)$；

5.3 将归一化后的矩阵按行求和：$\bar{\omega}_i=\sum_{j=1}^{n}\bar{b}_{ij},(i=1,2,...n)$；

5.4 对向量 $\bar{W}=[\bar{\omega}_1,\bar{\omega}_2,...\bar{\omega}_n]^T$进行归一化：$\omega_i=\bar{\omega}_i/\sum_{k=1}^{n}\bar{\omega}_i \quad (i=1,2,...n)$，则特征向量为 $W=[\omega_1, \omega_2, \ldots \omega_n]^T$，即得到基础权值；

5.5 求得特征根值 $t=\sum_{i=1}^{n}(AW)_i/n\omega_i$，其中 A 为判断矩阵，W 为基础权值，并据此计算一致性指标 CI ＝ (t-n)/(n-1)；对照标准平均随机一致性指标进行一致性检验，如果不通过则调整判断矩阵 A 并跳转到步骤 5.2；否则转到步骤 5.6；

5.6 如果检测到第 i 类攻击的异常次数 m_i大于相应的惩罚阈值 c_i，则令 $\Delta_i=m_i-c_i$，对该类攻击的基础权值进行修正 $\bar{a}=[\bar{a}_1,\bar{a}_{2,...}\bar{a}_n]^T$，其中 $\bar{a}_i=\omega_i\sqrt{\Delta_i}$；

5.7 对权值向量归一化：$a_i=\bar{a}_i/\sum_{k=1}^{n}\bar{a}_i,(i=1,2,..n)$ 得到最终权值：$a=[a_1, a_2, \ldots a_n]^T$；

5.8 求出最终拟合后的安全态势值 $S=\sum_{i=1}^{n}a_i\times T_{Attacki}$。

一种软件定义网络安全态势评估方法

技术领域

[0001] 本发明涉及一种数字信息传输技术，具体涉及一种网络安全状况监测评估技术，用于软件定义网络 (Software Defined Network) 的安全态势评估。

背景技术

[0002] 随着软件定义网络 (SDN) 的普及和进一步研究，网络具有更大的灵活性、开放性和可维护性，网络开发或维护者可以将各种不同功能的应用部署到控制器中实现网络的持续创新。一项重要的应用是对网状况的态势感知，即对影响网络安全的因素进行获取、理解和评估，是对网络安全性进行定量分析，这在网络安全监测和防护领域有重要的意义。而现有对 SDN 网络安全的研究特别是对网络转发面的研究主要是接入认证、简单的入侵检测等，如在 SDN 中控制器通过 TLS/SSL 来认证和授权转发节点的身份以保证转发设备身份的可靠性以及控制器与转发面信道的安全。SDN 网络除了认证、授权外还需要对网络节点的行为进行监测、评估，以获取网络的安全态势。传统分布式网络中对网络安全态势评估存在诸多问题，首先传统网络除了要直接从相邻观节点观测到的数据中得出直接信任值外还要接收别的节点对特定节点的推荐信息，同时要确保推荐信息不被伪造，从而增加了信息收集量和甄别的难度。另外传统网络在参数信息的传递与计算上具有空间局限性，由于分布式网络数据的收集要从局部到整体逐级传递，给网络带来较高的负担和延时，难以对网络的变化进行全面实时的监测。而且传统网络中设备差异大，要收集的信息可能千差万别，给评估方法的建模带来新的难度。传统安全评估方案都较复杂，评估模型复杂化这对于全网安全方案的升级变更带来不便，可扩展性差。因此现有网络安全状况研究方案的缺点使得对网络进行准确、实时以及高效的检测评估带来困难。

发明内容

[0003] 针对现有技术的不足，本发明旨在提供一种 SDN 网络安全态势评估方法，通过在 SDN 中设置异常检测模块和安全态势评估模块，由 SDN 控制器负责整个网络集中化的监测和评估，同时保证方案的简洁、高效和较强的可扩展性强。其中异常检测模块针对三类典型网络攻击的特点抽取出要在 SDN 中进行检测的具体特征，并应用 SVM 分类器对异常状况进行分类和识别，而安全态势评估模块则根据得到的统计数据利用贝叶斯理论得到攻击的信任值，并且根据不同攻击的威胁程度基于层次分析法拟合出综合的网络安全态势值。

[0004] 为了实现上述目的，本发明采用如下技术方案 ：

[0005] 首先由异常检测模块给出各类攻击的预判，然后安全态势评估模块在预判的基础上建立针对各类攻击的网络安全态势，具体包括如下步骤 ：

[0006] 步骤 1，控制器周期性地对各个转发节点的网络指标参数进行采集，异常检测模块根据各类攻击的特点从采集到的样本数据中提取具体的特征指标 ；

[0007] 步骤 2，在一段时间内收集各类攻击的特征指标 $Y = (y_1, y_2, .. y_n)$，将这些特征指标作为训练集，通过支持向量机 (SVM) 分类器进行训练 ：首先确定分类个数为 2，即正常或

异常，分类器将所有样本集的特征分类，计算 SVM 分类器中每个特征向量的相关值，并根据这些相关值计算协方差矩阵空间，然后计算特征系数，获得模型参数；最后对步骤 1 中的样本数据进行测试分类；

[0008] 步骤3，进行M次采样后，统计出在该M次采样中，转发节点在各类攻击下的正常次数和异常次数；

[0009] 步骤 4，安全态势评估模块接收到所述异常检测模块的统计数据后，根据贝叶斯理论计算出转发节点在各类攻击下的当前信任值，以评估在各类攻击下转发节点的安全状况；

[0010] 步骤 5，安全态势评估模块在步骤 4 中计算得出的各个信任值和不同攻击类型对网络的不同危害程度的基础上，为各类攻击对网络安全态势的影响分配相应的权值，并通过拟合得到网络的综合安全态势值。

[0011] 需要说明的是，所述攻击类型包括 TCP 洪泛攻击、网络扫描攻击以及转发设备俘获攻击。

[0012] 进一步需要说明的是，所述 TCP 洪泛攻击的特征指标包括流平均数据包数以及流平均字节数，其中流平均数据包数以及流平均字节数均采用下式进行计算：

[0013]

$$mid(X)=\begin{cases} x_{(n+1)/2} & n\text{为奇数} \\ \dfrac{x_{n/2}+x_{(n+2)/2}}{2} & \text{其他} \end{cases};$$

[0014] 其中 $X=(x_1, x_2 \ldots x_n)$ 是各流的数据包数目或者字节数目组成的序列，并且按从小到大排列，即 $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n$。

[0015] 进一步需要说明的是，所述网络扫描攻击的特征指标包括端口号变化率和大于空闲超时流表项比例，其中端口号变化率采用如下公式进行计算：

[0016] $$GDP=\frac{Num\_ports_{t_2}-Num\_ports_{t_1}}{t_2-t_1};$$

[0017] 其中，$Num\_ports_{t_2}$ 和 $Num\_ports_{t_1}$ 分别为 t_2 和 t_1 时刻下的端口号数目；

[0018] 另外，所述大于空闲超时流表项比例为超过空闲超时的流表项数站总流表项数的比例，所述空闲超时是指一个流表项没有数据流的时间超过设定的值后流表项会被删除。

[0019] 进一步需要说明的是，所述转发设备俘获特征指标包括转发节点端口流量变化率和流表一致性检查，其中端口号流量变化率的计算方法如下：

[0020] $R_{tra}=(S_{tra2}-S_{tra1})/(t_2-t_1)$；

[0021] 其中 S_{tra2}, S_{tra1} 分别为 t_2 和 t_1 时刻的端口数据流速率；

[0022] 流表一致性检查是指检查控制器和交换机流表状态是否出现不一致。

[0023] 需要说明的是，步骤 4 中，根据贝叶斯理论，二元事件服从 Beta 分布，则转发节点在每个攻击类型下的当前信任值计算如下：

[0024] $$T_0=\frac{m'+1}{m'+m+1}$$

[0025] 其中，m’ 和 m 分别为在该类攻击下的正常次数和异常次数，m’+m = M。

[0026] 进一步需要说明的是，样本数据进行实时更新，大小为 M 的样本组成一个长度为 M 的窗口，若当前的信任值 T_0 计算完成后，样本中的数据整体右移一位，原来的第 M 个样本数据即离当前时间最远、最陈旧数据的从窗口中淘汰，然后把刚计算出来的 T_0 放入原来 T_1 的位置，即第一个位置，参与下一次信任值的计算，同时保证样本实时更新。

[0027] 需要说明的是，步骤 5 中，不同攻击类型的权值是基于层次分析法进行分配的，并且当遭受某类攻击超过一定程度后将对得到的权值进行修正；所述综合安全态势值的计算方法具体如下：

[0028] 5.1 初始化要拟合的元素个数 n、某时刻转发节点在各类攻击下的信任值 $T = \{T_{Attack1}, T_{Attack2}, \ldots T_{AttackN}\}$、n×n 判断矩阵 A 以及各类攻击的惩罚阈值 $C = \{c_1, c_2, \ldots, c_n\}$；

[0029] 5.2 将判断矩阵 A 的每一列归一化：$\bar{b}_{ij} = b_{ij} / \sum_{k=1}^{n} b_{kj}, (i = 1,2,...n)$；

[0030] 5.3 将归一化后的矩阵按行求和：$\bar{\omega}_i = b_{ij} / \sum_{j=1}^{n} b_{ij}, (i = 1,2,...n)$；

[0031] 5.4 对向量 $\bar{W} = [\bar{\omega}_1, \bar{\omega}_2, ...\bar{\omega}_n]^T$ 进行归一化：$\omega_i = \bar{\omega}_i / \sum_{k=1}^{n} \bar{\omega}_i \quad (i = 1,2,...n)$，则特征向量为 $W = [\omega_1, \omega_2, \ldots \omega_n]^T$，即得到基础权值；

[0032] 5.5 求得特征根值 $t = \sum_{i=1}^{n} (AW)_i / n\omega_i$，其中 A 为判断矩阵，W 为基础权值，并据此计算一致性指标 CI = (t-n)/(n-1)；对照随机一致性指标进行一致性检验，如果不通过则调整判断矩阵 A 并跳转到步骤 5.2；否则转到步骤 5.6；

[0033] 5.6 如果检测到第 i 类攻击的异常次数 m_i 大于相应的惩罚阈值 c_i，则令 $\Delta_i = m_i - c_i$，对该类攻击的基础权值进行修正 $\bar{a} = [\bar{a}_1, \bar{a}_{2,...} \bar{a}_n]^T$，其中 $\bar{a}_i = \omega_i \sqrt{\Delta_i}$；

[0034] 5.7 对权值向量归一化：$a_i = \bar{a}_i / \sum_{k=1}^{n} \bar{a}_i, (i = 1,2,..n)$ 得到最终权值：$a = [a_1, a_2, \ldots a_n]^T$；

[0035] 5.8 求出最终拟合后的安全态势值 $S = \sum_{i=1}^{n} a_i \times T_{Attacki}$。

[0036] 本发明的有益效果在于：

[0037] 1、本发明以安全态势值来表示转发节点遭受攻击的状况，充分利用 SDN 集中控制机制，由 SDN 控制器充当安全评估的主体，引进动态变化的安全态势值作为转发节点的安全度量，避免在网络不稳定时单次判断造成高误判率；同时 SDN 控制器对转发面设备进行信息收集，跳数少、速度快，保证了实时性，同时转发面设备支持统一的标准如 OpenFlow 协议，使得信息的收集更加规范高效，从而能以较小代价在整个 SDN 网络上对安全状况做出客观、实时的评估；

[0038] 2、本发明具有开放性和可扩展性，网络开发和维护人员可以根据各自特定的需求对安全框架进行扩展，同时所得的评估结果可以被其它上层应用所使用，对于新的攻击只要添加对于这种攻击的检测指标就能得到针对这种攻击的安全态势；

[0039] 3、本发明结合 SDN 网络的特点和面临的典型威胁，给出了需要监测的具体特征以及识别方法，同时在 SDN 控制器中利用 SVM 分类算法识别是否存在攻击，给出各类攻击的预判；

[0040] 4、本发明在异常检测模块预判结果的基础上，利用贝叶斯理论将离散的预判值转化为 0 到 1 之间的有理数，实现由此建立各类攻击下的安全态势图。

[0041] 5、本发明利用建立起来的安全态势图，通过调节阈值实现对三类典型攻击的及时准确的检测，将网络噪声期间把无攻击误判为攻击以及攻击期间把攻击误判为无攻击的误判率都控制在很低的限度内。

[0042] 6、本发明根据不同攻击的威胁程度，基于层次分析法分配不同的拟合权值，能对不同威胁程度的攻击作出准确、敏捷的度量；

[0043] 7、本发明所采用的系统简洁、灵活，能以较少的资源实现对 SDN 网络安全状况的监测和评估。

附图说明

[0044] 图 1 为本发明的实施示意图；

[0045] 图 2 为异常检测模块的功能模块示意图；

[0046] 图 3 为仿真实验的网路拓扑示意图；

[0047] 图 4 为网络噪声和攻击存在期间的安全态势变化示意图；

[0048] 图 5 和图 6 为阈值与误判率的关系示意图；

[0049] 图 7 为安全态势拟合算法与 AHP 权值分配算法效果比较示意图；

[0050] 图 8 为采样间隔与系统 CPU 占用率的关系示意图。

具体实施方式

[0051] 以下将结合附图对本发明作进一步的描述，需要说明的是，本实施例以本技术方案为前提，给出详细的实施方式和具体的操作过程，但本发明的保护范围并不限于本实施例。

[0052] 如图 1 所示，一种 SDN 网络安全态势评估方法，首先由异常检测模块给出各类攻击的预判，然后安全态势评估模块在预判的基础上建立针对各类攻击的网络安全态势，具体包括如下步骤：

[0053] 步骤 1，控制器周期性地对各个转发节点的网络指标参数进行采集，异常检测模块根据各类攻击的特点从采集到的样本数据中提取具体的特征指标；

[0054] 步骤 2，在一段时间内收集各类攻击的特征指标 $Y = (y_1, y_2, .. y_n)$，将这些特征指标作为训练集，通过支持向量机 (SVM) 分类器进行训练：首先确定分类个数为 2，即正常或异常，分类器将所有样本集的特征分类，计算 SVM 分类器中每个特征向量的相关值，并根据这些特征相关值计算协方差矩阵空间，然后计算特征系数，获得模型参数；最后对新的样本数据进行测试分类。

[0055] 需要说明的是，选择使用 SVM 的原因在于：(1)SVM 广泛地应用于统计分类以及回归分析，是最常用的的分类器之一；(2)SVM 非常适合二类问题，而本发明中需要根据指标进行有无异常的判断；(3)SVM 即适用于线性数据的分类也适用于非线性数据的分类；(4)

SVM 对小样本情况下的自动分类有着较好的分类结果，而本发明中要对样本进行周期性的更新，所以并不需要很大的训练样本。

[0056] 步骤 3，进行 M 次采样后，统计出在该 M 次采样中，转发节点在各类攻击下的正常次数和异常次数。例如 TCP 洪泛攻击、网络扫描攻击、转发设备俘获攻击得到的正常次数和异常次数分别为，(a_1, a_2)，(b_1, b_2)，(c_1, c_2)，其中 a_1, a_2, a_3 分别为三类攻击的正常次数，则 $a_1+a_2 = b_1+b_2 = c_1+c_2 = M$。

[0057] 步骤 4，安全态势评估模块接收到所述异常检测模块的统计数据后，根据贝叶斯理论计算出转发节点在各类攻击下的当前信任值，以评估在各类攻击下转发节点的安全状况；

[0058] 步骤 5，安全态势评估模块在步骤 4 中计算得出的各个信任值和不同攻击类型对网络的不同危害程度的基础上，为各类攻击对网络安全态势的影响分配相应的权值，并通过拟合得到网络的综合安全态势值。

[0059] 需要说明的是，如图 2 所示，所述攻击类型包括 TCP 洪泛攻击、网络扫描攻击以及转发设备俘获攻击。

[0060] 进一步需要说明的是，所述 TCP 洪泛攻击的特征指标包括流平均数据包数以及流平均字节数，其中流平均数据包数以及流平均字节数均采用下式进行计算：

[0061]

$$mid(X)=\begin{cases} x_{(n+1)/2} & n\text{为奇数} \\ \dfrac{x_{n/2}+x_{(n+2)/2}}{2} & \text{其他} \end{cases};$$

[0062] 其中 $X = (x_1, x_2 \ldots x_n)$ 是各流的数据包数目或者字节数目组成的序列，并且按从小到大排列，即 $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n$。

[0063] 进一步需要说明的是，所述网络扫描攻击的特征指标包括端口号变化率和大于空闲超时流表项比例，其中端口号变化率采用如下公式进行计算：

[0064] $$GDP=\frac{Num\_ports_{t_2}-Num\_ports_{t_1}}{t_2-t_1};$$

[0065] 其中，$Num\_ports_{t_2}$ 和 $Num\_ports_{t_1}$ 分别为 t_2 和 t_1 时刻下的端口号数目；

[0066] 另外，所述大于空闲超时流表项比例为超过空闲超时的流表项数站总流表项数的比例，所述空闲超时是指一个流表项没有数据流的时间超过设定的值后流表项会被删除。

[0067] 进一步需要说明的是，所述转发设备俘获特征指标包括转发节点端口流量变化率和流表一致性检查，其中端口号流量变化率的计算方法如下：

[0068] $R_{tra} = (S_{tra2}-S_{tra1})/(t_2-t_1)$；

[0069] 其中 S_{tra1}, S_{tra2} 分别为 t_1 和 t_2 时刻的端口数据流速率；

[0070] 流表一致性检查是指检查控制器和交换机流表状态是否出现不一致。

[0071] 需要说明的是，步骤 4 中，根据贝叶斯理论，二元事件服从 Beta 分布，则转发节点在每个攻击类型下的当前信任值计算如下：

[0072] $$T_0=\frac{m'+1}{m'+m+1}$$

[0073] 其中，m’和 m 分别为在该类攻击下的正常次数和异常次数，m’+m ＝ M。这样就将样本中的正常次数 m’和异常次数 m 转化一个 0 到 1 之间的值。

[0074] 需要进一步说明的是，样本数据进行实时更新，大小为 M 的样本组成一个长度为 M 的窗口，若当前的信任值 T_0 计算完成后，样本中的数据整体右移一位，原来的第 M 个样本数据即离当前时间最远、最陈旧数据的从窗口中淘汰，然后把刚计算出来的 T_0 放入原来 T_1 的位置，即第一个位置，参与下一次信任值的计算，同时保证样本实时更新。

[0075] 需要说明的是，步骤 5 中，不同攻击类型的权值是基于层次分析法进行分配的，当遭受某类攻击超过一定程度后将对得到的权值进行修正；所述综合安全态势值的计算方法具体如下：

[0076] 5.1 初始化要拟合的元素个数 n、某时刻转发节点在各类攻击下的信任值 T ＝ $\{T_{Attack1}, T_{Attack2}, \ldots T_{Attackn}\}$、n×n 判断矩阵 A 以及各类攻击的惩罚阈值 C ＝ $\{c_1, c_2, \ldots, c_n\}$；

[0077] 5.2 将判断矩阵 A 的每一列归一化：$\bar{b}_{ij} = b_{ij} / \sum_{k=1}^{n} b_{kj}, (i = 1,2,...n)$;

[0078] 5.3 将归一化后的矩阵按行求和：$\bar{\omega}_i = \sum_{j=1}^{n} \bar{b}_{ij}, (i = 1,2,...n)$

[0079] 5.4 对向量 $\bar{W} = [\bar{\omega}_1, \bar{\omega}_2, ...\bar{\omega}_n]^T$ 进行归一化：$\omega_i = \bar{\omega}_i / \sum_{k=1}^{n} \bar{\omega}_i \quad (i = 1,2,...n)$，则特征向量为 W ＝ $[\omega_1, \omega_2, \ldots \omega_n]^T$，即得到基础权值；

[0080] 5.5 求得特征根值 $t = \sum_{i=1}^{n} (AW)_i / n\omega_i$，其中 A 为判断矩阵，W 为基础权值，并据此计算一致性指标 CI ＝ (t-n)/(n-1)；对照平均随机一致性指标进行一致性检验，如果不通过则调整判断矩阵 A 并跳转到步骤 5.2；否则转到步骤 5.6；

[0081] 5.6 如果检测到第 i 类攻击的异常次数 m_i 大于阈值 c_i，则令 $\Delta_i = m_i - c_i$，对该类攻击的基础权值进行修正：$\bar{a} = [\bar{a}_1, \bar{a}_{2,...} \bar{a}_n]^T$，其中 $\bar{a}_i = \omega_i \sqrt{\Delta_i}$；

[0082] 5.7 对权值向量归一化：$a_i = \bar{a}_i / \sum_{k=1}^{n} \bar{a}_i, (i = 1,2,..n)$ 得到最终权值：a ＝ $[a_1, a_2, \ldots a_n]^T$；

[0083] 5.8 求出最终拟合后的安全态势值 $S = \sum_{i=1}^{n} a_i \times T_{Attacki}$。

[0084] 以下将通过仿真实验获得的大量数据，分析方案各个变量的关系，以及不同参数的选取对实验结果的影响。

[0085] 实验环境

[0086] 实验通过仿真进行，软硬件环境如下，硬件环境：主机 3.00GHz Core(TM)2Duo CPU，2.00G 内存。软件环境：Ubuntu12.04 操作系统。实验采用开源的网络仿真工具 Mininet 2.0.0 来搭建网络，Pox0.1.0 作为整个网络的控制器，由 Scapy 导入背景流量并且作为网络噪声和攻击产生器，代码均采用 Python 语言编写。

[0087] 实验拓扑

[0088] 仿真采用的网路拓扑如图 3 所示，一个 SDN 控制器，负责整个网络的管理。转发面有 6 个转发节点交换机，其中主机 A 接入交换机 1，主机 B 接入交换机 3，主机 D 接入交换机 6。攻击者 C 接入交换机 4，整个网络的链路带宽设置为 10Mbps。主机 A 同时向主机 B 和主机 D 发送背景数据流，发送速率分别为 1000pps 和 200pps。主机 D 同时向主机 A 和主机 B 发送背景数据流，速率分别为 1200pps 和 800pps。网络偶发状况或不可预知的异常造成的网络噪声由主机 A 来模拟。

[0089] 考虑到网络噪声的随机性特点，主机 A 向主机 D 发送源 IP 地址和端口号变化，并且速率在 100pps 到 2000pps 范围内变动的数据流，发送数据流的间隔和持续时间在 0 到 30 秒内随机变化。用 IP 地址和端口号的变化来模拟不同的用户和应用，速率的随机变化来模拟网络流量大幅波动。发送数据流的间隔和持续时间的随机变化来模拟引起网络噪声因素的随机、不持续和不可预测性等特点。实验中由控制器对转发面进行检测，对交换机 4 的数据进行分析以对该节点的安全态势进行评估。评估系统可以根据真实网络得到的安全态势图进行相应的变通处理，如对噪声进行衰减时调整单调区间的大小等。

[0090] 实验数据分析

[0091] (1) 方案有效性分析

[0092] 如果网络状态十分稳定，极少出现网络状态大幅波动，则控制器对网络节点的单次采样即可由异常检测系统给出预判值，这时的预判值不再是一种预判而是准确可靠的判断。但是遗憾的是实际的网络是一个非线性的复杂系统，网络由各个网络设备和用户组成，每个设备虽然通过有线或无线链路连接在一起，但是也有各自的独立性。每个个体状态的变化都会给整个网络施加影响，造成网络状态波动。特别是具有突发性的网络偶发状况或不可预知的因素如网络设备故障、人为的群体性活动等都会给网络状态带来剧烈振荡。这种网络振荡对我们检测和评估网络是否受到攻击造成干扰，从而成为检测和评估攻击的噪声。在此期间如果仍然仅仅以一次采样得出的预判值作为最终的判断则显得非常草率，很有可能将这次检测误判为攻击。在网络噪声持续期间会判断出一个时间点网络受到攻击，相隔很短时间又得出网络正常的判断，并且这两种相反的判断结果交替出现。显然这种判断前后矛盾，上层安全决策模块或其他希望获得网络节点安全状态的模块面对这么多的假报警显得无所适从，难以根据检测结果采取相应的动作。

[0093] 究其根本原因是仅仅采用离散的预判值难以描述网络的安全态势变化趋势，无法辨别网络噪声和正真攻击到来时的区别。所以本发明将离散的预判值量化为在实数域上的安全态势值，综合考虑一段时间内网络状态的变化趋势，将网络偶发状况或其他异常引起的网络状态振荡和真正攻击到来时网络状态变化的特点都呈现在安全态势图上。如图 4 所示，采样间隔为 1s，即 1s 给出一个安全态势值。0s 到 80s 是网络噪声存在的时间，90s 后是 TCP 洪泛攻击正真到来的时间，在网络噪声引起的网络状态振荡期间安全态势值也随之增加或减少，呈现随机震荡变化的规律。当攻击正真到来时，由于攻击的持续性，安全态势值会持续地单调下降，其下降的单调区间很长。这与网络噪声的特点形成鲜明对比。所以可以先得到某段时间内的安全态势值，然后通过设置阈值的方法来判断是否有攻击存在。阈值设置的越低，对于网络噪声引起的误判的抗击效果越好，如图中将阈值设置为 0.6 或小于 0.6 时，几乎可以消除网络噪声带来影响，使得评估系统在有网络噪声期间将噪声误判为攻击的误判率降到最低。但是阈值设置的过低对有攻击到来时将攻击误判为网络正常的

误判率带来一定提升，主要是当安全态势值从高位开始下降时，虽然攻击已经到来，但却误判为没有攻击。这种误判率的提高使得安全态势评估系统对攻击到来时的反应时间增长。但当态势值一旦下降到阈值以下后就极少会出现误判。反之，阈值设置的越高，其效果与以上分析相反，即有利于对攻击的判断，不利于抗击网络噪声带来的误判。图中十字线表示对原始安全态势值进行预处理，根据 5.1 中描述的方法，单调区间设置为 1/2 窗口大小，这里为 15s。

[0094] (2) 安全态势评估系统的误判率

[0095] 评估系统的误判率分为将有攻击误判为没有攻击和将没有攻击误判为有攻击两种。将有攻击记为 True，没有攻击记为 False。将有攻击误判为没有攻击的误判率记为 R_{TF}，将没有攻击误判为有攻击的误判率记为 R_{FT}。当网络状态非常稳定没有噪声时，评估系统能准确判断有无攻击到来，可以直接用预判值来确定有无攻击。只有当网络状态随时间变化，并存在各种因素造成的网络噪声时，会有较高的误判率，所以我们只考虑有网络噪声存在的情况。当网络噪声和攻击同时存在时，由于网络噪声会引起网络偏离稳定状态随机振荡，攻击也使网络大幅偏离网络稳定状态，所以当网络噪声和攻击并存时，安全态势值必然下降，也即必然能检测到攻击。但是我们是通过给安全态势图划定阈值进行判断是否有攻击的，即安全态势值大于阈值判断为无攻击，反之小于阈值则有攻击。所以对于有攻击时的误判率 R_{TF}（无论是否有噪声）只与阈值设定有关。而只有网络噪声时（没有攻击），将没有攻击误判为有攻击的误判率 R_{FT} 也与阈值设定相关。但两者的误判率的降低对于阈值设定的要求是矛盾的，对于它们的关系在 (1) 已经做了描述。我们希望将有噪声存在期间（没有攻击干扰，否则攻击会覆盖掉噪声）误判率 R_{FT} 和攻击存在期间将有攻击误判为没有攻击的误判率 R_{TF}。对于有噪声期间的误判率 R_{FT} 都限制在较低的水平。模拟网络噪声程序由 Host A 运行，持续时间 30 分钟，在此期间记录每次是否有攻击和每一个安全态势值。对于攻击存在期间的误判率 R_{TF}，各类攻击的持续时间为 30 分钟，在此期间对于类攻击记录每次是否有攻击和每一个安全态势值。最后计算用离散的预判值得到的整体误判率 R，以及根据选取的合适的阈值计算 R_{FT} 和 R_{TF}。实验中将采样间隔设置为 1s，样本大小 M 设置 30，流表的 Idle_timeout 设置为 10s，Hard_timeout 为 30s。安全态势评估系统每隔 1s 给出一个安全态势值。

[0096] 1) 误判率 R_{FT}

[0097] 对于只有网络噪声存在期间的误判率 R_{FT}，表 1 中给出了阈值 k 为 0.78 时将噪声误判为三类攻击的误判率。当阈值 k 设置为 0.78 时，针对三类攻击的误判率有了显著的降低。平均误判率 R_{FT} 为 3.03％。

[0098] 表 1

[0099]

误判率 / 攻击	R	R_{FT}
TCP 洪泛攻击	38.9%	2.7%
网络扫描攻击	40.2%	3.2%
设备俘获攻击	39.8%	3.3%

[0100] R_{FT}与阈值的设定有密切的关系，图 5 给出网络噪声期间不同阈值下阈三类攻击的平均误判率，从图中可以看出设置不同的阈值对误判率 R_{FT}有较大影响。当阈值超过 0.78 时，随着阈值 k 的上升误判率将有明显上升。当阈值 k 为 0.82 时，三类攻击的平均误判率上升到 12.3%，但即便如此，相对直接用离散的预判值法，仍然将误判率降低了约 68.9%。所以系统可以通过调整阈值来对确定可以接受的误判率。采用安全态势值然后划分阈值的方法对去除网络噪声带来的误判有很好的效果。

[0101] 2) 误判率 R_{TF}

[0102] 对于攻击期间的误判率 R_{TF}，在攻击开始下降时，在阈值以上部分会认为攻击没有发生，而实际攻击已经发生，但是一旦安全态势值低于阈值则能够准确判断出攻击。图 6 给出攻击存在期间不同阈值下阈三类攻击的平均误判率，误判率随着阈值的增大，总体呈类似线性下降的规律。表 2 中给出了阈值 k 为 0.78 时将攻击误判为正常的误判率 R_{TF}。从表中可以看到使用安全态势值方法比离散的预判值的误判率稍高，但总体上两者的误判率都较低，都能够满足实际的需求。

[0103] 表 2

[0104]

误判率 / 攻击	R	R_{TF}
TCP 洪泛攻击	0.17%	0.64%
网络扫描攻击	0.18%	0.59%
设备俘获攻击	0.13%	0.57%

[0105] 虽然阈值设置低一些对总体的误判率影响不大，但是会造成攻击真正到来时与评估系统判断为攻击之间存在延时。实际上系统的安全态势值已经在降低，只不过当安全态势值还在高位的时候考虑可也能由于网络噪声引起而暂不判断为攻击，一旦态势值低于阈值，后续的判断一样有效。

[0106] (3) 不同攻击对综合安全态势的影响

[0107] 在拟合算法中，我们取判断矩阵 A＝[1,1/3,1/7 ;3,1,1/4 ;7,4,1]，设定所有攻击的惩罚定阈值为 15，即当样本异常次数超过 15 次时，将会对相应权值有所调整。图 7 是测试分别只受到三类攻击中的一类攻击时，应用经典 AHP 算法和经过修改的安全态势值拟合算法得出的综合安全态势值的变化趋势，攻击在时刻 0s 发起。由圆点组成的线为 TCP 洪泛攻击，棱形线为网络扫描攻击，十字线为设备俘获攻击。图中实线为使用经典 AHP 算法所得出来的拟合结果。虚线为经过修改的拟合算法得出的结果。首先无论应用哪种算法，考虑到 TCP 洪泛攻击的危害相对较小，初始化时判断矩阵给予的权值较小，所以 TCP 洪泛攻击对整体安全态势值影响最小。转发设备俘获攻击危害最大，给予最大的权值，网络扫描攻击则居于两者之间。图中数据也体现这一点，TCP 洪泛攻击使安全态势值下降最慢，设备俘获攻击则使态势值下降最快，这体现了我们设置判断矩阵的意图。虚线部分为使用改进的权值分配算法后的安全态势变化趋势。算法为每类攻击设置了惩罚阈值，当某类攻击持续进行，评估样本中异常次数超过了惩罚阈值后适当加大该攻击权值，从而加大该攻击对整体安全态势值的影响。比较可得对于经典的 AHP 权值分配算法，无论攻击是否发生，判断矩阵一定下来这三类攻击的权值将固定不变。而经过改进的权值分配算法在判断矩阵的基础上会适当加大当前正受到攻击的权值，从而增大正在造成侵害和损失的攻击对综合安全态势值的影响力。

[0108] (4) 采样频率与评估系统的 CPU 占用率

[0109] 图 8 表示采样频率与安全态势评估系统的 cpu 占用率的关系。可以看到当采样间隔大于 40ms 时，系统对 cpu 的消耗在 10％以内，当 cpu 的采样间隔小于 40ms 时系统对 cpu 的消耗会急剧升高，当采样间隔为 0.1ms 时，系统对 cpu 占有率高达 90％。所以要在采样频率和系统资源消耗之间做出权衡。若将采样频率设为 100ms，cpu 占有率下降到 3.5％ ；当采样频率设置为 1s 时，cpu 占有率小于 1％，并已经能对三类攻击很好的检测和评估，从而以较小的资源消耗完成对 SDN 整体网络的安全态势评估。

[0110] 对于本领域的技术人员来说，可以根据以上的技术方案和构思，给出各种相应的改变和变形，而所有的这些改变和变形都应该包括在本发明权利要求的保护范围之内。

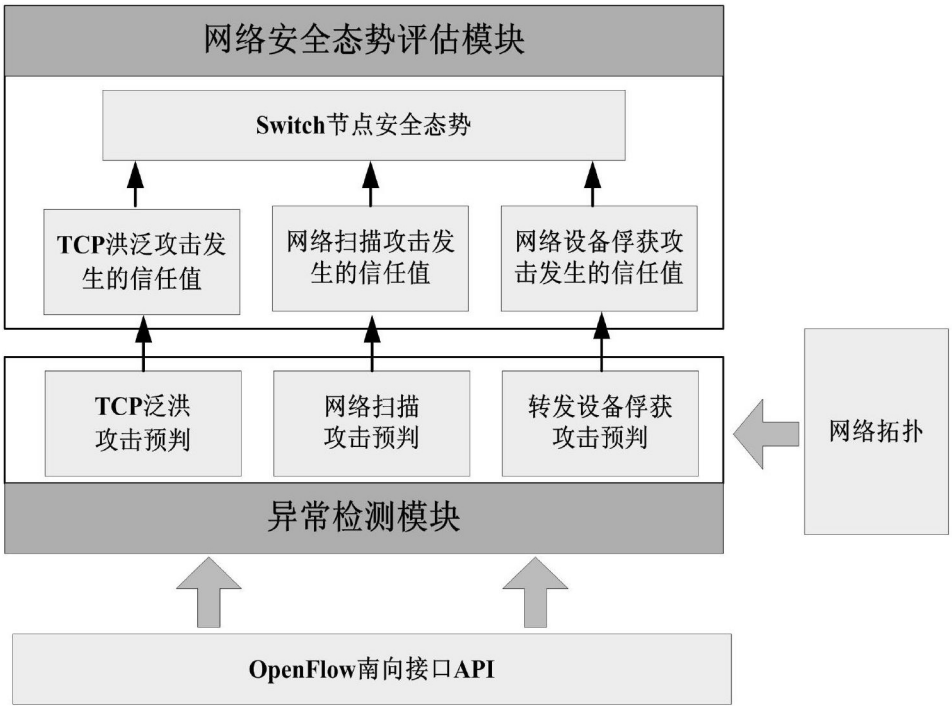

网络安全态势评估模块
Switch节点安全态势
TCP洪泛攻击发生的信任值
网络扫描攻击发生的信任值
网络设备俘获攻击发生的信任值
TCP泛洪攻击预判
网络扫描攻击预判
转发设备俘获攻击预判
网络拓扑
异常检测模块
OpenFlow南向接口API

图 1

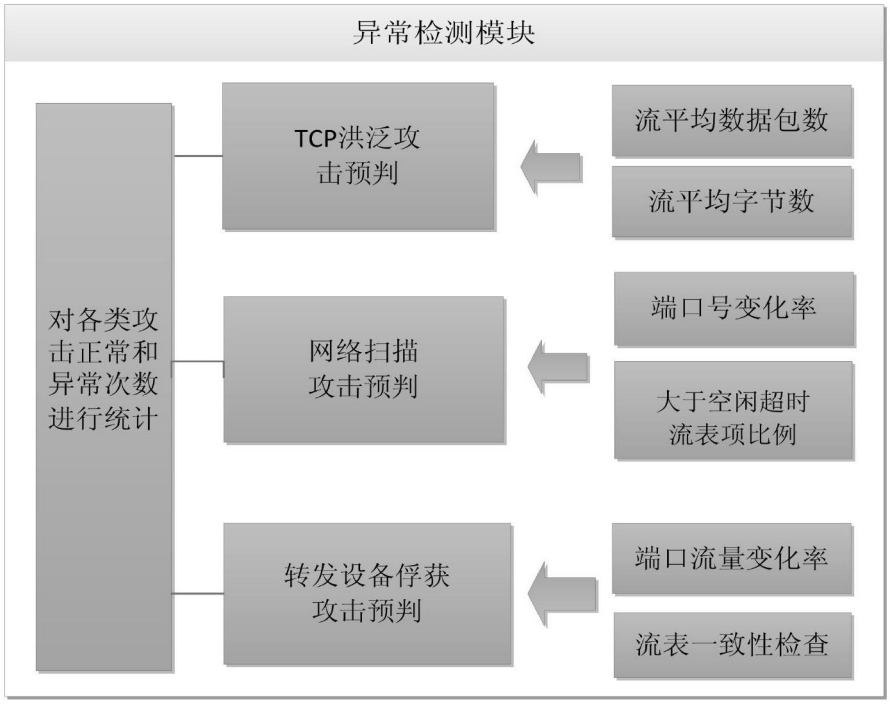

异常检测模块
对各类攻击正常和异常次数进行统计
TCP洪泛攻击预判
网络扫描攻击预判
转发设备俘获攻击预判
流平均数据包数
流平均字节数
端口号变化率
大于空闲超时流表项比例
端口流量变化率
流表一致性检查

图 2

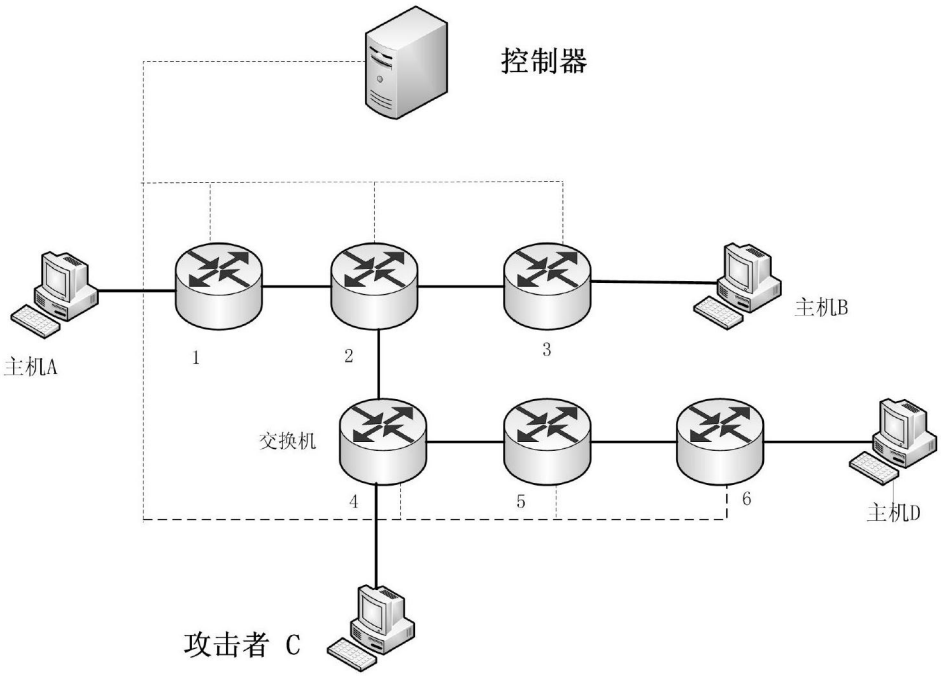

控制器
主机A
1
2
3
主机B
交换机
4
5
6
主机D
攻击者 C

图 3

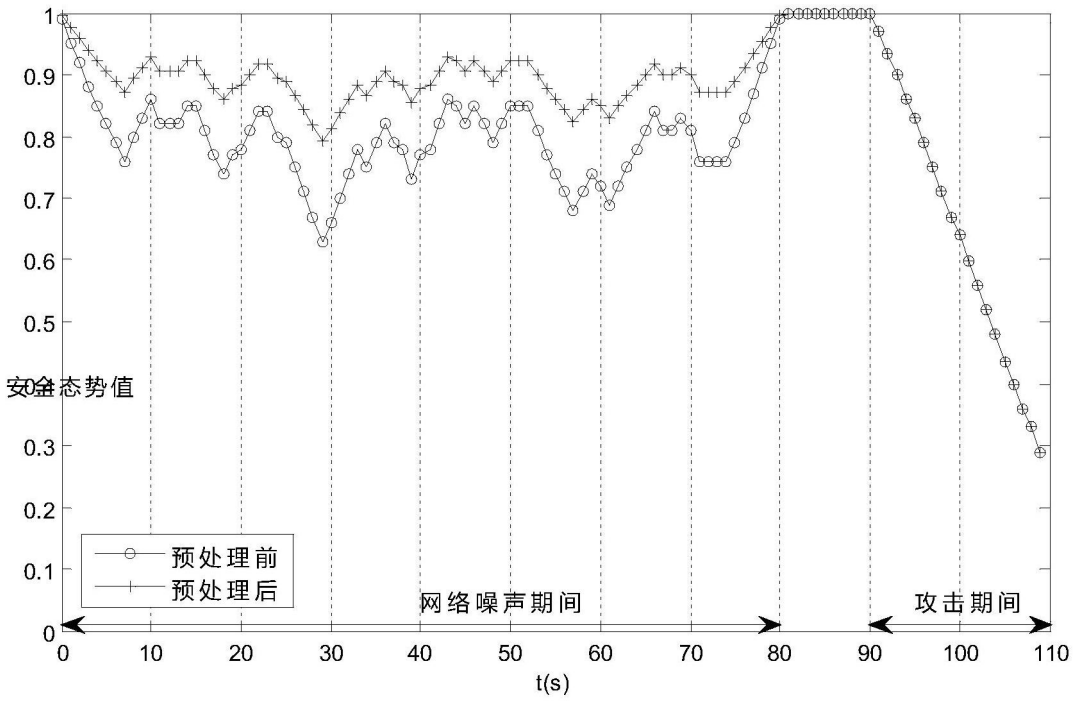

安全态势值
t(s)
预处理前
预处理后
网络噪声期间
攻击期间

图 4

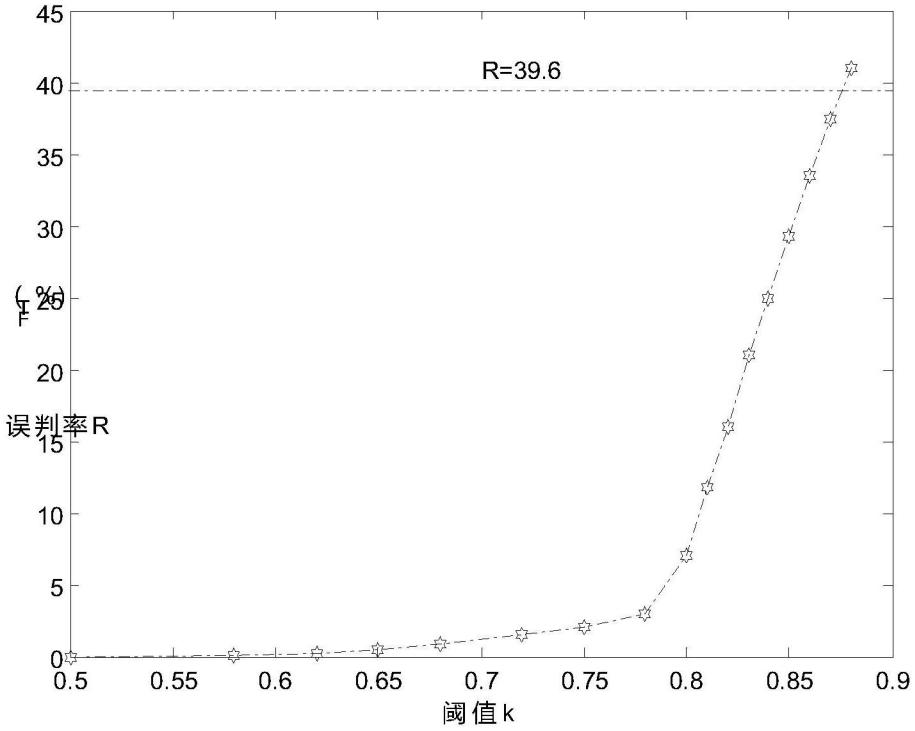


图 5

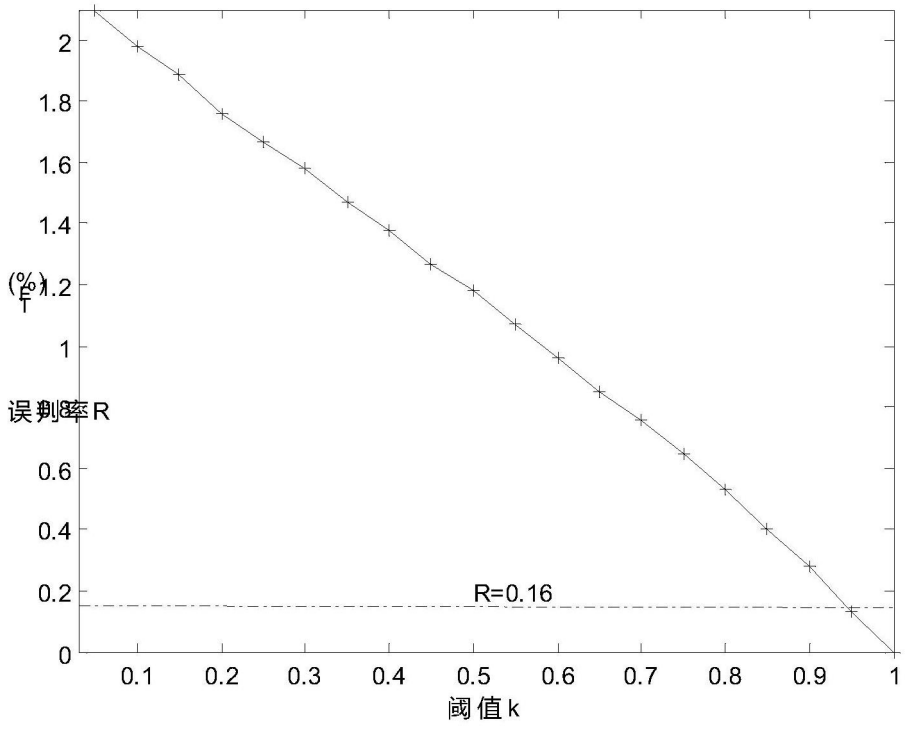


图 6

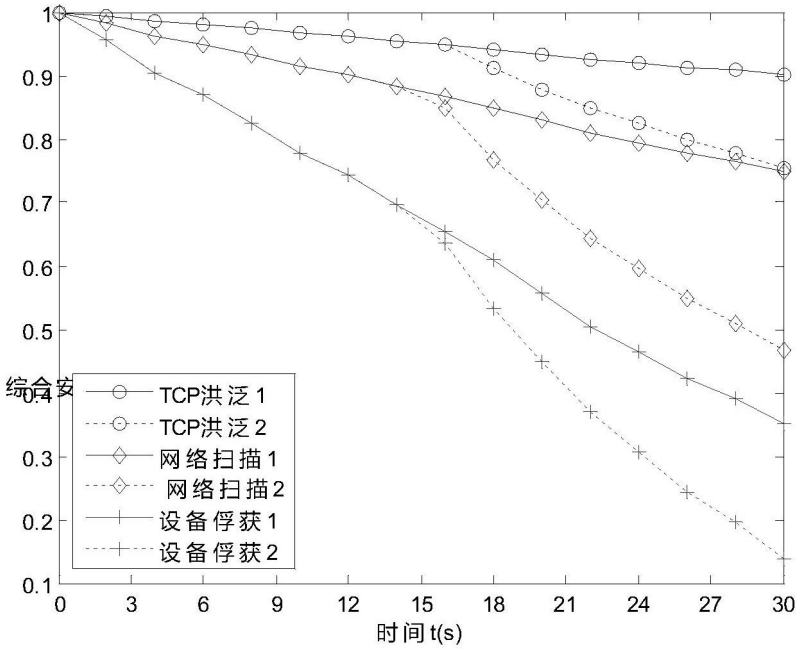

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
综合安
TCP洪泛 1
TCP洪泛 2
网络扫描 1
网络扫描 2
设备俘获 1
设备俘获 2
0 3 6 9 12 15 18 21 24 27 30
时间 t(s)

图 7

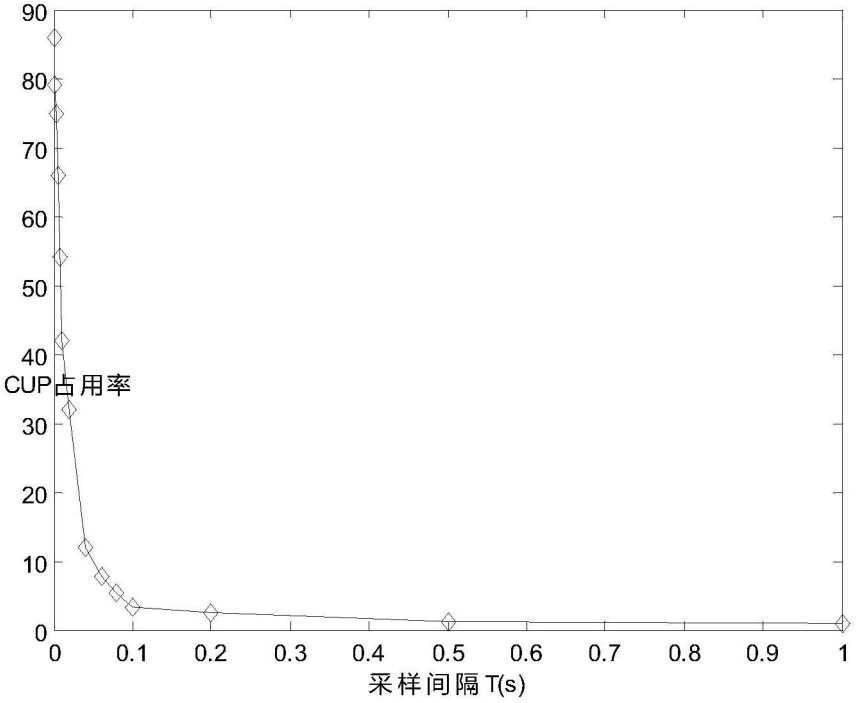

90
80
70
60
50
40
CUP占用率
30
20
10
0
0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1
采样间隔 T(s)

图 8