基于异质多传感器融合的网络安全态势感知模型*)

刘效武[1,2] 王慧强[1] 梁 颖[1] 赖积保[1]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1]
(曲阜师范大学计算机学院 日照 276826)[2]

摘 要 网络安全态势感知NSSA(Network Security Situation Awareness)是目前网络安全领域的热点研究内容,开展NSSA的研究,对提高我国的网络安全水平有着重要的意义。本文提出了一个NSSA模型,利用多层前馈神经网络,对采集的多个异质的传感器数据进行了融合。为提高融合的实时性,本文还设计了简单易行的特征约简方法,大大降低了融合引擎的输入维数。最后,本文利用安全态势生成算法,对网络安全事件进行了加权量化。实验表明,本文所提出的模型和方法是可行的和有效的。

关键词 网络安全态势感知,多层前馈神经网络,多传感器融合,特征约简,安全态势生成

Network Security Situation Awareness Model Based on Heterogeneous Multi-sensor Fusion

LIU Xiao-wu[1,2] WANG Hui-qiang[1] LIANG Ying[1] LAI Ji-bao[1]
(Department of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[1]
(College of Computer, Qufu Normal University, Qufu 276826, China)[2]

Abstract Network Security Situation Awareness (NSSA) is a hot research spot in the area of network security and it is significant to study NSSA in order to improve the security level of our nation. This paper presents a NSSA model based on data fusion. The NSSA model employs multi-layer feedforward neural network as its fusion engine and fuses the data provided by the sensors in an intelligent and efficient manner. Furthermore, this paper discusses a network security situation generation agorithm which expresses the security situation by the weighted quantization of security events. In addition, it also designs a feature reduction method in order to improve the real-time nature of the NSSA. Our model and approach are proved to be feasible and effective through a series experiments using real network traffic.

Keywords Network security situational awareness, Multi-layer feedforward neural network, Multi-sensor data fusion, Feature reduction, Security situation generation

1 引言

态势感知(Situation Awareness, SA)源于航天飞行的人因研究,此后在军事战场、空中管制和核反应控制等领域得到广泛的研究和应用。1999年,Tim Bass将安全态势引入网络安全领域,首次提出了网络态势感知的概念(Cyberspace Situation Awareness, CSA)[1]。但对于网络安全态势感知(Network Security Situation Awareness, NSSA),目前还没有成熟的模型和完善的理论基础,NSSA的研究刚刚起步,发展缓慢。对于一个NSSA系统,其主要特点是多源异质、实时和数据融合处理。所以在研究NSSA的过程中不可避免地要处理这三个问题。本文就是在此基础上探讨了一系列处理NSSA的模型和方法。

2 相关工作

在文献[2]中,Endsley将SA定义为在一定的时空条件下对环境因素的获取、理解以及对未来状态的预测,并将态势感知的过程分为三级模型:态势要素提取、态势理解和态势预测,如图1所示。但目前对NSSA仍没有全面和普遍接受的定义。本文认为,NSSA是指在大规模网络环境中对能够引起网络安全态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。其中,态势是一个整体和全局的概念,任何一个单一的因素都不能称其为态势。

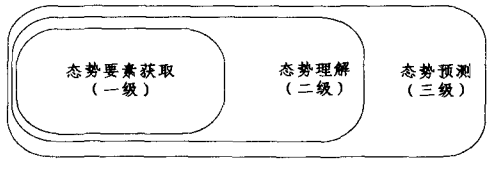


图1 态势感知三级模型

在过去的10年中,研究者提出了约30多个数据融合的模型,被引用最多的是美国国防部的JDL模型[3]。但JDL模型仅仅是对融合体系结构中的一些组成元素的简要描述,并没有提及任何软件或系统部署方面的内容。数据融合在目标

*)国家"八六三"高技术研究发展计划项目基金(2007AA01Z401)、国防十一五预研重点项目(513150602)和高等学校博士学科点专项科研基金项目(20050217007)。**刘效武** 博士研究生,主要研究方向为网络安全、数据融合、网络安全态势感知;**王慧强** 博士,教授,博导,主要研究方向为可信网络与信息安全、系统可信性评测、网络态势感知;**梁 颖** 博士研究生,主要研究方向为网络与信息安全;**赖积保** 博士研究生,主要研究方向为网络与信息安全。

跟踪、图像融合等军事领域已经出现了不少成熟的应用，但网络安全方面，应用相对较少。Bass 提出了一个基于多传感器融合的入侵检测系统的模型，实现对入侵行为的检测、威胁评估和态势评估等[1]。Salerno 将态势概念应用于网络安全领域，提出了一个理论融合模型，与 Bass 一样，也没有给出实现的原型和方法[4]。除了对模型的研究，很多的机构也开始着手研制 NSSA 的系统工具。美国能源研究中心的劳伦斯伯克利国家实验室开发了“Spinning Cube Potential Doom”，极大地提高了网络感知能力，但该系统只是用三维空间点来表示网络流量，比较侧重可视化[5]；美国国家高级安全系统研究中心的 SIFT 项目[6]和卡内基梅隆大学开发的 SILK[7]，也仅限于通过可视化网络流量和连接状态来获得对网络安全态势的感知。其中 SIFT 项目已经开发出 NVisionIP，UCLog＋等软件。但是在一些相对大型和连接数目较多的网络环境中，单纯通过可视化很难获得准确的网络安全态势。除此之外，美国国防部计算机安全中心、加拿大国防研究与开发中心等机构也在它们的研究计划中明确提出关于 NSSA 的研究内容。

国内 NSSA 的研究刚刚起步，与国外比较还有相当大的差距。文献[8]对当前的 NSSA 系统的框架、关键技术和难点问题做了深入的阐述；陈秀真等提出了一个层次化的网络安全威胁态势分层量化评估方法，从而实现对当前网络的量化评估[9]；张慧敏等实现了一个集成化网络安全监控平台，该平台可以实现多种异构传感器、多源证据关联和可视化的安全监控，但该平台主要关注推理的可视化[10]；刘炜等对安全态势估计的本质特征、求解模型等做了深入的探讨，但其研究工作仍然局限于传统的入侵识别领域[11]；其他的研究机构也对 NSSA 做了尝试性的研究，但由于总体上缺乏成熟的框架模型和理论基础，仍处于探索阶段。

纵观国内外研究现状，NSSA 已经成为网络安全领域的热点研究内容。本文就是在上述研究基础之上，通过对 NSSA 模型、融合算法和态势生成方法的探讨，进一步推动 NSSA 的研究和探索。

3 结构模型

就目前国内外 NSSA 的研究而言，仍然没有一个普遍适用的模型。陈秀真等将网络系统分为服务层、主机层和网络层三个层次进行威胁态势评估，但该方法只适用于局域网的评估，对大型的网络仍然缺少行之有效的方法；而 Bass 的下一代入侵检测模型和 JDL 融合模型也不能直接应用于 NSSA 领域。NSSA 的模型是 NSSA 的前提和基础。鉴于此，本文结合三者的优点，设计了一个 NSSA 的模型，如图 2 所示。本模型将 NSSA 划分为三个层次，即数据层、信息层和知识层，从而实现数据层获取、信息层融合和知识层感知。

数据是融合和 NSSA 的基础，能够提供何种数据，直接关系到融合的水平和结果。数据采集模块中包含两个子模块：传感器模块和前处理模块。对于 NSSA 系统而言，多源异构是它的重要特征之一。所谓多源异构指的是数据来源于多个不同类型的传感器。作为课题的一个试探性研究，本模块中选择 Cisco NetFlow 和 Snort 作为两个异质的传感器，这样部署的目的是在保障完成数据采集功能的基础上，也使得整个课题实施相对比较廉价。第二个子模块是前处理模块，它的功能包括传感器数据之间的同步、格式化、不完整数据的剔除和特征约简等功能。本文的其他部分将对 NSSA 的其他模块做更深入的探讨。

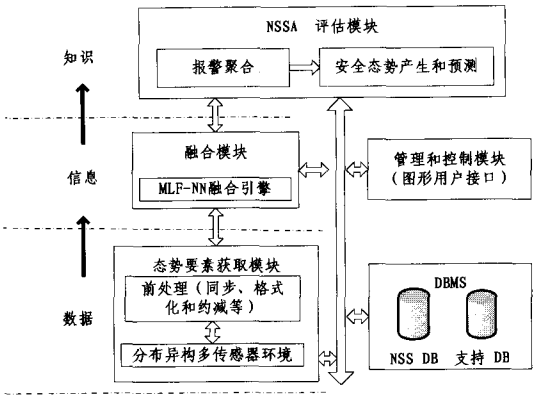


图 2 NSSA 模型

4 多传感器融合和多层前馈神经网络

4.1 多传感器融合

近几年来，多传感器融合在军事和非军事领域都引起了研究者的广泛关注，不同的模型和新算法也不断涌现。融合引擎融合来自多个传感器的数据，以便于更准确地获取当前系统的状态，这是单个传感器很难做到的。数据融合是 NSSA 非常关键的一部分，它是一种从多个（异质的）数据源获取数据，并通过融合技术将它们融合到一起，提高系统的准确性和鲁棒性，从而获得对被监控目标的更精确的推断和感知的一种技术。在一个安全系统内，存在多个安全传感器，但获取一个复杂网络系统的整个态势通常是困难的，特别是这些安全检测点分布在不同地理位置的情况下更是如此。因此，如何以有效和智能的方式融合这些传感器数据变得尤为重要。

根据 JDL 的融合模型，多传感器融合可以分为五级（Level 0 到 Level 4）；但是有些低层的融合方法，比如卡尔曼滤波，难以应用于 NSSA。实际上，根据第 3 部分的模型层次划分，本文的方法体现在 JDL 层次结构上是在 Level 2 融合，Level 3 感知。而目前多数的研究内容是在更低层次融合。作者的目的是力求在更高层次融合中找到适用于 NSSA 的融合方法。

4.2 多层前馈神经网络

从融合方法的角度来讲，目前贝叶斯理论、人工神经网络和支持向量机等都被广泛地应用于多传感器数据融合。在本文的模型中，选取多层前馈神经网络（Multi-Layer Feedforward Neural Network，MLF-NN）作为融合引擎，因为神经网络具有很强的泛化能力，能够比较智能地处理一些非线性的问题。就 MLF-NN 而言，它还具有以有效和智能的方式处理多分类问题的能力。

神经网络是由许多广泛连接的神经元组成的一种高并行处理系统。本层神经元的输出作为下层神经元的输入，最终在神经网络的输出层得到整个网络的输出。MLF-NN 是在许多领域中用得较为广泛的一种神经网络模型，图 3 是包含了两个隐层的 MLF-NN 的拓扑结构图。

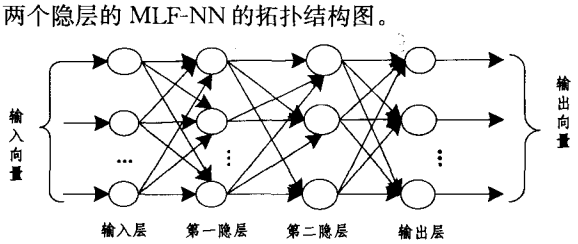


图 3 多层前馈神经网络结构

在 MLF-NN 中，最为关键的是网络的输出和权值调整公式[12,13]。公式(1)是 MLF-NN 的隐层神经元和输出层神经元的计算公式：

$$O_{k,j}=f(Net_{k,j}) \tag{1}$$

其中 $O_{k,j}$ 为第 k 层中第 j 个神经元的输出，$f(x)$ 为其激励函数，$Net_{k,j}$ 为其输入值的加权和，计算公式如(2)所示：

$$Net_{k,j}=\sum_i w_{ji}O_{k-1,i}+\theta_j \tag{2}$$

其中，w_{ij} 为连接权值，θ_j 为阈值。

应用神经网络的第一步要对神经网络进行训练。目前最主要的训练算法是 BP 算法，其中最关键的内容是误差计算公式(3)、权值调整公式(4)和阈值调整公式(5)：

$$\delta_{k,j}=\begin{cases}O_{k,j}(1-O_{k,j})(t_{k,j}-O_{k,j}), & \text{若 } j \text{ 为输出层神经元}\\ O_{k,j}(1-O_{k,j})\sum_m \delta_{k,m}w_{mj}, & \text{若 } j \text{ 为隐层神经元}\end{cases} \tag{3}$$

$$w_{ij}(t+1)=w_{ji}(t)+\eta\delta_j O_{k,j} \tag{4}$$

$$\theta_j(t+1)=\theta_j(t)+\eta\delta_j \tag{5}$$

结合公式(3)、(4)和(5)，BP 算法的训练算法可以描述如下：

(1)初始化隐层和输出层的 w_{ji} 和 θ_j；

(2)输入训练向量 X_l 和期望输出向量 D_h，其中 l 和 h 为输入向量和输出向量的维数，从第(3)步到第(5)步进行迭代；

(3)根据公式(1)计算各隐层和输出层神经元的输出；

(4)按照公式(3)计算隐层和输出层神经元的误差；

(5)根据公式(4)、(5)调整权值和阈值；

(6)一轮学习结束，判断误差精度，若满足要求，则学习结束；否则转(2)，继续下一轮迭代。

为了便于将 MLF-NN 应用于 NSSA，本文创建一个结构：

$$MLF=\{IL,HL1,HL2,OL\} \tag{6}$$

IL 表示输入向量的维数，$HL1$ 和 $HL2$ 分别表示第一个和第二个隐层神经元的数目，OL 表示神经网络输出神经元的数目。例如，{35,35,35,3}表示本 MLF-NN 包含 35 维的输入向量、两个隐层都有 35 个神经元以及输出层含有 3 个神经元。对于任意一个输入向量 $X_l=[a_1,a_2,\cdots,a_l]$，分量 a_i ($i=1\cdots l$)的取值可能是数值也可能是字符。为了便于融合，在前处理模块中将输入向量按照公式(7)进行量化，将所有的分量映射到[0,1]区间：

$$x_i=(x_i-x_{min})/(x_{max}-x_{min}) \tag{7}$$

对于任意一个输出向量，$D_h=[b_1,b_2,\cdots,b_n]$，$n=1,\cdots,h$，每一种分量的组合代表一种形式网络异常，如[0,0,1,$\cdots$,0]代表当前网络出现了 DoS 攻击。本文融合模型将网络行为分为五个类别：Normal，DoS，Probe，U2R，R2L。因此，MLF-NN 的输出层只要三个输出神经元就可以了。实际上，三个输出神经元有八种不同的组合，本文使用了五种，其他的组合根据以后的需求进行扩展。

4.3 特征约简

“维数灾难”是阻碍多传感器融合技术应用于 NSSA 的巨大障碍。高维数的输入向量带来巨大的运算量，这必然使得 NSSA 系统失去实时性。而特征约简的目的是识别对于融合来说比较重要的特征，删除对融合结果影响很小或者基本没有影响的特征。它的实质就是寻找一个输入特征的子集，这个子集中的特征是对融合结果影响较大的特征集合。从而可以通过特征约简，减少融合引擎的输入维数，改善系统的实时性。

NetFlow(版本 9)有 89 个域，其中约 60 个对目前的网络分析是有一定作用的；Snort 的输出中，有 24 个属性。如果直接将这个具有 84 个分量的向量作为融合引擎的输入，基本不具备可行性，所以特征约简是不可避免的。Lippmann 等提出了一个关键字选择算法[14]；Zhang 等采用粗糙集理论实现特征约简算法[15]。但是这些算法相对比较复杂。本文采用了一种简单有效的特征约简算法，描述如下：

(1)使用含有 84 个分量的输入向量训练 MLF-NN，定义一个集合 $Reduction\_Set=\Phi$；

(2)使用测试集测试多层前馈神经网络的分类能力，得到对于某些异常检测率 CR_{DoS}，CR_{Probe}，CR_{U2R} 和 CR_{R2L}。

(3)去掉输入向量的第 i 个特征，得到新的测试 $New\_Test\_Set_i$，$i=1\cdots84$，利用每个输入向量具有 83 个分量的 $New\_Test\_Set_i$ 测试 MLF-NN，得到新的检测率 CR'_{DoS}，CR'_{Probe}，CR'_{U2R} 和 CR'_{R2L}；

(4)定义一个阈值 ε($0\leqslant\varepsilon<<1$)，计算(3)中得到检测率是否满足公式(8)：

$$|CR_i-CR'_i|<\varepsilon, i\in\{Dos,Probe,U2R,R2L\} \tag{8}$$

(5)若满足公式(8)，则将此特征删除；若不满足，将此特征加入集合 $Reduction\_Set$：

$Reduction\_Set\leftarrow Reduction\_Set+i$；

(6)循环执行(3)-(5)，直到所有特征测试完。

经过 84 轮的循环，集合 $Reduction\_Set$ 中即为入向量中关键和重要的特征。

5 网络安全态势产生

NSSA 评估模块主要是产生当前系统的安全态势和威胁程度。该模块分为两个子模块：报警聚合子模块、安全态势产生和评估子模块。报警聚合子模块中，主要是报警聚合算法的实现。首先定义一个报警聚合结构，$V_i(t)=(COUNT,ATK\_TYPE,SIP,TME\_STAMP,P_{Severity}^{ATK\_TYPE})\ i\in\{DoS,Probe,U2R,R2L\}$。其中 $COUNT$ 表示该类聚合的警报数目，ATK_TYPE 表示攻击类型，SIP 表示攻击的源地址，TME_STAMP 表示该聚合的时间戳，$P_{Severity}^{ATK\_TYPE}$ 表示按照攻击类型分类该类聚合所具有的态势威胁因子(权值)。然后设置一个时间窗口，在该时间窗口内，如果两个报警的 ATK_TYPE 和 SIP 相同，则将它们加入到同一个 $V_i(t)$ 中，每一个报警加入到该类聚合 $V_i(t)$ 中，则对执行：$COUNT\leftarrow COUNT+1$。对于一个安全系统来讲，通常报警量比较巨大，通过这种简单的聚合方法，可以有效地降低报警量。

在大多数的研究中，报警的威胁因子 $P_{Severity}^n$ 一般根据管理员的经验赋值，没有一个客观的标准。本文中将权值因子分配算法[16]引入到 SA 领域，用于产生态势威胁因子：

$$P_{Severity}^n=\begin{cases}\dfrac{1}{2}+\dfrac{\sqrt{-2\ln\frac{2i}{n}}}{6}, & 1\leqslant i\leqslant\dfrac{n}{2}\\ \dfrac{1}{2}, & i=\dfrac{n}{2}\\ \dfrac{1}{2}-\dfrac{\sqrt{-2\ln\left(2-\frac{2i}{n}\right)}}{6}, & \dfrac{n}{2}\leqslant i\leqslant n\end{cases} \tag{9}$$

其中，i 表示严重程度等级，n 表示攻击类别的数目。这样就可以比较客观地对不同的异常赋予不同的威胁因子。将时间窗内的所有 $V_i(t)$ 按照公式(10)计算每一类异常的安全态势值：

$$S_n = \sum_{n=ATK\_TYPE} 10^{P^n_{Severity}} COUNT, n \in (DoS, \Pr obe, U2R, R2L) \quad (10)$$

之后系统总的安全态势可以由公式(11)得到：

$$S = \sum_n S_n, n \in \{DoS, \Pr obe, U2R, R2L\} \quad (11)$$

在公式(10)中使用的是 $10^{P^n_{Severity}}$ 而没有直接使用 $P^n_{Severity}$，目的是为了强调威胁因子的重要性，弱化数量对安全态势的影响程度。

6 试验

6.1 基本配置

试验的第一步是网络拓扑结构的设计，如图 4 所示。训练集和测试集使用 DARPA 1999 入侵检测数据集，数据流的生成采用 NetPoke 根据测试集和训练集的数据分布生成实际流量[17]。在融合之前要对采集到的数据按照公式(7)进行格式化，将每一个输入向量的分量映射到[0,1]区间。MLF-NN 的训练集和测试集如表 1 所示。表 1 中同时给出了根据公式(9)所计算出的威胁因子，其中严重程度分为三级，有四种不同的攻击类别。

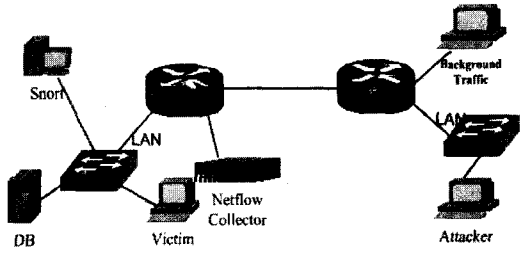


图 4 网络拓扑结构

表 1 训练集、测试集和威胁因子

类型	训练集	测试集	威胁因子
DoS	4334	2218	0.696
Probe	1798	1007	0.500
U2R	184	98	0.304
R2L	503	356	0.304
Normal	8500	4500	* * * *

6.2 属性约简性能测试

首先使用训练集按照本文中第 4.2 节讨论的训练算法进行训练，然后按照第 4.3 节的特征约简算法进行约简，最终形成一个 37 维的约简特征集。将原始的 84 维输入的神经网络约简为(37,37,37,3)，其他具体细节在文献[18]中有更详细的描述。表 2 中列出了属性约简之后和约简之前的 CPU 时间消耗的对比。从表中可以看出，属性约简减少了 CPU 的运算时间，从而使得 MLF-NN 具有更好的实时性和在线能力。

表 2 CPU 时间消耗

特征数目	NN 结构	测试集(秒)
84	(84,84,84,3)	3.66
37	(37,37,37,3)	2.17

6.3 NSSA 评估

本试验中，使用了三种类型的视图。第一种是攻击数目的态势图。首先，将测试数据集分成表 3 所示的四个子集，然后将四个子集随机注入到各个时间段内(间隔为 1h)。前处理模块对采集到数据进行同步、剔除特征缺失的输入，然后通过融合，再按照第 5 部分描述的方法统计攻击数目，试验结果见图 5。试验中没有使用入侵检测系统中的一些检测率或者是 ROC 曲线等评估方法，而是采用了可视化的形式将网络安全状况表示出来，这样就没有必要为相对比较微小的误警花费太多的精力。从图 5 中可以比较直观地获取当前网络遭受攻击的情况，也可以将相对比例比较小的误警掩盖到统计特性之中。并且，可以设置攻击数目的阈值，这个阈值可以作为是否需要采取自动响应的一个开关值，这样就可以解决目前入侵检测系统中一大难题，使得网络安全中自动响应成为可能。这并不是说 NSSA 就不能做到诸如检测率等衡量入侵检测性能的参数，而是对于 NSSA 评估而言，应该有一套新的指标体系和评估方法，这也是本课题的后续研究内容。

表 3 四个数据子集

类型	DoS	Probe	U2R	R2L	Normal
子集 1	500	124	72	165	1900
子集 2	67	324	16	39	930
子集 3	103	77	89	28	550
子集 4	173	145	31	302	680

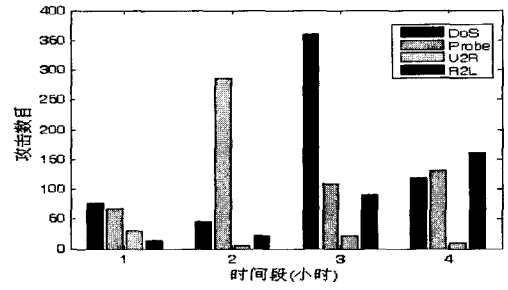


图 5 攻击数目态势

为了获取当前网络的安全态势演化情况，试验中将测试集的数据由 NetPoke 生成网络数据流，按图 2 中模块所示流程，经量化、融合、聚合和评估，根据第 5 部分所描述的态势生成方法，以 15s 为一个时间窗，结合公式(10)、(11)和表 1 中的态势威胁因子，生成两种安全态势图：网络安全态势图和分类安全态势图(图 6 和图 7)。在本文的模型中有多个分类态势图，限于篇幅，只给出了 Probe 和 R2L 的安全态势动态演化图。

通过对系统的安全要素进行量化计算，可以将定性的分析转化为定量的显示，这样可以直观地获得目前的网络安全态势的演化以及目前系统总体和某项异常对网络安全威胁的程度。除此之外还可以利用一些预测技术，比如马尔可夫模型，来预知将来的态势演化情况，便于根据目前的安全威胁提前采取应对措施。

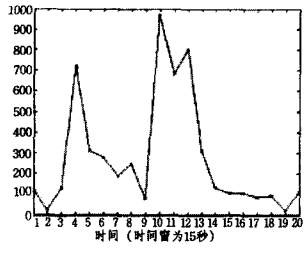


图 6 网络安全态势

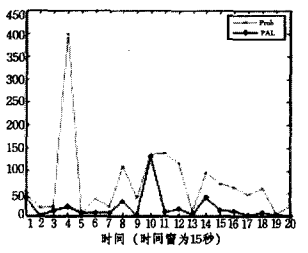


图 7 分类安全态势

结束语 本文设计了一个 NSSA 模型，并结合多传感器融合技术和态势生成技术，实现了一个 NSSA 原型。试验表明，它使安全分析员更直观地感知当前网络的安全态势，也为监控和管理网络带来了新的方法和手段。

NSSA是一项新兴的研究内容，仍有许多未知领域需要做更加深入的探讨。就目前而言，更加有效的NSSA的异质多传感器融合算法仍然需要去探索；安全态势生成算法是单一的态势量化值，仍然需要讨论更多态势要素，找到更多的态势生成和威胁因子赋值算法，从而能够更细粒度地生成网络安全态势；安全态势生成需要综合分析更多的网络安全要素，比如系统漏洞等，而不只是入侵攻击；除此之外NSSA的预测技术也是下一步的重要研究目标。

参 考 文 献

[1] Bass T. Multi-sensor Data Fusion for Next Generation Distributed Intrusion Detection Systems // Proceeding of IRIS National Symposium on Sensor and Data Fusion. 1999

[2] Mica R E. Design and Evaluation for Situation Awareness Enhancement // Proceeding of Human Factors Society 32nd Annual Meeting. Santa Monica, 1988

[3] Steinburg A N, Bowman C L, White F E. Revisions to the JDL Data Fusion Model // Joint NATO/IRIS Conference. Quebec, 1998

[4] John J S, Michael L H, Douglas M B. A Situation Awareness ModelApplied to Multiple Domains // Proceedings of SPIE. 2005, 5813: 65-74

[5] Stephen L. The Spinning Cube of Potential Doom. Communications of ACM, 2004, 47(6): 25-26

[6] Yurcik W. Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suit // 19th Usenix Large Installation System Administration Conference. San Diego, 2005

[7] Carnegie Mellon's SEI. System for Internet Level Knowledge (SILK). http://silktools.source forge.net, 2005

[8] 王慧强，赖积保，朱亮，等. 网络态势感知系统研究综述. 计算机科学，2006，33(10)：5-10

[9] 陈秀真，等. 层次化网络安全态势量化评估方法. 软件学报，2006，17(4)：885-897

[10] 张慧敏，等. 集成化网络安全监控平台的研究与实现. 通信学报，2003，24(7)：155-163

[11] 刘炜，刘鲁. 基于模糊模式识别和D-S证据理论的安全态势估计. 计算机工程与应用，2006，22：20-26

[12] 崔荣一，洪炳熔. 关于前馈神经网络隐层构建问题的研究. 计算机研究与发展，2004，41(4)：524-530

[13] 周晓东，邓伟，陆建德. 多层前馈神经网络的面向对象的程序设计框架. 苏州大学学报，2006，26(1)：57-61

[14] Richard P L, Robert K C. Improving Intrusion Detection Performance Using Keyword Selection and Neural Networks. Computer Networks, 2000, 34: 597-603

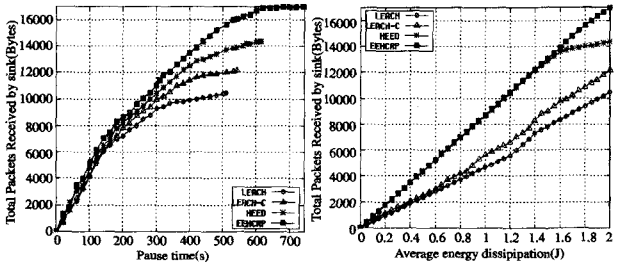
[15] Zhang M, Yao J T. A Rough Sets Based Approach to Feature Selection // Proceeding of the 23rd International Conference of NAFIPS. Banff, 2004

[16] 陈继军. 多传感器管理及信息融合. 硕士论文. 西安：西北工业大学，2002

[17] Lincoln Laboratory. Darpa Intrusion Detection Evaluation. http://www.ll.mit.edu, 1999

[18] Liu X W, Wang H Q, Liang Y, et al. Heterogeneous Multisensor Data Fusion with Neural Network: Creating Network Security Situation Awareness // Proceeding of ICAIA'07. Hong Kong, 2007

（上接第34页）



(c)基站收到的数据量—时间　　(d)基站收到的数据量—能耗

图4

图4(a)对网络中生存节点的个数进行了仿真，图4(b)对全网的能量消耗进行了仿真，从图中可以看到，EEHCRP使得网络的生存周期显著增长，单位时间内全网的能耗更低。从而验证了本文使用混合分簇可以减少簇重构带来的开销，引入胞腔划分算法及多网关机制可以更好地均衡节点之间的能量消耗，从而延长网络的生命周期这一思想。图4(c)和(d)从时间和能量角度分别仿真了基站收到的数据量，以此来表征协议的鲁棒性。从图4(c)中可以看出单位时间内使用EEHCRP，基站收到的数据量更大；从图4(d)中可以看出单位能耗内，使用EEHCRP进行数据传输时，其性能明显优于LEACH和LEACH-C，略优于HEED。这表明EEHCRP具有较强的鲁棒性，这主要是由于本文使用多路径路由树建立簇间路由，使其在链路发生故障时可以在很短的时间内切换到备用路径继续传输采集到的数据。此外频繁的簇重构也会对基站收到的数据量有影响，显然EEHCRP所采用的混合分簇减少了簇重构的次数，提高了基站接收到的数据量。

结束语　分簇路由协议是目前无线传感器网络路由协议研究的主流方向，而如何选举簇头，建立一个什么样的簇以及在生成簇的基础上如何建立簇间、簇内路由是影响网络生命周期的关键因素，也是目前研究的热点。本文针对上述问题，提出一种基于混合分簇的无线传感器网络路由协议(EEHCRP)。EEHCRP使用胞腔算法初始化簇，之后，周期性地根据簇的状态和全网的状态进行局部簇更新和全局簇更新。然后在生成簇的基础上，利用多路径路由树及多网关机制建立簇间路由，使用CMMBCR算法建立簇内路由。仿真实验表明，该方法与同类算法相比不仅有效地均衡了网络能量消耗，延长网络生命周期，而且具有较强的鲁棒性。

参 考 文 献

[1] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless micro networks // IEEE Proceedings of the Hawaii International Conference on System Sciences. 2000: 1-10

[2] Younis O, Fahmy S. Distributed clustering in ad-hoc sensor networks: A hybrid energy efficient approach // Proc. 13th Joint Conf on IEEE Computer and Communications Societies (INFOCOM). 2004, 3(4): 660-669

[3] Heinzelman W. Application - Specific protocol architectures for wireless networks. Ph. D. Thesis. Boston: Massachusetts Institute of Technology, 2000

[4] Toh CK. Maximum battery life routing to support ubiquitous mobilecomputing in wireless ad hoc networks[J]. IEEE Communication Magazine, 2001, 39(6): 138-147

[5] Nasrabadi N M, King R A. Image coding using vector quantization: a review[J]. IEEE Transaction on Communications, 1988, 36(8): 957-971

[6] Wang Y-H, Tsai C-H, Mao H-J, et al. An Energy-Efficient Hiera-rchicalMultiple-Choice Routing Path Protocol for Wireless Sensor Networks[C] // Proceedings of the IEEE International Conference on SUTC'06

[7] 刘明，曹建农，陈贵海，等. EADEEG：能量感知的无线传感器网络数据收集协议[J]. 软件学报，2007，18(5)：1092-1109

[8] 于鹏程，张华忠，刘志杰. 基于聚簇的多跳路由协议的研究[J]. 计算机应用，2007，27(2)：351-354

[9] Sobeih A, Chen W-P, Hou J C, et al. J-sim: a simulation environment for wireless sensor networks[C]//Proceedings of the 38th IEEE Annual Simulation Symposium (ANSS'05). [S. l.]: IEEE Press, 2005: 175-187