软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(8):2099−2114 [doi: 10.13328/j.cnki.jos.004852]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

网络安全态势认知融合感控模型*

刘效武[1], 王慧强[2], 吕宏武[2], 禹继国[1], 张淑雯[1]

[1](曲阜师范大学 信息科学与工程学院,山东 日照 276826)

[2](哈尔滨工程大学 计算机科学与技术学院,黑龙江 哈尔滨 150001)

通讯作者: 刘效武, E-mail: ycmlxw@126.com

摘 要: 为了分析网络威胁的演化趋势,并探讨安全态势的自主感知和调控问题,将跨层结构和认知环融入模型的设计,提出一种基于融合的网络安全态势认知感控模型,增强网络安全系统的层间交互和认知能力.在分析模型组件及其功能的基础上,利用多源融合算法得到各异质传感器对网络安全事件的准确决策,结合对安全事件威胁等级和威胁因子关系的推演,克服威胁因子获取过程中需处理网络组件间复杂隶属关系的不足,从而提出包含服务级、主机级和网络级的层次化态势感知方法,提高对网络威胁的表达能力.而且通过对态势感知曲线的分析,搭建离散计算和连续控制之间的桥梁,形成闭环反馈控制结构,解决安全态势自感知和自调控的问题.仿真实验结果表明:基于融合的网络安全态势认知感控模型及方法能够融合异质安全数据,动态感知威胁的演化趋势,并具有一定的自主调控能力,达到了认知感控的研究目的,为监控和管理网络提供了新的方法和手段.

关键词: 网络安全态势感知;认知计算;多源融合;量化感知;认知调控

中图法分类号: TP393

中文引用格式: 刘效武,王慧强,吕宏武,禹继国,张淑雯.网络安全态势认知融合感控模型.软件学报,2016,27(8):2099−2114. http://www.jos.org.cn/1000-9825/4852.htm

英文引用格式: Liu XW, Wang HQ, Lü HW, Yu JG, Zhang SW. Fusion-Based cognitive awareness-control model for network security situation. Ruan Jian Xue Bao/Journal of Software, 2016,27(8):2099−2114 (in Chinese). http://www.jos.org.cn/1000-9825/4852.htm

Fusion-Based Cognitive Awareness-Control Model for Network Security Situation

LIU Xiao-Wu[1], WANG Hui-Qiang[2], LÜ Hong-Wu[2], YU Ji-Guo[1], ZHANG Shu-Wen[1]

[1](School of Information Science and Engineering, Qufu Normal University, Rizhao 276826, China)

[2](School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract: For the purpose of exploring the evolution trend and analyzing the autonomous awareness and control problems, this paper proposes a cognitive awareness-control model for network security situation based on fusion. This model is characterized by the design of the cross-layer architecture and cognitive circle which can improve the interactive and cognitive ability between the different network layers. Based on the analysis of the model components and their functions, this paper uses the fusion algorithm to obtain the accurate decision on the security events made by heterogeneous multi-sensor. Combining with the reasoning of the relation between threat gene and threat level, a hierarchical quantification method is put forward, encompassing service layer, host layer and network layer. This approach has the advantage of overcoming the shortcoming of dealing with the complex memberships among network components and improving the expression ability against network threat. In addition, through establishing the bridge between dispersed computing and the continuous control, the close-up feedback structure is formed and the self-awareness and self-control problems are solved. The simulation experiments prove that the presented model and algorithms can fuse heterogeneous security data, dynamically perceive the evolution trend

* 基金项目: 国家自然科学基金(90718003, 61370212); 教育部博士点基金(20122304130002); 山东省高校科技计划(J11LG09)

Foundation item: National Natural Science Foundation of China (90718003, 61370212); Ph.D. Programs Foundation of the Ministry of Education of China (20122304130002); Shandong Province Higher Educational Science and Technology Plan of China (J11LG09)

收稿时间: 2013-09-22; 采用时间: 2015-05-08

of network threat and possess the autonomous regulation and control ability. This study meets the research goal of cognitive awareness-control and it provides a new method of monitoring and administrating the networks.

Key words: network security situation awareness; cognitive computing; multi-source fusion; quantification awareness; cognitive control

当今网络与信息技术在经济、社会、国防中的作用日益重要,已上升到关系国家和全民利益的高度,逐渐成为经济发展和国家战略部署的重要因素.然而,当前网络系统的异构异质性、复杂性、使用环境的持续恶化、规模的不断扩大以及各种新兴应用的不断涌现,传统"堵漏洞、作高墙、防外攻"的安全模式因缺乏自适应性、统一调度和有效协同,从而导致网络入侵和破坏行为普遍存在,造成重大经济损失,带来恶劣社会影响,甚至酿成机毁人亡的重大责任事故.

网络安全态势感知(network security situation awareness,简称 NSSA)被认为是解决网络安全领域中存在问题的一种新途径,它能够融合各网络部件对安全事件的检测,并实时感知网络安全状况和面临的风险,已成为国际上一个前沿且具有多学科交叉性质的热点研究领域.自 1999 年 Bass[1]提出基于多传感器融合的态势感知模型起,融合模型成为这一阶段的代表性研究,包括 Tadda 等人[2]提出的由要素提取、状态感知和态势预测组成的三级模型以及由 Shen 等人[3]提出的网络态势融合感知与风险评估模型.同时,可视化技术也是 NSSA 研究初始阶段的重要分支,劳伦斯伯克利国家实验室、美国国家高级安全系统研究中心等国外军事部门和研究中心开发了诸如"Spinning Cube Potential Doom"[4],NVisionIP[5]等可视化态势感知软件,甚至至今,态势可视化仍是一大研究方向[6].在 NSSA 研究的这一时期,较关注框架模型的构建和可视化工具的开发,但模型所涉及的方法和机制仍待应用验证;且在大型网络中,单纯通过网络流量和连接状况的可视化,也很难准确地获得网络安全态势.

2006 年,陈秀真等人[7]提出了层次化的网络安全威胁态势量化评估方法,虽然该研究中威胁权值仍依靠专家经验,也未对融合感知做深入探讨,但其提出的层次化威胁评估理念对态势感知的研究具有重要的推动作用.这一阶段,在层次量化感知的研究方向上呈现出了蓬勃发展的局面,其中尤其值得关注的是 Hu 等人[8]提出的 AHP 层次分析方法.但此类方法中仍存在态势知识表达不健全、态势威胁因子主观依赖较大、获取困难等问题.

从 2008 年开始,融合感知逐渐成为 NSSA 研究领域的热点,且融合算法是研究过程中的核心内容之一.由于网络安全事件的随机性和突发性,获取其先验概率和条件概率的难度大,难以处理融合过程中的不确定性.而 D-S 证据理论切合了态势感知对多源融合的需求,数据通信量需求小,推理过程对先验概率要求低,在处理不确定方面也表现出了良好的适应性.韦勇等人[9]提出了基于 D-S 线性加权的融合感知方法,而 Zhang 等人[10]则采用平均法改进 D-S 合并规则,处理 NSSA 的融合感知问题.上述对 NSSA 融合感知的研究,证实了融合感知的可行性,但在对 D-S 证据融合改进的过程中,仍存在辨识框架不归一和融合冲突问题.

自 2010 年以来,态势感知的认知能力和反馈控制问题引起了研究者的极大关注,也出现了诸多代表性的研究成果.文献[11]认为,认知感知是目前信息融合领域的重要挑战,并探讨了依赖型理论、扩展构造函数等认知态势感知的形式理论基础问题;龚正虎等人[12]在提出的网络态势框架中强调了 NSSA 研究的反馈控制结构,并认为,扩展控制循环模型(OODA)提供了处理多并发、潜在交互的数据融合机制;张勇等人[13]构建了一个基于 Markov 博弈的 NSSA 模型,虽然其研究核心是利用风险传播网络构建三方参与的博弈模型,但所提出的安全系统加固理念强调了态势感知研究中不仅要实现威胁状况的感知,也应关注系统状态的控制.

认知计算被认为是解决目前 NSSA 研究中问题的一种新机制,其中对认知环、跨层结构和自适应性研究尤其值得关注.虽然其中对认知环的构造形式和跨层的体系结构仍存在较大分析,但已出现了诸多重要意义的研究成果.Thomas 等人[14]和 Fortuna 等人[15]赞同认知计算应采用类似于 OODA 环的设计,从而提升系统的认知能力.跨层设计是认知计算的又一研究热点,也是学术界较为普遍接受的结构形式.Clark 等人[16]和 Shakkottai 等人[17]认为,跨层结构是认知计算的基础,能够克服传统网络层次间信息交互困难的弊病,并已在无线网络的信道管理[18]、自干扰[19]和路径选择[20]等研究中得到了初步应用和检验,但仍存在只针对特定网络层次、优化功能重叠等不足.

认知计算的自主特性和动态配置能力,也被认为是实现系统自适应性的可行途径.学术界,Gomez 等人[21]提出了一个认知计算框架 ALOE(abstraction layer and operating environment),能够实现为实时执行的系统平台提

供动态配置、资源感知和运行控制等功能;Gupta[22]和 Ogiela 等人[23]都认为,认知计算具有自主的推理和感知的能力,能够模拟学习、记忆、推理和感知等认知功能,可被应用于安全、信息系统决策等诸多领域.上述研究为采用认知计算实现具有自主特性、感知和学习能力的智能系统提供了可行的理论基础.而国外的军方和科研机构则纷纷从认知计算动态配置能力的角度展开各自的研究计划,如:美国国家自然科学基金、DARPA、NASA 资助了 BNA(bio-networking architecture project)[24],Rainbow[25]等研究;欧盟也展开了第七框架计划(FP7)[26]的研究,此类研究计划以系统实证的方式验证认知计算能够建立自适应性系统,并可提供一种自管理的新方法;在国内,采用认知计算提升系统认知能力的研究还较少,虽然文献[27]中提出了一个网络攻击认知模型,可实现对攻击步骤、攻击行为和攻击过程的认知,但更多研究仍较集中于对计算系统资源的复杂管理[28]和 QoS 水平的动态配置[29].究竟何种类型认知结构和机制适用于 NSSA,仍待理论探讨和实际验证.

从NSSA的发展进程来看,随着新兴系统的出现和下一代网络应用到来,NSSA 已从感知网络向感控网络过渡.本文在吸取已有研究成果的基础上,将认知理念融入对安全态势感知的研究,提出了网络安全态势认知融合感控模型,研究适用于异质传感器环境的多源融合算法,实现对网络安全态势的动态量化感知,并探讨 NSSA 的调控机制,从而形成闭环反馈控制结构,感知外部环境信息,控制内部运行状态,建立离散计算与连续控制之间的桥梁,达到认知感控的目的.

1 NSSA 认知感控模型

本文在网络安全态势层次感知的基础上,将认知理念融入 NSSA 的框架设计,提出基于融合的网络安全态势认知感控模型,如图 1 所示.

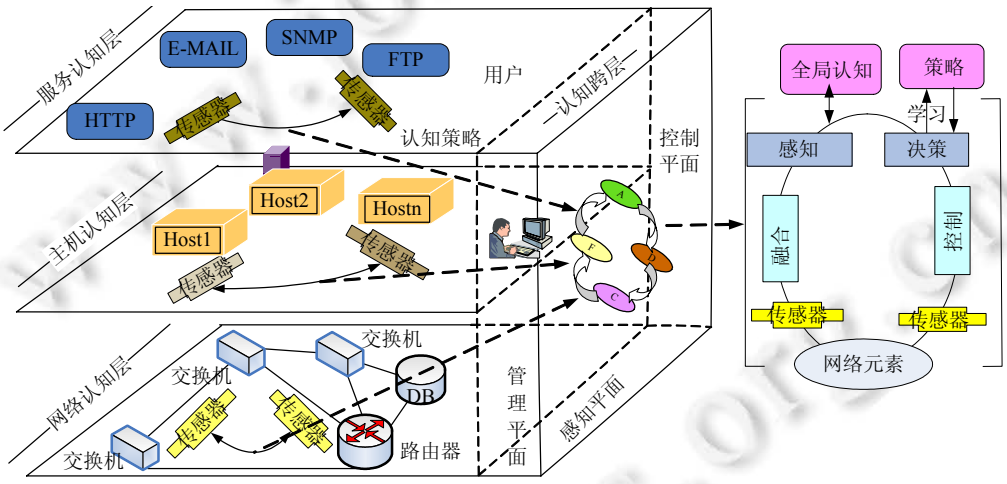


Fig.1 Network security situation cognitive awareness-control model

图 1 网络安全态势认知感控模型

该模型包括 4 个层次,分别是网络认知层、主机认知层、服务认知层和跨层结构.网络认知层包括路由器、交换机等运行协议栈的网络实体,并包含位于该层的各种流量传感器、NIDS、防火墙等类型的安全部件;而主机认知层主要由网络和计算系统的软硬件资源构成,并包含了 HIDS、日志分析等各类传感器;服务认知层主要包含网络系统所提供的各种服务,也包括支撑系统运行的策略、用户接口、检测和管理服务运行状态的传感器等;在该模型中,跨层结构是区别于传统网络结构的关键层次,其既继承现有网络的分层体系和 NSSA 的层次感知需求,又能够解决严格层次划分带来的信息流通不畅问题,使信息在安全系统的各不相邻层次之间传递,更好地应对复杂网络威胁,其核心是由融合(fusion)、感知(awareness)、决策(decide)和控制(control)组成的 FADC 认知环,并通过组件之间的协作形成闭环反馈控制结构,使 NSSA 具备异构、并发、同步等特性,如图 2 所示.

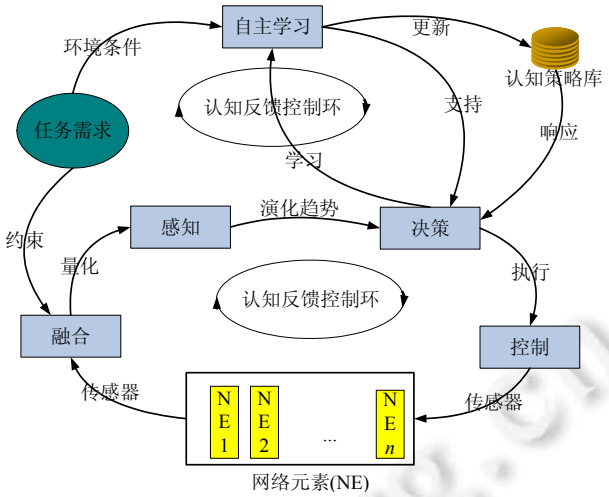


Fig.2 Cognitive circle synchronization response model

图 2 认知环的同步响应模型

2 多源融合与 CPSO-DS

多源融合是感知的基础,其决定着 FADC 认知环中感知、控制等组件的准确性和鲁棒性.虽然 D-S 证据理论是 NSSA 融合算法研究中被广泛采用的一种决策层融合算法,但对不同层次、不同属性的传感器赋予相同的可信程度,极易出现 Zadeh 悖论,从而大大降低 NSSA 的感控精度.对 D-S 证据融合的研究中,证据加权被广泛采用,但仍存在线性加权[9]不满足证据组合规则的结合律、指数加权[30]依赖经验递推的问题,准确性不高,对未来样本的适应能力有限,重新获取新权值的代价较高.鉴于此,本文提出跨层群粒子优化(cross-layer particle swarm optimization,简称 CPSO)算法改进传统 D-S 证据融合,解决跨层融合问题,如图 3 所示.

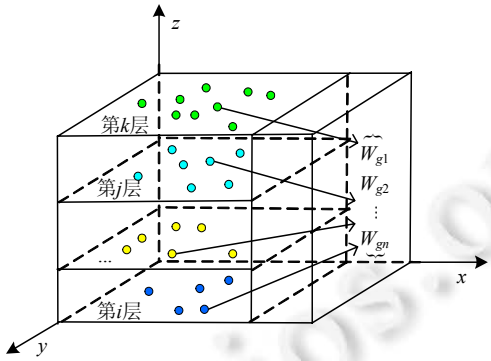


Fig.3 Cross-Layer particle swarm optimization

图 3 跨层粒子群优化

利用粒子群的速度和位置更新公式(1),搜索 D-S 证据融合过程中的指数优化权值:

$$\begin{cases} v_{td} = w \cdot v_{td} + c_1 \cdot rand\_num \times (p_{td} - x_{td}) + c_2 \cdot rand\_num \cdot (p_{gd} - x_{td}) \\ x_{(t+1)d} = x_{td} + v_{td} \end{cases} \tag{1}$$

其中,t=1,2,…,S,S 是粒子群体规模;c_1 和 c_2 为常数,是将微粒推向局部最优 p_{td} 和全局最优 p_{gd} 的统计加权权重;$rand\_num$ 为[0,1]之间的随机数;w 为递减惯性权值.在融合参数寻优的过程中,还要满足适应度函数(2):

$$F_i=\max\{m(A_i)-\max\{m(A_j)\}|j\neq i,j=1,2,\ldots,i-1,i+1,\ldots,h\} \tag{2}$$

其中,h 为命题个数;$m(A)$为其他命题的合成基本概率分配(basic probability assignment,简称 BPA);决策目标 A_i 对应的 BPA 为 $m(A_i)$;$F_i(1\leqslant i\leqslant h)$为决策目标 A_i 的适应度函数,含义为,经加权融合之后,使得决策目标的 BPA 与其他非决策目标的 BPA 差值最大,即,更准确地判断决策目标的所属类别.在适应度函数的约束下,跨层粒子群为不同传感器来源的数据赋予不同的指数融合权值:$w_1,w_2,\ldots,w_h$,则 D-S 的指数加权融合公式演化为式(3):

$$m(A)=\frac{\sum_{A_1\cap A_2\cap\ldots\cap A_h=A} m_1(A_1)^{w_1}m_2(A_2)^{w_2}\ldots m_h(A_h)^{w_h}}{1-K_h} \tag{3}$$

其中, $A\neq\phi, K_h=\sum_{A_1\cap A_2\cap\ldots\cap A_h=\phi} m_1(A_1)^{w_1}m_2(A_2)^{w_2}\ldots m_h(A_h)^{w_h}$.

通过此处理过程,既满足 D-S 证据理论辨识框架归一、结合律、分配率等基本属性,又能对不同安全数据源赋予不同的可信程度,减低融合冲突,提高融合精度,减少不确定性.而且在出现新的安全事件时,可利用 PSO 不需要对已学习样本进行重新训练的优势,自主调整融合权值,达到自适应的目的.

3 网络安全态势量化感知

经过 CPSO-DS 跨层优化融合,解决了数据的准确性、一致性等问题.态势感知则是依据融合结果,以态势要素提取和层次威胁评估为关键问题,生成网络系统的动态演化视图.

3.1 态势要素提取

对于一个成功的 NSSA 系统而言,有效的感知依赖于准确的要素提取.态势要素的构成应当包含网络中所有能够引起态势变化的关键因素,比如攻击威胁因子(威胁程度)、攻击强度(事件频率)、资产重要性等.其中,资产重要性、攻击强度等为易知属性,但威胁因子生成是目前的难点研究内容.从研究现状来看,经验递推[7,9]和 AHP 层次分析方法[8]是威胁因子研究中较为成功的研究方案.但经验递推方法较依赖专家经验,主观性强、获取难度大;AHP 方法需要对问题组成因素的关联影响及隶属关系做复杂的推演.本文将权系数生成理论[31]引入到 NSSA 领域,并研究其与 NSSA 的拟合.设网络环境中存在 n 类目标需要分配威胁因子,决策目标为 n 种不同类型的事件获取 m 个威胁因子.把每个威胁因子看作一随机变量 x_i,值取 1 和–1,目的是使得该随机变量满足均值为 0 的分布.令 $X_n=\sum_{i=1}^{n}x_i, Y=\frac{X_n}{\sqrt{n}}$,当 $n\to\infty$时,Y 服从正态分布,则 X_n 渐进的服从正态分布 $N(0,\sqrt{n})$,则正态分布曲线的横坐标为决策目标的重要性(威胁因子大小),纵坐标为决策目标的数目(按威胁等级由高到低排序).根据正态分布的特性,可将威胁因子模式做如下描述:对网络安全态势影响越大,事件的威胁因子越靠近第一象限偏右的位置;反之,其威胁因子在第二象限越靠左的位置,如图 4 所示.下面将通过推理简化威胁因子的获取过程,使得仅在已知威胁等级的情况下,简易地计算威胁因子.

对正态分布曲线的纵坐标以 α为比例因子做如图 5 所示的等间隔划分,将第 2 象限的曲线以直线 $f(x)=A$ 为对称轴进行变换,并将纵轴左移 3σ,得图 6.

图 6 中,纵坐标为自变量(排队等级),横坐标为函数(威胁因子大小),不符合常规的函数表达方式.为此,对图 6 继续做坐标变换为图 7,取正态分布的密度函数 m=0,并解出 x 关于 $f(x)$的表达式,用 y 代替 x,x 代替 $f(x)$:

$$y=\begin{cases}3\sigma+\sqrt{-2\sigma^2\ln[\sigma\sqrt{2\pi}x]}, & 0<x<\dfrac{1}{\sigma\sqrt{2\pi}}\\ 3\sigma, & x=\dfrac{1}{\sigma\sqrt{2\pi}}\\ 3\sigma-\sqrt{-2\sigma^2\ln\left[\sigma\sqrt{2\pi}\left(\dfrac{2}{\sigma\sqrt{2\pi}}-x\right)\right]}, & \dfrac{1}{\sigma\sqrt{2\pi}}<x<\dfrac{2}{\sigma\sqrt{2\pi}}\end{cases} \tag{4}$$

由公式(4)可知,目标等级取值区间为 $\left(0,\frac{2}{\sigma\sqrt{2\pi}}\right)$.将其 n 等分 $\left(x_i=\frac{i}{n}\times\frac{2}{\sigma\sqrt{2\pi}},1\leqslant i\leqslant n\right)$ 代入公式(4),则与 x_i

相对应的 y_i 为排队等级 i 的威胁因子.由图 7 可知,最大威胁因子 $y_{\max}\approx 6\sigma$,则第 i 个威胁因子(G_i)可量化为

$$G_i=\frac{y_i}{y_{\max}}=\begin{cases}\dfrac{1}{2}+\dfrac{\sqrt{-2\ln\dfrac{2i}{n}}}{6}, & 1\leqslant i<\dfrac{n}{2}\\ \dfrac{1}{2}, & i=\dfrac{n}{2}\\ \dfrac{1}{2}-\dfrac{\sqrt{-2\ln\left[2-\dfrac{2i}{n}\right]}}{6}, & \dfrac{n}{2}<i<n\end{cases} \tag{5}$$

至此,威胁因子获取仅需已知不同的威胁类型(n),并针对每种类型威胁对网络的危害程度大小排序(i),即可得到第 i 等级事件的威胁因子.此种威胁因子获取方法具有较好的环境迁移性,当 NSSA 应用于具有不同攻击敏感度的网络时,仅需对威胁类型重新排列等级即可.该方法可以大大降低威胁因子获取的复杂度,改善威胁因子获取主观性较强、复杂度高、依赖专家经验的现状.

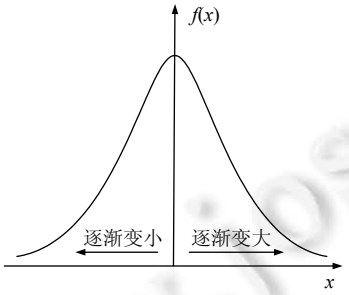


Fig.4 Threat gene pattern

图 4 威胁因子模式

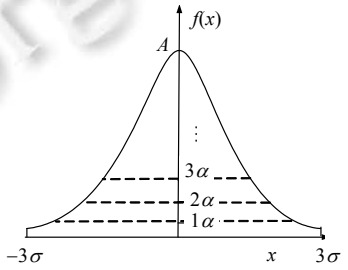


Fig.5 Threat equal interval separation

图 5 威胁等间隔划分

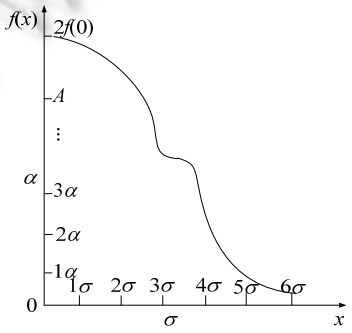


Fig.6 Symmetry axis transformation

图 6 对称轴变换

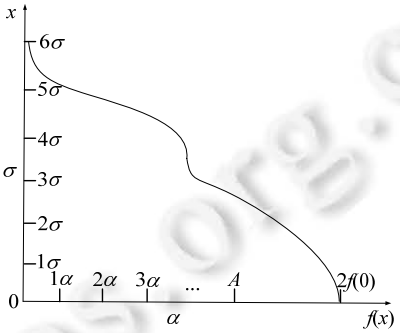


Fig.7 Coordinate transformation

图 7 坐标变换

3.2 威胁量化评估

本文将网络安全态势分为服务级、主机级和网络级这 3 个不同的级别,核心思想是:在 3 个不同层次上的安全态势值均以网络系统对攻击类型的敏感程度为基础,按照以态势要素为中心的观点实现层次量化感知.

3.2.1 服务安全态势

定义 1(威胁因子). 在时间窗口 tw 内,服务 $s_i(0\leqslant i\leqslant u)$遭受到 n 种不同类型的攻击 $a_{ij}(0\leqslant j\leqslant n)$,按照攻击对服务 s_i 的威胁程度排队,可将 n 个的攻击分为 $g(1\leqslant g\leqslant n)$个不同的威胁等级(多种不同类型的攻击可属于同一威胁等级),则等级 k 的威胁因子为

$$l_k=\begin{cases}\dfrac{1}{2}+\dfrac{\sqrt{-2\ln\dfrac{2k}{n}}}{6}, & 1\leqslant k<\dfrac{n}{2}\\ \dfrac{1}{2}, & k=\dfrac{n}{2}\\ \dfrac{1}{2}-\dfrac{\sqrt{-2\ln\left[2-\dfrac{2k}{n}\right]}}{6}, & \dfrac{n}{2}<k<n\end{cases} \tag{6}$$

根据攻击类型的不同,由定义 1 可以确定攻击对服务的威胁程度量化权重.除此之外,服务安全态势还与攻击强度有关,据此得出定义 2.

定义 2(服务安全态势). 在定义 1 的前提下,g 种不同的攻击的威胁因子量化权重为 $l_k(1\leqslant k\leqslant g)$;服务 s_i 遭受到各类攻击的总数目为 N_i,其中,第 $j(0\leqslant j\leqslant g)$类攻击的数目记为 N_{ij},称为攻击强度,且满足 $N_i=\sum_{j=0}^{g}N_{ij}$.则服务 s_i $(0\leqslant i\leqslant u)$的安全态势为

$$V_{S_i}=\sum_{k=1}^{g}(N_{ik}10^{l_k}) \tag{7}$$

其中,u 为服务的数目.公式(7)使用 10^{l_k} 的目的是强调威胁因子的重要性,弱化攻击强度对服务安全态势的影响.

3.2.2 主机安全态势

主机安全态势不仅与主机上的运行的服务数目和服务安全态势有关,而且与服务相对于主机的重要程度相联系.

定义 3(主机安全态势). 在时间窗口 tw 内,主机 $H_l(0\leqslant l\leqslant v)$上运行 u 种服务,服务 s_i 的重要程度以服务失效后产生不良后果的程度为依据确定为 f_{s_i} $(0\leqslant i\leqslant u)$,则主机安全态势为

$$V_{H_l}=\sum_{i=1}^{u}(V_{s_i}f_{s_i}) \tag{8}$$

其中,主机服务 H_l 上存在的 u 种服务,按照重要程度赋予威胁程度为 $(t_{s_1},t_{s_2},...,t_{s_u})$,并对其归一化:

$$f_{s_i}=\frac{t_{s_i}}{\sum_{j=1}^{u}t_{s_j}}.$$

3.2.3 网络安全态势

网络安全态势由时间窗 tw 内主机安全态势和主机数目等组成.

定义 4(网络安全态势). 在时间窗口 tw 内,网络系统 NS 中存在 v 台主机,其中,主机 $H_l(1\leqslant l\leqslant v)$的重要程度权重为 g_{H_l} $(1\leqslant l\leqslant v)$,则网络安全态势为

$$V_{NS}=\sum_{i=1}^{v}(V_{H_i}g_{H_l}) \tag{9}$$

其中,主机重要性由主机上运行关键服务数目、资产值和是否存在机密数据等确定为 $(t_{H_1},t_{H_2},...,t_{H_v})$,并对其归一化得主机权重:

$$g_{H_l}=\frac{t_{H_l}}{\sum_{j=1}^{v}t_{H_j}}.$$

网络系统中,V_{NS} 数值越大,说明网络系统中所面临的威胁越严重;反之,网络系统较为安全.与入侵检测相区别的是,安全态势感知技术将离散的报警事件映射为连续的安全状况演化曲线,直观地表达当前网络系统面临的威胁及演化趋势,结合可视化技术,即可生成分层次、按区域的二维曲线,也可构建多要素、全方位的多维动态演化视图,直观感知服务、主机和网络等多个不同抽象程度的安全态势,为监控和管理网络提供新的方法和

手段,也为安全控制提供参考依据.

4 认知调控

当前服务和应用对高安全性的需求,促使安全系统不仅能够保护各种应用,也促使其具有动态演化特性,具备一定的自管理和自调控能力.而采用认知理念的自主调控机制,可以通过对安全态势曲线的分析,反映网络系统的安全性演化,从而选择恰当的调控方法,保证系统的高安全性.

4.1 二维感知曲线认知调控

在态势感知的过程中,量化感知通常会生成离散的态势威胁值,无法满足连续调控的需求.而且采用手动加固的方式[13],对管理员要求高,实时性差,出错概率大.为满足连续调控的研究需求,本文提出一种基于态势瞬时梯度的认知调控机制,达到 NSSA 自主调控的目的,并最终实现 FADC 的闭环反馈结构.对离散威胁量化态势值,可采用 Lagrange 插值[32]方法实现离散态势值与连续曲线的拟合或分段拟合,生成连续的安全态势感知曲线.设该曲线 D 为态势值的函数,若 D 为二维曲线,可利用公式(10)计算其瞬时态势梯度:

$$G_d(x_1,x_2)=\frac{\partial f}{\partial x_1}\vec{i}_1+\frac{\partial f}{\partial x_2}\vec{i}_2 \tag{10}$$

分析影响安全态势感知的环境因素(资源、漏洞、操作、响应、算法、参数、稳定性等)之间相互联系、相互影响的制约关系,对其进行描述、量化、传递及综合,结合认知单元预设策略库,在线评估当前时刻的安全态势值 d,计算其瞬时梯度 G_d,并结合安全态势历史先验变化曲线,搜索与该点具有相同梯度的前驱点集 $P_{Gd}=\{P_1,P_2,\ldots,P_n\}$;依次记录梯度增长的后继邻接点 $S_{Gd}=\{S_1,S_2,\ldots,S_n\}$;以 P_{Gd} 为始点设定梯度滑动窗口,观察安全态势变化梯度的演化趋势,调用相应的应对方案对传感器、融合及量化等组件进行认知调整,如图 8 所示.

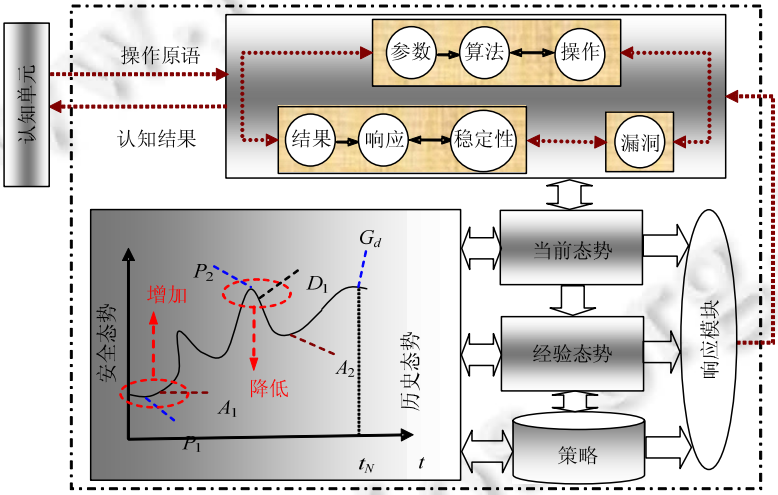


Fig.8 Two-Dimension situation curve cognitive regulation and control choice mechanism

图 8 二维态势曲线的认知调控选择机理

以态势梯度为依据,对不同的梯度变化情况,依据下述情况选择不同的应对策略,实现对态势感知的自主决策和执行.

(1) 梯度增长,即,P_i 与 S_i 之间的安全态势值持续增长时:依据先验态势感知曲线找出 S_{Gd} 各成员的〈触发条件(trigger condition)→应对策略(strategy)〉集 $S_{CS}=\{\langle TC_1\rightarrow TS_1\rangle,\langle TC_2\rightarrow TS_2\rangle,\ldots,\langle TC_n\rightarrow TS_n\rangle\}$尝试调节触发条件,计算先验梯度增长极大值 $\max\{S_{CS}\}$;最终选择 $\max\{S_{CS}\}>d$ 的调节策略进行当次触发条件的响应,将结果反馈至认知单元,调节融合和感知的相关参数,并利用效应器执行相应的动作.一旦出现

$\max\{S_{CS}\}<d$ 的情况,则调用策略库,对所有可能的触发条件依据相互之间的依赖关系自底向上依序尝试,找出最大 $d_{T_{\max}}$,实施当次响应.之后记忆 $d_{T_{\max}}$ 对应的 $\langle TC_{T_{\max}} \rightarrow TS_{T_{\max}} \rangle$,扩展先验态势感知变化曲线,以便适用于类似情况下的安全事件响应.

(2) 梯度不变,即 P_i 与 S_i 之间的安全态势值不变时:实施 S_{Gd} 响应策略.

(3) 梯度下降,即 P_i 与 S_i 之间存在安全态势下降点集 $D_d=\{d_1,d_2,\ldots,d_m\}$ 时:扩大滑动窗口步长,采用与情形(1)相同的机理实施当次响应.

4.2 多维感知曲线认知调控

对于 NSSA 包含了多个独立子系统或者具有多个安全目标时,可将二维态势曲线的调控机理推广到态势曲线为多维的情况.此时,公式(11)即为态势多维图像的瞬时态势梯度:

$$G_d(x_1,x_2,\ldots,x_l)=\frac{\partial f}{\partial x_1}\vec{i}_1+\frac{\partial f}{\partial x_2}\vec{i}_2+\ldots+\frac{\partial f}{\partial x_l}\vec{i}_l \tag{11}$$

对应的调控策略选择步骤与二维的情况一致.通过上述处理,安全态势感知系统具备了无人干预的自主决策与执行,最终形成封闭式 FADC 反馈控制认知环,既能改变融合和感知的参数,又能根据态势梯度主动执行调控策略,达到 NSSA 认知感控的目的.

5 仿真实验与分析

5.1 融合性能

根据研究需求,设计如图 9 所示的网络拓扑结构,分别部署 Netflow,Snort 和 Snmp 等 3 类传感器,检测各层次数据,并利用 XML 技术完成跨层异质传感器数据传递和格式化处理;3 类传感器与跨层认知环组件的关系以及 Snmp 传感器的设计结构如图 10 所示.

训练集与测试集选取 DARPA 99 入侵检测数据的 10%数据集的 20%和 9%(表 1),数据选取的过程中,基本按照现实网络中攻击类型的流量比例选取,并采用 Netpoke 重放,以期最大程度的仿真互联网络.利用 3 类传感器的检测结果对 CPSO-DS 融合引擎进行多轮次训练,群体规模为 55,在[0,1]内搜索优化权值,结合离线寻优和在线调整,降低噪声对优化权值的影响,并利用期望偏差以及 Netflow 的端口变化率和流量出入比获取异质传感器的 BPA,见表 1.

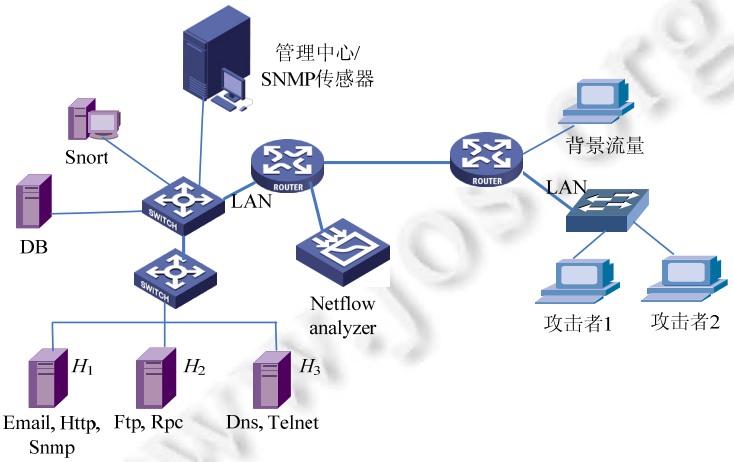


Fig.9 Network topology

图 9 网络拓扑结构

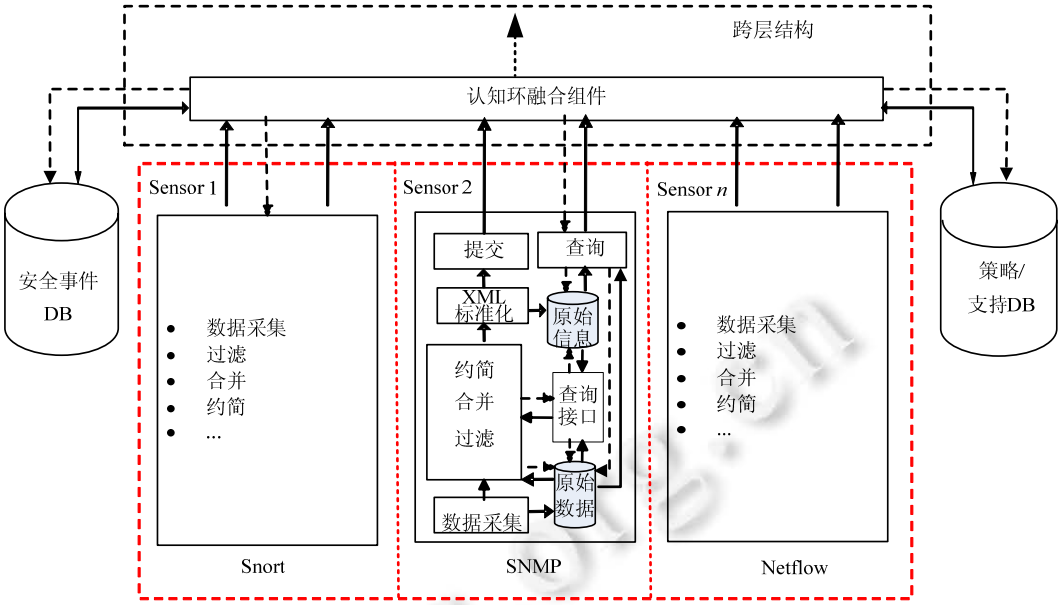


Fig.10 Relations between sensors and cognitive circle components

图 10 传感器与认知环组件关系

Table 1 Basic experiment data

表 1 基本实验数据

类型	训练集	测试集	$BPA_{Netflow}$	BPA_{Snort}	BPA_{Snmp}	$w_{Netflow}$	w_{Snort}	w_{Snmp}	威胁等级	威胁因子
R2L	226	98	0.098	0.194	0.347	0.26	0.71	0.67	1	0.726
U2R	31	11	0.146	0.203	0.261	0.23	0.91	0.69	1	0.726
DoS	78291	33665	0.283	0.189	0.167	0.93	0.34	0.22	2	0.611
Probe	822	354	0.367	0.288	0.188	0.88	0.60	0.41	3	0.389
New	*	*	0.106	0.126	0.037	0.58	0.71	0.43	0	1

依据图 9 的网络拓扑,利用 CPSO-DS 对重放测试集产生的报警进行融合,并与不加权的传统 D-S、经验权值 D-S 融合[30]、两数据源融合的 PSO-DS[33]在检测率(DR)和误警率(FDR)方面进行了比较,见表 2.

Table 2 Fusion ability

表 2 融合性能

参数	传统 D-S (%)	经验加权 D-S (%)	PSO-DS(两数据源) (%)	CPSO-DS(三数据源) (%)
DR	73.33	82.60	86.67	88.11
FDR	9.86	5.80	5.63	5.06

实验结果表明,CPSO-DS 多源融合在检测率、误警率上都优于其他方法;而且与文献[33]中采用两个传感器研究比较而言,传感器数目增加有助于提高检测率,降低误警率.实验过程中,从 U2R 和 R2L 的角度,单纯靠传感器数目增加较难改善其检测效率,应设计更多基于主机的传感器,从而更显著提高其检测能力.除此之外,从两数据源和三数据源的性能比较上,增加数据源可以带来准确性的提升,但有时并不能显著提升融合准确性,亦即:对于多源融合而言,数据源的数目也并非越多越好,融合的准确性与所加入传感器本身的检测性能和特性密切相关.

5.2 层次量化感知

5.2.1 服务安全态势

根据 CPSO-DS 融合引擎的输出,即可按照要素提取、要素量化和层次感知等的步骤进行威胁评估.本感知

方法需量化攻击强度、攻击类型和威胁因子等.攻击强度可通过对 CPSO-DS 融合引擎的输出,在时间窗口内统计确定.攻击类型及其威胁排队等级见表 1,并根据公式(6)计算威胁因子(n=5,g=4).仿真网络共运行一周(2013 年 6 月 10 日~2013 年 6 月 16 日),攻击方包含两个终端,由其自主安排攻击时间,在防守方不知情的情况下模拟黑客行为,将测试集的攻击数据向局域网选择性重放,并按照公式(7)获取某一服务的安全态势动态演化曲线.图 11 所示为主机 H_1 上所运行的 Email,Http 和 Snmp 这 3 种服务经拟合后的安全态势演化视图,横坐标为时间,长度为 7 天,时间窗口大小为 2 小时;纵坐标为服务安全态势值,表达攻击对服务的威胁程度.

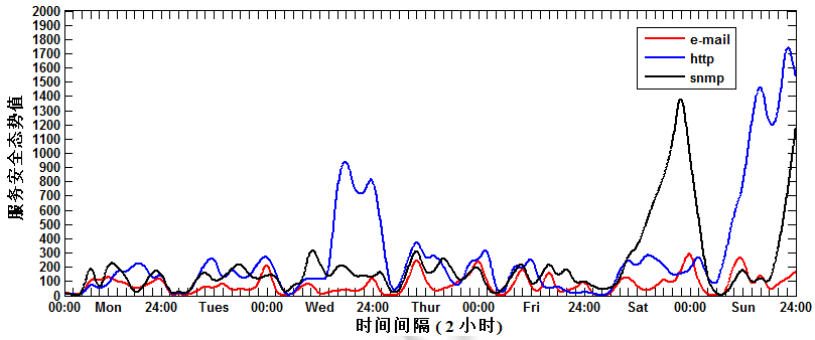


Fig.11 Service security situation

图 11 服务安全态势

从图 11 中可以直观地看出,Http 和 Snmp 服务均在周日遭受到严重的攻击;在周三下午和晚上,Http 的安全状况也应关注;而 Snmp 在周六深夜受到了较大威胁;Email 服务整个监控时段内安全态势较为平稳.根据服务安全态势感知曲线,网络分析员应在威胁较为严峻的时段对所管理服务加强监管,并对并对漏洞、配置情况等做进一步检查.从服务安全态势视图中还可以看出,在某一时间段内,安全威胁存在渐进严重的规律性,管理员应根据服务安全态势及其趋势,提前采取相应措施.限于篇幅,本文仅展示主机 H_1 上 E-mail,Http 和 Snmp 的安全态势,对主机 H_2 和 H_3 的服务安全态势演化视图不再一一列举.

5.2.2 主机安全态势

主机安全态势与主机上运行的服务和服务失效后所产生的不良影响程度相关.从主机 H_1 的角度,其 E-mail,Http 和 Snmp 这 3 种服务的重要程度 t_{s_i} 分别设为中、高、低这 3 个等级,则主机 H_1 的安全态势根据公式(8)获取.对于主机 H_2 和 H_3 可采用类似的方式处理,形成主机安全态势动态演化视图,如图 12 所示.

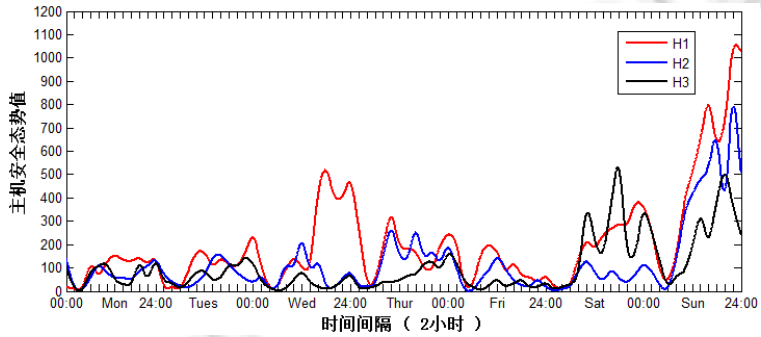


Fig.12 Host security situation

图 12 主机安全态势

对于主机 H_1,在周三的下午和晚上出现了较为严重的攻击态势;3 台主机在周末遭受了大量的攻击,并且可以反映攻击者的活动规律,较为严重的攻击一般发生在下午或晚间,在这些时段管理员需对所管理的网络加强

监控,并在威胁来临之前,提前制定应对策略.

5.2.3 网络安全态势

网络安全态势的感知需要确定主机重要性权重,但主机权重的确定要比服务权重复杂,其与主机资产价值(V_h)、服务关键程度(C_s)、访问频率水平(A_f)和是机密程度(D_c)等许多因素相关,其重要性等级见表 3,其中,主机复合重要性 $t_{H_1}=k_V V_{h_i}+k_C C_{s_i}+k_A A_{f_i}+k_D D_{c_i}$,k_V=0.2,k_C=0.3,k_A=k_D=0.25.在主机安全态势的基础上,利用表 3 获取主机的复合重要性权重,利用公式(9)可生成整个网络系统的安全态势演化视图,如图 13 所示.

Table 3 Host weight grade

表 3 主机等级

主机	V_{h_i}	C_{s_i}	A_{f_i}	D_{c_i}
H_1	高	中	中	高
H_2	中	低	中	中
H_3	中	低	低	低

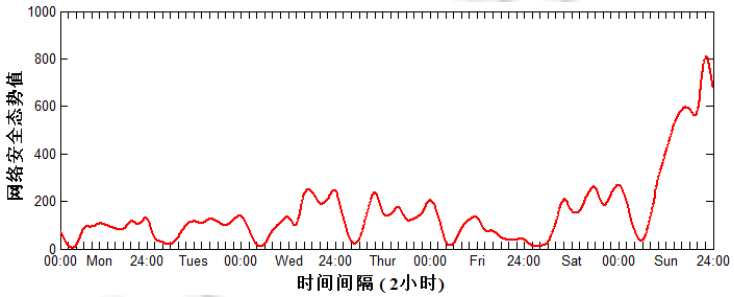


Fig.13 Network security situation

图 13 网络安全态势

从图 13 可以看出一周之内整个网络的安全态势的演化情况:在周三、周四和周六的某些时段,出现了需引起关注的攻击事件,可能是黑客尝试对网络发动攻击造成,虽然需要对个别主机和服务进行安全维护,但仍未对整个网络产生巨大影响;网络系统在 2013 年 6 月 16 日出现了非常严重的攻击态势,需管理员重点监控,并采取适当的行为,避免整个网络系统低效甚至崩溃情况的出现.

本文所提出层次量化感知方法除了可以动态评估服务、主机和网络的威胁态势以外,还具有良好的环境适应性,表现出了一定的认知能力.本文提出的基于权系数的威胁因子获取方法,在态势感知系统应用于新的网络时,管理员仅需要对本网络敏感的攻击重新排列等级即可.假设一个新的网络环境中服务对攻击的敏感程度依次为未知攻击、DoS、U2R 和 R2L、Probe,则对表 1 中的威胁因子按照公式(6)可做如表 4 所示的自动调整,并依据表 1、表 4、公式(7)~公式(9),即可生成服务、主机和网络这 3 个层次的安全态势感知曲线,而不需要对组成态势的组件和要素做复杂的关联分析.在与图 11 所示相同的攻击下,威胁因子自适应之后,主机 H_1 上 E-mail, Http 和 Snmp 的安全态势演化曲线如图 14 所示,同样可以感知所监控服务的安全态势,且表现出了与图 11 类似的态势演化趋势,但同样的攻击数据对不同网络通常会表现为不同的威胁程度.

Table 4 New threat gene

表 4 新威胁因子

攻击类型	威胁等级	威胁因子
R2L	2	0.611
U2R	2	0.611
DoS	1	0.726
Probe	3	0.389
New	0	1

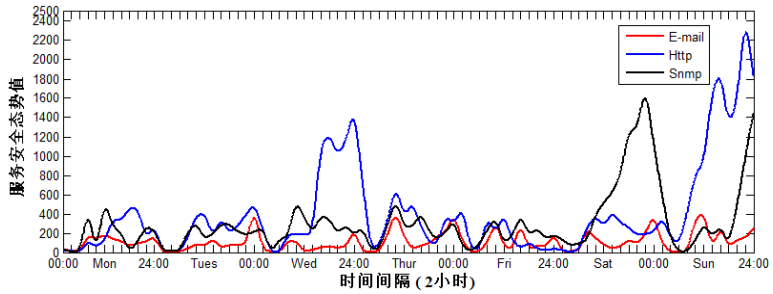


Fig.14 Service security situation after self-adapting

图 14 自适应后服务安全态势

5.3 认知调控

网络安全态势认知感控不仅能够感知网络的威胁状况,而且能够根据感知效果调整感知技术.依据态势感知曲线,可计算其瞬时态势梯度,并依据调控策略调整感知参数、威胁因子等,自主选择调控策略,实现认知适应性.在目前的仿真实验中,仅根据态势梯度在路由器上依据数据包的源 IP、目的 IP、源端口、目的端口,采用丢包策略对某一或某些引起梯度变化攻击类型的分组进行过滤,降低攻击数据对网络系统的影响,并调用层次感知组件,感知新的安全态势.而且,考虑网络系统本身的容忍能力,即使在出现梯度增长的区间内,若安全态势低于某一上限阈值,仍不会影响网络系统的正常运行,可不执行相应的调控策略,从而避免频繁调控和降低出现调控抖动的概率.依据调控策略,并设置容忍阈值为 150,对网络安全态势感知进行自主调控.从图 15 中可以看出,经调控之后,攻击对整个网络的威胁程度大大减低,可以真正实现无人值守的自感知和自调控.但同时也可以看出,调控之后的态势感知视图中仍存在高于容忍阈值的态势区间,可能的原因包括时间窗口大小、调控滞后性和执行策略等方面的问题.该实验中,调控策略仅丢弃影响态势梯度最大的某一或某些类型的攻击数据包,导致即使调控之后仍存在威胁网络运行的因素.当然,也可以采用丢弃所有来自某一源的所有数据包,但在实用系统中,过于严格的调控策略通常会禁止来自同一源地址正常用户的访问.上述认知调控过程说明本文提出的调控机制是可行的,但更为科学合理的调控策略仍需进一步研究.

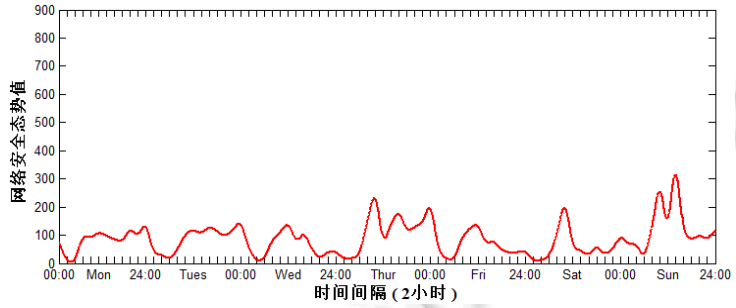


Fig.15 Network security situation after regulation and control

图 15 调控后的网络安全态势

对图 11~图 15 的层次化威胁量化评估,还可以设置不同的时间粒度,显示以小时、分钟甚至秒为时间窗口的安全态势视图,实现更细粒度的态势感知.本文所采用的基于融合的态势感控机制,以可视化形式将安全传感器的离散报警事件转化为连续的态势演化视图,将严重阻碍安全技术应用于网络系统的虚警、漏警等掩盖入统计特性之中,提供一种新的威胁表示方法,并能够从态势曲线的当前及历史态势的演化趋势中获取网络异常的时间、手段的变化规律,使得提前自动响应成为可能.而且与目前典型研究在威胁因子获取、量化感知、调控等方面相比具有突出的特点,见表 5.跨层认知的安全态势融合感控模型可适用于异构异质的网络系统,拓宽了

态势感知系统的应用范围,并在下一代网络系统中也有广泛的应用前景;基于权系数的威胁因子获取方法与AHP 层次分析相比,只需按照威胁水平和重要程度进行排队即可,而且在将态势感知系统迁移至另一网络环境中时具有良好的环境认知能力,无需对安全组件的关联影响和隶属关系做复杂的分析.从感知过程分析,本文采用公式法规范量化感知过程,明确态势要素之间的关系,实现态势感知的形式描述,更利于在不同的目标范围内确切的表达态势知识及其演化规律.同时,基于态势梯度的调控机制可以真正实现无人值守的自主调控.至此,网络安全态势认知融合感控最终形成封闭式 FADC 反馈控制结构,既能自主调整融合和感知的参数,又能根据态势梯度主动选择调控策略,达到了用技术管理技术的目的.

Table 5 Typical research comparison

表 5 典型研究比较

研究	特点					
	数据源	融合算法	评估模式	威胁因子	自适应性	调控方法
文献[1]	IDS/Sniffer	–	定性	–	–	–
文献[2]	IDS/Log	–	定性	–	–	–
文献[30]	IDS/Traffic/Virus	D-S/经验加权	定量	主观经验	较弱	–
文献[7]	IDS	–	权值计算/层次化	主观经验	较弱	–
文献[9]	Vulnerability/Log	D-S	权值计算/结点级	主观经验	较弱	–
文献[8]	IDS	–	权值计算/层次化	AHP	弱	–
文献[13]	Vulnerability/IDS/Firewall	–	博弈分析	风险传播网络	弱	手动
本文	IDS/Traffic/SNMP/Others	CPSO-DS/指数权	公式法	客观自适应	较强	自主

6 结论和进一步的工作

本文分析了网络安全感知现有的模型、融合算法和感知方法,并对认知计算进行了简要的讨论,提出了一个网络安全态势认知融合感控模型.在模型的指导下,讨论了适用于异构网络的 CPSO-DS 多源融合算法,以威胁因子获取为基础,综合分析服务、主机和网络这 3 个不同层次的网络安全态势感知方法,并利用态势梯度实现了对网络安全态势的自主调控.仿真实验表明,基于融合的网络安全态势感控模型及其方法能够准确地识别网络安全事件,动态感知不同层面的威胁演化趋势.而且,所提出的模型和算法具备良好的认知能力,能够形成闭环反馈控制结构,可以达到自我感知和自主调控的目的,从而为监控网络、制定安全策略和采取响应措施等提供了新的研究尝试和技术手段.

本文仅是在已有研究成果的基础上提出了解决网络安全态势感知研究中部分关键问题的初步方法,后续亟需解决的问题还有很多:首先,本文仅讨论了网络安全态势感控的跨层框架,对模型形式描述以及认知环状态空间抽象规约和求解验证仍是不可回避的研究挑战;其次,本文仅讨论了决策层的融合,其他层次中实时性更好、准确性更高的融合算法是下一步的重要研究内容;再次,层次量化感知仅是安全态势感知的方法之一,其他形式的态势知识表示和更多类型的态势要素仍需探讨;最后,适用于复杂网络环境的多维调控策略有待深入分析,并需要在各种现实网络中进行不断的测试,最终构建既适用于当今网络又可运行于下一代网络的安全态势感控系统.

致谢 感谢研究同行无私地奉献了诸多的优秀研究成果,也衷心感谢各位评审专家对本文提出的宝贵意见.

References:

[1] Bass T. Multi-Sensor data fusion for next generation distributed intrusion detection systems. In: Proc. of the IRIS National Symp. on Sensor and Data Fusion. 1999. 24−27.

[2] Tadda G, Salerno JJ, Boulware D, Hinman M, Gorton S. Realizing situation awareness within a cyber environment. In: Proc. of the Multi-Sensor, Multi-Source Information Fusion: Architecture, Algorithms, and Applications, Vol.6242. 2006. 1−8. [doi: 10.1117/12.665763]

[3] Shen D, Chen G, Cruz JB, Haynes JL, Kruger M, Blasch E. A Markov game theoretic approach for cyber situational awareness. In: Proc. of the Multi-Sensor, Multi-Source Information Fusion: Architectures, Algorithms, and Applications, Vol.6571. 2007. 1−11. [doi: 10.1117/12.720090]

[4] Stephen L. The spinning cube of potential doom. Communications of the ACM, 2004,47(6):25−26. [doi: 10.1145/990680.990699]

[5] Lakkaraju K, Yurcik W, Lee AJ. NVisionIP: NetFlow visualizations of system state for security situational awareness. In: Proc. of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security. 2004. 65−72. [doi: 10.1145/1029208.1029219]

[6] Shiravi H, Shiravi A, Ghorbani AA. A survey of visualization systems for network security. IEEE Trans. on Visualization and Computer Graphics, 2012,18(8):1313−1329. [doi: 10.1109/TVCG.2011.144]

[7] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. Ruan Jian Xue Bao/Journal of Software, 2006,17(4):885−897 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/885.htm [doi: 10.1360 /jos170885]

[8] Hu W, Li J, Jiang X. A hierarchical algorithm for cyberspace situational awareness based on analytic hierarchy process. High Technology Letters, 2007,13(3):291−296.

[9] Wei Y, Lian YF, Feng DG. A network security situational awareness model based on information fusion. Journal of Computer Research and Development, 2009,46(3):353−362 (in Chinese with English abstract).

[10] Zhang Y, Huang SG, Guo SZ, Zhu JM. Multi-Sensor data fusion for cyber security situation awareness. Procedia Environmental Sciences, 2011,10:1029−1034. [doi: 10.1016/j.proenv.2011.09.165]

[11] Dapoigny R, Barlatier P. Formal foundations for situation awareness based on dependent type theory. Information Fusion, 2013, 14(1):87−107. [doi: 10.1016/j.inffus.2012.02.006]

[12] Gong ZH, Zhuo Y. Research on cyberspace situational awareness. Ruan Jian Xue Bao/Journal of Software, 2010,21(7):1605−1619 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3835.htm [doi: 10.3724/SP.J.1001.2010.03835]

[13] Zhang Y, Tan XB, Cui XL, Xi HS. Network security situation awareness approach based on Markov game model. Ruan Jian Xue Bao/Journal of Software, 2011,22(3):495−508 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3751.htm [doi: 10.3724/SP.J.1001.2011.03751]

[14] Thomas RW, Dasilva LA, MacKenzie AB. Cognitive networks: Adaptation and learning to achieve end-to-end performance objectives. IEEE Communication Magazine, 2006,44(12):51−57. [doi: 10.1109/MCOM.2006.273099]

[15] Fortuna C, Mohorcic M. Trends in the development of communication networks: Cognitive networks. Computer Networks, 2009, 53(9):1354−1376. [doi: 10.1016/j.comnet.2009.01.002]

[16] Clark DD, Partridge C, Ramming JC. A knowledge plane for the internet. In: Proc. of the 2003 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM). 2003. 3−10. [doi: 10.1145/863956.863957]

[17] Shakkottai S, Rappaport T, Karlsson P. Cross-Layer design for wireless networks. IEEE Communications Magazine, 2003,41(10): 74−80. [doi: 10.1109/MCOM.2003.1235598]

[18] Aniba G, Aissa S. Cross-Layer designed adaptive modulation algorithm with packet combining and truncated ARQ over MIMO nakagami fading channels. IEEE Trans. on Wireless Communications, 2011,10(4):1026−1031. [doi: 10.1109/TWC.2011.030311.100487]

[19] Tran NH, Hong CS, Lee S. Cross-Layer design of congestion control and power control in fast-fading wireless networks. IEEE Trans. on Parallel and Distributed Systems, 2013,24(2):260−274. [doi: 10.1109/TPDS.2012.118]

[20] Aguilar T, Syue SJ, Gauthier V, Afifi H. CoopGeo: A beaconless geographic cross-layer protocol for cooperative wireless ad hoc networks. IEEE Trans. on Wireless Communications, 2011,10(8):1−13. [doi: 10.1109/TWC.2011.060711.100480]

[21] Gomez I, Marojevic V, Gelonch A. ALOE: An open-source SDR execution environment with cognitive computing resource management capabilities. IEEE Communications Magazine, 2011,49(9):76−83. [doi: 10.1109/MCOM.2011.6011737]

[22] Gupta M. On fuzzy logic and cognitive computing: some perspectives. Scientia Iranica, 2011,18(3):590−592. [doi: 10.1016/j.scient.2011.04.010]

[23] Ogiela MR, You I. Cognitive and secure computing in information management. Int'l Journal of Information Management, 2013, 33(2):243−244. [doi: 10.1016/j.ijinfomgt.2012.11.009]

[24] Wang M, Suda T. The bio-networking architecture. In: Proc. of the 2001 Symp. on Applications and the Internet. 2001. 43−53. [doi: 10.1109/SAINT.2001.905167]

[25] Garlan D, Cheng S. Rainbow: Architecture-based self-adaptation with reusable infrastructure. IEEE Computer, 2004,37(10):46−54. [doi: 10.1109/MC.2004.175]

[26] Schmid S, Eggert L, Brunner, M, Quittek J. Towards autonomous network domains. In: Proc. of the 25th IEEE Int'l Conf. on Computer Communications (INFOCOM). 2006. 1−6. [doi: 10.1109/INFOCOM.2006.351]

[27] Zhao WT, Yin JP, Long J. A cognition model of attack prediction in security situation awareness systems. Computer Engineering and Science, 2007,29(11):17−19 (in Chinese with English abstract).

[28] Zang C, Huang ZD, Dong JX. State-Based generalized autonomic computing models. Journal of Computer-aided Design and Computer Graphics, 2007,19(11):1476−1481 (in Chinese with English abstract).

[29] Feng GS, Wang HQ, Ma CG, Li BY, Zhao Q. Dynamic self-configuration of user QoS oriented to cognitive network. Journal on Communications, 2010,31(3):133−140 (in Chinese with English abstract).

[30] Ma LR, Yang L, Wang JX. Research on security information fusion from multiple heterogeneous sensors. Journal of System Simulation, 2008,20(4):981−989 (in Chinese with English abstract).

[31] Chen JJ. Multi-Sensor administration and information fusion [MS. Thesis]. Xian: Northwester Polytechnical University, 2002 (in Chinese with English abstract).

[32] Zhao YX, Chen XD, Chen X. BFOA-Based optimal point selection for Lagrange interpolation. Journal of System Simulation, 2012, 24(10):2232−2235 (in Chinese with English abstract).

[33] Liu XW, Wang HQ, Yu JG, Cao BX, Gao ZH. Network security situation awareness model based on multi-source fusion. Advanced Science Letters, 2012,5(2):775−779. [doi: 10.1166/asl.2012.1852]

附中文参考文献:

[7] 陈秀真,郑庆华,管晓宏,林晨光.层次化网络安全威胁态势量化评估方法.软件学报,2006,17(4):885−897. http://www.jos.org.cn/1000-9825/17/885.htm [doi: 10.1360/jos170885]

[9] 韦勇,连一峰,冯登国.基于信息融合的网络安全态势评估模型.计算机研究与发展,2009,46(3):353−362.

[12] 龚正虎,卓莹.网络态势感知研究.软件学报,2010,21(7):1605−1619. http://www.jos.org.cn/1000-9825/3835.htm [doi: 10.3724/SP.J.1001.2010.03835]

[13] 张勇,谭小彬,崔孝林,奚宏生.基于 Markov 博弈模型的网络安全态势感知方法.软件学报,2011,22(3):495−508. http://www.jos.org.cn/1000-9825/3751.htm [doi: 10.3724/SP. J.1001.2011.03751]

[27] 赵文涛,殷建平,龙军.安全态势感知系统中攻击预测的认知模型.计算机工程与科学,2007,29(11):17−19.

[28] 臧铖,黄忠东,董金祥.基于状态的通用自主计算模型.计算机辅助设计与图形学学报,2007,19(11):1476−1481.

[29] 冯光升,王慧强,马春光,李冰洋,赵倩.面向认知网络的用户 QoS 动态自配置方法.通信学报,2010,31(3):133−140.

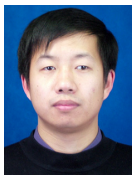
[30] 马琳茹,杨林,王建新.多源异构安全信息融合关联技术研究系.系统仿真学报,2008,20(4):981−989.

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

[32] 赵翼翔,陈新度,陈新.基于 BFOA 的拉格朗日插值点最优配置.系统仿真学报,2012,24(10):2232−2235.

刘效武(1976－),男,山东东营人,博士,副教授,CCF 专业会员,主要研究领域为安全态势感知,信息融合,认知计算.

王慧强(1960－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络技术与信息安全,认知计算,智慧网络.



吕宏武(1983－),男,博士,讲师,CCF 专业会员,主要研究领域为自律计算,可信性评价.

禹继国(1972－),男,博士,教授,CCF 高级会员,主要研究领域为无线网络与通信,分布式计算.

张淑雯(1991－),女,硕士生,CCF 学生会员,主要研究领域为网络安全,数据融合.