面向大规模网络的安全态势实时量化感知模型

郑黎明[1] 邹 鹏[2] 张建锋[1] 贾 焰[1] 韩伟红[1]

(国防科技大学计算机学院 长沙 410073)[1] (装备指挥技术学院 北京 100029)[2]

摘 要 网络安全态势感知能够实时发现潜在的网络风险,对提高网络的应急响应和主动防御能力起着重要的作用。现有的各种态势感知算法在规模上和时间上都不能适应大规模网络实时态势感知的要求,提出了基于指标体系的实时大规模网络安全态势量化感知模型,首先建立了层次化的指标体系,通过数据融合、关联分析等方法对网络安全日态数据进行处理,再针对各个属性采用不同的量化方法,将其聚集成综合网络安全态势指数。最后通过系统实际部署运行过程中的两个案例对所提出的网络安全态势感知模型和算法进行实例分析,结果证明了所提模型和算法的有效性和合理性。

关键词 网络安全,指数,指标体系,态势感知

中图法分类号 TP393.08 **文献标识码** A

Real Time Situational Awareness Model for Large-scale Networks

ZHENG Li-ming[1] ZOU Peng[2] ZHANG Jian-feng[1] JIA Yan[1] HAN Wei-hong[1]

(School of Computer, National University of Defense Technology, Changsha 410073, China)[1]

(Academy of Equipment Command and Technology, Beijing 100029, China)[2]

Abstract NSAS (Network Situation Awareness System) can identify and predict potential attacks. It plays an important role in improving the emergency response capacity and proactive defense capability of the networks. Existing NSASs have many faults, such as lacking for multi-source information, higher computational complexity, which are difficult to be applied to large-scale networks and real-time situational awareness. This paper introduced an NSAS for large-scale network. The situational awareness model was proposed first, and then the details of key technologies, including data fusion, correlation analysis, index quantification and event predication, were given. The experimental results demonstrate the effectiveness and reasonability of the proposed model.

Keywords Network security, Index, Index system, Situation awareness

1 引言

随着互联网技术的广泛应用,其规模不断增大,各类网络应用层出不穷,给人类的生产、生活带来了极大的便利,互联网已经成为当今社会的重要信息交流平台。然而互联网时刻都遭受来自各方面各种形式的攻击,如黑客入侵、DDoS、蠕虫爆发、网站挂马、网络钓鱼等。为了应对日趋严峻的网络安全挑战,IDS、防火墙、防病毒网关、身份认证、数据加密、安全审计等安全防护工具得到了广泛的应用。但是,1)这些工具功能分散,只关注特定网络安全事件,形成了相互隔离的"安全孤岛";2)这些工具产生的告警数据浩如烟海,让人应接不暇,网络管理者无法从这些海量数据中发现真正的网络安全威胁,更谈不上对当前网络安全态势进行感知和预测;3)告警数据可理解性较差,需要专业知识才能提取出告警数据所蕴含的态势。如果能够综合考虑网络安全态势的各种影响要素,辅助一定的专家知识,实时地对网络安全态势进行量化感知,就能为网络管理者提供一个动态的全局视图,直观地反应网络中面临的主要威胁和当前的安全状态,帮助网络管理者选择合适的危机应对措施。所以实时网络安全态势感知具有重要的理论价值和实用价值。

网络安全态势感知是指在一定的时空条件下,对影响网络安全的各种要素进行获取和理解,通过数据的整合处理和分析来判断网络安全的现状并预测其未来的发展趋势。态势感知起源于航空领域和军事领域,后来逐渐推广到交通管理、物流管理、核反应控制、医疗应急调度等其他领域。1999年Tim Bass首次把态势感知引入网络安全领域,并提出利用多传感器进行数据融合的网络安全态势感知框架[1],但没有阐述其具体的实现。Yin等人借助可视化技术,提出了基于Netflow的网络安全态势感知框架模型[2],但网络管理者并不能从IP连接流量直接获取网络安全态势。Wing等通过比

本文受国家高技术研究发展计划(863,2011AA010702)资助。

郑黎明(1983-),男,博士生,主要研究方向为网络与信息安全、数据挖掘,E-mail:lmzheng@nudt.edu.cn;邹 鹏(1957-),男,硕士,教授,博士生导师,主要研究方向为网络与信息安全、分布式计算;张建锋(1984-),男,博士生,主要研究方向为网络与信息安全、数据挖掘;贾 焰(1961-),女,博士,教授,博士生导师,主要研究方向为网络与信息安全、数据挖掘、社会网络;韩伟红(1973-),女,博士,副研究员,主要研究方向为网络与信息安全、数据挖掘。

较系统对外暴露的资源来评判攻击的相对安全级别，然后通过考察系统暴露资源的安全代价来感知系统的安全态势[3]，但是该方法关注维度单一，未能充分考虑其他要素。Arnes采用隐马尔科夫模型对网络安全态势进行实时感知，认为网络风险是主机风险的组合，主机处于不同的安全状态，而状态之间的转换是一个隐马尔科夫过程，而主机处于每种状态的概率决定其安全风险[4]。该方法计算的时间和空间复杂度较高，不适合大规模网络的实时态势感知。Cristina Abad等人提出了利用UCLog+设计安全态势感知系统，用于安全事件存储、查询和关联分析，综合得到网络安全态势感知结果[5]，但该方法缺乏量化分析，无法准确反映网络安全态势。在实际系统构建方面，美国国家高级安全系统研究中心进行了SIFT(Security Incident Fusion Tool)系统的开发，通过一个网络安全数据融合工具的集成框架对Internet的安全态势进行感知。在国内，陈秀真等人提出了层次化的实时网络安全态势感知模型[6]，该模型把整个网络分为系统、主机、服务和攻击4个层次，采用先局部后整体的感知策略，但该模型也存在计算量大，实时性不够的缺点，不适合大规模网络实时态势感知。张海霞等人引入攻击图理论，提出了基于攻击能力增长的网络安全分析模型[7]，但该模型主要从脆弱性角度来分析网络安全态势，角度单一。韦勇等人引入D-S证据理论将多数据源信息进行融合，经过态势要素融合和节点态势融合计算网络安全态势[8]，但该方法可操作性不够，也不适合大规模网络安全实时态势感知。

综上所述，国内外研究者提出了很多可行的解决方法，为下一步的研究奠定了基础，但同时这些方法也存在诸多方面的不足，例如缺乏对网络安全态势影响要素全面的考虑，感知数据来源单一，使得感知结果的可信度较差；很多方法只是对威胁或者漏洞进行感知，而网络安全态势应该是一个全方位整体的概念；没有考虑同一数据源不同数据之间以及不同数据源各数据之间的关联性和冗余性；感知算法时间和空间复杂度较高，不适应大规模网络实时态势感知的要求；大部分只侧重于概念研究，距离实际应用还有一段差距。

针对上述问题，首先对多异构数据源进行数据融合，随后对网络安全数据进行关联分析，基于动态可配置的指标体系对数据进行量化和评估，最后从威胁、脆弱、基础运行和风险四个不同的维度以直观的形式向用户展示网络的当前态势。

2 网络安全态势指标体系

2.1 层次化指标体系

网络安全态势是一个整体的概念，需要综合各个不同要素，采用层次化的指标体系来量化和评估网络安全态势，通过指数来描述网络的安全状态，通过指数的变化来刻画网络安全状态的变化。图1给出了指标体系的大致结构，详细内容可参看“网络安全评价指标体系(2009B43)”国内标准立项。该体系自下而上设定了3级指数，由部分到整体，逐渐汇聚成整体的网络安全态势指数。主要的宏观指数包括风险维、基础运行维、脆弱维和威胁维4个指数。风险维指数用于展示网络中存在的风险状态，基础指数展示网络基础运行安全状况，脆弱性指数展示网络存在的潜在风险状况，威胁性指数展示网络面临的网络攻击状况，综合态势指数是一级指数，由基础设施运行安全指数、脆弱维指数、威胁维指数和风险维四个维度集成而来。各个二级指标又分别由流量、服务状态、资源消耗、漏洞状态、防护软件、木马等各种指数进行综合计算得到，最底层的指数由各个经过归一化处理的属性值量化计算而来。

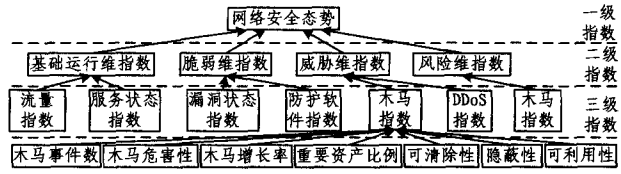

图1 层次式网络安全指标体系

2.2 网络安全态势量化模型

指标体系中各要素的量化方法和综合评价算法是指标体系的核心。本文所提出的感知模型对基础运行维指数、网络脆弱维指数、网络威胁维指数和风险维指数分别进行计算，然后综合得到网络安全态势。这四个维度的计算方法相似，在此以网络安全威胁指数为例阐述指数计算过程。指数的计算分为量化和综合计算两步，网络安全威胁指数T由DDOS攻击指数、僵尸网络指数、蠕虫指数等各类威胁指数综合计算得到，即 $T=f_t(T_{DDoS},T_{Botnet},T_{Worm},T_{Trojan},T_{Scan},\cdots)$，又仅以木马指数计算过程中量化算法为例进行阐述。

在指标体系中，木马考虑的相关要素(攻击特征)有危害程度、数目、增长率、目标IP资产重要性、可清除性和隐蔽性，对于不同的攻击特征需要选择不同的量化方法。针对危害程度、可清除性、隐蔽性等定性指标，把评语集划分为5个等级，优、良、中、差、危，并对个等级进行量化，如表1所列。该模型采用专家打分法和模糊综合评判方法，按照木马的基本原理为每一类木马的危害程度、可清除性、隐蔽性进行赋值，木马事件可形式化表示为 $E_{Trojian}=[r_1,r_2,\cdots,r_i,\cdots,r_n,r_{Type}]$，$(2\leqslant i\leqslant n)$，其中 r_i 为木马事件的属性，如源IP、目的IP、源PORT，目的PORT等，专家知识库中事件分类赋值可表示为四元组 $K=\langle r_{Type},\mathrm{Compromise},\mathrm{Removability},\mathrm{Elusive}\rangle$，赋值后的事件表示为 $E=E_{Trojan}\times K$。最后针对木马事件该3维属性值，采用加权平均的方式完成量化。

表1 威胁评估等级划分

值	威胁等级	说明
1	优	无效攻击
2	良	安全信息泄露
3	中	恶意代码执行
4	差	远程文件操作，系统状态变更
5	危	远程权限获取

针对事件数目，采用最大-最小值法，其中MaxValue和MinValue分别为事件数目的历史最大值和历史最小值，通过历史数据获取。当然还需要针对该指标与态势指数之间的正、负相关性做一些变化，在此仅以正相关为例。

$$g(x)=\begin{cases}1, & x>MaxValue\\ \dfrac{x-MinValue}{MaxValue-MinValue}\\ 0, & x<MinValue\end{cases}$$

$MinValue\leqslant x\leqslant MaxValue$

针对增长率、重要资产个数这类最大值不易确定的指标则采用反正切函数法，如对增长率的量化，先计算增长率：$x=(Num_{now}-Num_{last})/Num_{now}$，再对增长率进行归一化处理 $g(x)=\mathrm{arctg}(x)/\pi+0.5$，重要资产个数量化方法：$g(x)=2$

· arctg(x)/ π。

具体的量化算法如下：

算法 1 Trojan_threat_calculate

输入：时间窗口 W 内网络安全事件序列 $TL=\{t_1,t_2,\cdots,t_i,\cdots,t_n\}$，($1\leqslant i\leqslant n$)；专家知识库；指标体系

输出：木马维量化结果

Begin：

1)从 TL 中筛选出木马事件，构成木马事件序列：$TrojanL=\{tr_1,tr_2,\cdots,tr_j,\cdots,tr_m\}$；

2)构建木马事件矩阵 $M_{Trojan}=(tr_1,tr_2,\cdots,tr_j,\cdots,tr_m)^T$；

3)木马事件矩阵 M_{Trojan} 与专家知识库 K 做连接操作：$M_e=M_{Trojan}\times K$；

4)读取指标体系；

5)for 木马指标的每个下层指标 A_k；

6) if A_k 是定性指标；

7) 对考察的属性列进行加权平均，即 $\sum_{j=1}^{m} r_{jk}/\max_{1\leqslant i\leqslant m}(r_{jk})*m$；

8) else if A_k 是定量指标；

9) 计算相关数值；

10) 按照指标体系配置的归一化方法进行归一化；

11) end if；

12)end for；

13) 计算木马维指数：$E(trojan)=\sum_{k=1}^{m} g(A_k(t))\times w_k$，$A_k(t)$为 t 时刻指标 A_k 的数值，$g(A_k(t))$为 $A_k(t)$的归一化值。ω_k 为各指标 A_k 对应的权重，满足归一化约束：$\sum_{k=1}^{m} w_k=1, w_k\geqslant 0, k=1,2,\cdots,m$

End.

2.3 基于关联分析的风险维量化

为了从海量的告警数据中提取出真正的风险事件，需要将来自不同数据源的各类网络安全事件进行关联分析。关联分析是指对不同地点、不同时间、不同层次的网络安全事件进行综合分析，从而挖掘出在时间和空间上分散的协同多步攻击，识别真正的网络风险。作为网络安全态势感知主要数据源的 IDS 普遍存在误报率和重复告警率较高的突出问题[9]，如何降低误报率和重报率是网络安全态势感知面临的重要挑战，而关联分析正是减少误报和重复报警的有力工具。当前的关联分析方法可以分为 4 类[10]：基于概率相似度的关联分析方法，如 Valdes. A 等利用告警数据的特征相似性对来自不同类型 IDS 的告警信息进行综合关联分析[11]；基于攻击场景的关联分析方法，如 M. Dain 等提出基于攻击场景重建的概率关联方法[12]；基于多步的关联分析方法，如 Cuppens 等提出的基于攻击时序关系关联分析方法[13]；基于过滤器的关联分析方法，其中最主要是把网络安全事件和脆弱性、网络资产数据进行关联分析，如 R. Gula 把 IDS 的日志信息和网络中存在的脆弱性数据进行关联分析，过滤虚假警报[14]。上述各种方法都只是针对特定维度进行关联。Fredrik V. 等人提出了利用多种关联分析方法进行综合关联的处理框架[15]，但是该框架试图囊括所有的关联分析方法，导致系统复杂，不能满足实时态势感知的实时性要求。本文把攻击场景和多步关联都形式化表示为规则，采用基于规则的推理机来进行事件与事件之间的关联分析，同时在事件处理前端引入基于过滤器的关联分析方法，把网络安全事件和网络脆弱性数据以及网络基础运行数据进行关联分析，最后得到网络中真实的高风险事件。

以往的网络风险量化方法大都是把 IDS 日志数据与网络主机、资产、脆弱性数据进行综合计算，对各个主机进行网络安全态势感知，然后把网络中所有主机的风险值之和作为网络的风险值。但是在现实的大型企事业单位，网络的全局管理者很难获取网络中各个主机的状态，同时在空间和时间复杂度上精确地获取每个主机的状态信息，再对每个主机进行风险感知，整个计算过程不可能在 6～10s 内完成(6～10s 是实时系统的要求)，针对大规模网络实时态势感知的要求，在关联分析的过程中，引入优先级参数，重点关注网络中应用服务器、数据库服务器、Web 服务器、路由器、核心交换机等重点设备，对网络中其他主机及设备统一采用默认值的方式进行处理。表 2 给出风险维关联分析参数定义。

表 2 关联分析参数定义

Severrity	威胁度	事件对网络威胁的严重程度，由专家按照 Sensors，EventT 威胁程度把事件进行分类
Asset	资产值	事件针对的资产的重要程度
Priority	优先级	事件被处理的优先级别
Reliability	可靠度	事件成功执行或者是真正攻击的可能性
Risk	风险值	网络安全事件的风险

本文采用了基于可靠度的树形逐级关联分析算法，用攻击事件的可靠度属性来度量该攻击事件成功发生的可能性。在关联分析过程中，首先将事件与网络中重要网络设备的脆弱性数据进行关联，再与重要资产的基础运行数据进行关联，随后是事件与事件的关联分析，在这个过程中，每当事件匹配上相应的规则时，都会在该事件的基础上生成更高级别的告警事件，赋予告警事件新的可靠度。在这个过程中，当可靠度数值超过一定的阈值时，将在原始事件的基础上产生一个警告事件。下面给出具体的关联分析算法：

算法 2 Collaborative_ Correlation

输入：网络安全事件序列 $TL=\{t_1,t_2,\cdots,t_i,\cdots\}$，网络主机漏洞集合 $V=\{\langle IP_i,CVEID_j\rangle, i\in H, j\in V_{CVE}\}$其中 H 为监控的主机集合、V_{CVE}为所有漏洞集合，网络基础运行信息$\langle IP,OSType\rangle$、$\langle IP,server,Port,protocol,version\rangle$，专家知识库 K。

输出：警告事件序列 $alarm=\{a_1,a_2,\cdots,a_j,\cdots\}$

Begin：

1)载入规则，初始化关联推理引擎；

2)while TRUE

3)一个网络安全事件 $event_k$ 到达(初始 $Reliability$ 赋值为 1)；

4)读取用户策略配置信息 $P=\langle SSet,DSet,SPorts,DPorts,Etype,Priority\rangle$其中 $SSet$ 和 $DSet$ 是源和目的地址集合，可取主机集合或者是网段，$SPoets$ 和 $DPorts$ 是源和目的端口集合，$Etype$ 是事件类型，$Priority$ 为符合匹配条件的事件处理优先级。按照配置策略为事件优先级属性赋值；

5)按照优先级把事件插入待处理事件列表；

//进入事件处理流程

6)从事件列表中取出一个事件 $event_i$ 进行处理；

7) if $event_i$ 是入侵事件

8) if $event_i\times V\times\langle Etype,CVEID\rangle\neq\emptyset$，即目的主机存在该入侵针对的漏洞

9) Reliability=10；

10) else

```
11)      if event_i 和目的主机操作系统、开放服务、服务端口、协议、
         软件版本分别匹配上，then Reliability 分别加 2；
12)      end if；
13)    end if；
       //进入事件与事件基于规则的匹配过程
14) if event_i×R〈if，then〉≠Ø，即 event_i 匹配上某条规则的前键
15)  if R〈if，then〉到达树形规则叶节点
16)    new alarm(event_i)；free(event_i)；
17)  else
18)    new EEngine(event_i)；free(event_i)；
19)    按照规则后键修改相关属性值；
20)    转 6)；
21)  end if；
22)end if；
23) if Reliability≥6
24)  new alarm(event_i)；free(event_i)；continue；
25)end if；
26)if persistence≥TIME_OUT
27)  free(event_i)；
28)end if；
29) end while；
End.
```

事件与事件关联分析是关联分析算法的核心，在实际系统的运行过程中，它也是算法的性能瓶颈。它需要对每一个可能的攻击场景和每一个多步攻击进行建模。关联分析引擎是一基于树形规则的推理引擎，规则树中的每一个结点对应一个匹配状态，每条边对应一条 if…then…规则。关联分析引擎将收到的网络安全事件按照从根节点到叶节点的顺序和树形规则依次匹配，每匹配一次将生成更高级别的告警事件，匹配越接近叶子节点，攻击的可靠度就越高。下面给出一条具体的木马匹配规则：

```
〈 scenario id="2801" name="Possible GateCrasher Trojan" priority
="5"〉
 〈rule type="detector" name="Intrusion rule matched" reliability
  ="2" occurrence="1" from="ANY" to="ANY" port_from="
  ANY" port_to="ANY" agent_type="D1001" event_type="
  147"〉
   〈rules〉
    〈rule type="detector" name="Rare but open dest port used"
     reliability="+4" occurrence="1" from="1:SRC_IP" to="1:
     DST_IP" port_from="1:SRC_PORT" port_to="1:DST_
     PORT" agent_type="D1104" event_type="101"〉
     〈rules〉
      〈rule type="monitor" name="More than 30 secs persistence"
       reliability="+2" from="1:SRC_IP" to="1:DST_IP" port
       _from="1:SRC_PORT" port_to="1:DST_PORT" agent_
       type="M2005" event_type="008" condition="ge" value
       ="30" interval="15" time_out="30" absolute="true"/〉
      〈rule type="detector" name="Attacked host is compromise"
       reliability="+2" occurrence="1" from="1:DST_IP" to="
       1:SRC_IP " agent_type="D1001" event_type="ANY" time
       _out="60"/〉
     〈/rules〉〈/rule〉
    〈/rules〉〈/rule〉
〈/scenario〉
```

3 网络安全态势感知算法

3.1 基于模糊层次分析法的权值确定算法

在整个态势感知系统中指标权值的确定非常关键，权值的合理性、准确性直接影响评价结果的合理性。针对大规模网络实时安全态势感知的实时性和合理性要求，把人类定性分析和计算机定量分析相结合，利用模糊层次分析法对指标进行赋权。层次分析法是美国运筹学家 A. L. Saaty 教授提出的一种把定性分析和定量分析相结合的系统分析方法[16]。但是层次分析法中判断矩阵的一致性检验计算量大，判断标准缺乏科学依据。文献［17］引进模糊一致矩阵的概念，构建了模糊层次分析法。针对实时量化感知的要求，对上述算法进行了改进，减少计算的时间复杂度，具体的算法流程如下：

1)构建指标体系层次结构模型。

2)构造模糊判断矩阵。对专家发放权重调查表，得出两两要素比较的隶属度，在此基础上构造模糊一致矩阵，参数取值如表 3 所列。

表 3 模糊矩阵取值度量定义

标度	定义	说明
0.5	同等重要	两要素相比较，同等重要
0.6	稍微重要	两要素相比较，一要素比另一要素稍微重要
0.7	明显重要	两要素相比较，一要素比另一要素明显重要
0.8	重要得多	两要素相比较，一要素比另一要素重要的多
0.9	及其重要	两要素相比较，一要素比另一要素极端重要
0.1，0.2 0.3，0.4	反比较	若要素 C_i 与要素 C_j 相比较得到判断 r_{ij}，则要素 C_j 与要素 C_i 相比较得到判断矩阵为 $r_{ji}=1-r_{ij}$

3)层次单排序。根据模糊一致矩阵的性质，若 r_{ij} 满足 $r_{ji}=1-r_{ij}$，则 R 为模糊一致矩阵，不需要再进行矩阵的一致性验证，层次单排序如表 4 所列。

表 4 层次单排序

比较指标	U_1	U_2	…	U_n	$\tilde{\omega}_i$
U_1	r_{11}	r_{12}	…	r_{1n}	$\tilde{\omega}_1$
U_2	r_{21}	r_{22}	…	r_{2n}	$\tilde{\omega}_2$
…	…	…	…	…	…
U_n	r_{n1}	r_{n2}	…	r_{nn}	$\tilde{\omega}_n$

求出层次中每个要素的权重值 $\tilde{\omega}_i$：

$$\tilde{\omega}_i=\frac{1}{n}-\frac{1}{2a}+\frac{1}{na}\times\sum_{k=1}^{n}\gamma_{ik},i\in U$$

式中，n 为 R 的阶数，$a=(n-1)/2$。

4)层次总排序。为了确定各个层次中每个要素，特别是最底层各要素相对于总目标的权重排序，需要进行层次总排序，采用如表 5 所列的公式计算各子准则层之间的相对权重。

表 5 层次总排序

层 A / 层 B	A_1 a_1	A_2 a_2	…	A_m a_m	B 层总排序权值
B_1	b_{11}	b_{12}	…	b_{1m}	$\sum_{j=1}^{m}b_{1j}a_j$
B_2	b_{21}	b_{22}	…	b_{2m}	$\sum_{j=1}^{m}b_{2j}a_j$
…	…	…	…	…	…
B_n	b_{n1}	b_{n2}	…	b_{nm}	$\sum_{j=1}^{m}b_{nj}a_j$

3.2 可配置的多指标聚集算法

为了更好地体现用户的感知偏好，适应网络安全态势实时变化特性，多指标聚集算法可由网络管理者动态配置。如系统中提供的聚集算法有加权平均法、最大值法、调和三角模法。加权平均算法又可分为算术平均法、几何平均法和调和平均法，如算术加权平均算法如下：

$$f(w_1 \cdot x_1, \cdots, w_n \cdot x_n) = \sum_{i=1}^{n} w_i \cdot x_i$$

它直观、易于理解，不过当各要素指数值差异较大时，它会淹没这种差异，不能很好地体现局部特性。

最大值法如下：

$$f(w_1 \cdot x_1, \cdots, w_n \cdot x_n) = \max_{i=1}^{n}(w_i \cdot x_i)$$

它能够表达局部最严重的情况，不过会丢失其他维度的信息。

调和三角模法如下：

$$f(w_1 \cdot x_1, \cdots, w_n \cdot x_n) = \prod_{i=1}^{n} w_i \cdot x_i / \prod_{i=1}^{n}(1 - w_i \cdot x_i)$$

它能够同时体现全局性和局部性，不过容易造成指数抖动。

网络管理者可以根据自己的感知目标，动态地选择最适合的聚集算法，同时也可以按照系统提供的基本接口实现自己的聚集算法。

4 实验

4.1 系统部署

为了验证所提网路安全态势感知模型的正确和合理性，作者课题组开发了 YH-SA 系统，系统结构图如图 2 所示，并在某中型企业真实的网络环境中进行了部署，在该企业中的部署情况如图 3 所示。

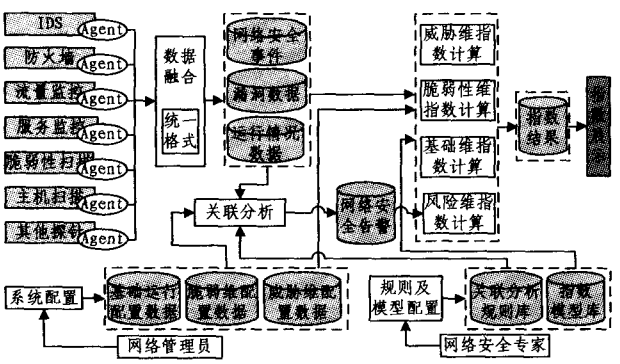

图 2 系统结构图

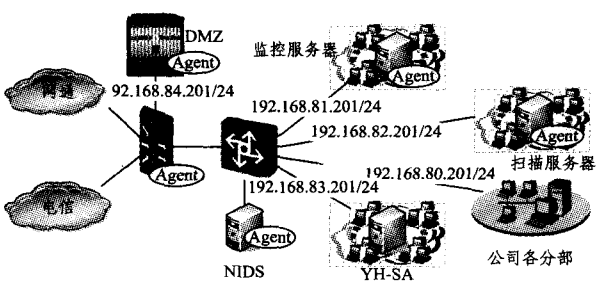

图 3 YH-SA 系统部署图

该公司主要采用华为 Quidway 系列产品进行组网，核心交换机为 Quidway_S5600 系列智能弹性三层交换机，防火墙采用的是 Quidway Eudemon 1000 硬件高速状态防火墙。如图 3 所示，YH-SA 系统主服务器部署在 192.168.83.0/24 网段；通过核心交换机提供的端口镜像功能，将核心交换机上其他端口的入口流量全部镜像到 NIDS 连接端口，在 NIDS 服务器上部署前端数据采集 Agent，监听 NIDS 产生的日志信息，进行格式转换、初步聚类后发送到服务器端；同时开启了 Quidway Eudemon 1000 防火墙的日志功能，并部署 Agent 收集防火墙产生的日志数据；DMZ 区域部署着该公司的网络服务器，在该公司的主要网络服务器上也部署了 Agent，收集相关服务器的日志数据并监控服务器状态；在 192.168.81.0/24 和 192.168.82.0/24 网段分别部署了网络状态、流量等监控服务器和扫描服务器。

在系统部署运行之初，需要依据 Snort 的规则手册、防火墙规则手册以及其他各类攻击的基本原理对事件进行分类，针对各类攻击的相关属性进行模糊评判，如为木马的危害程度、可利用性、可清除性、隐蔽性赋值；建立完整的层次化指标体系，并为各个节点的配置综合计算算法；利用模糊层次分析法确定各要素权值，如木马要素的模糊一致矩阵和各个底层要素的权值计算如表 6 所列；制定关联分析规则。为了达到实时量化感知的要求，本系统采用量化感知的时间窗口为 10s，每次把时间窗口内采集的网络安全事件进行分类量化，然后按照当前系统的权值和配置的聚集算法进行指数计算。

表 6 木马指标模糊一致矩阵

木马要素	数目	增长率	目的资产	危害性	可清除性	隐蔽性	可利用性	权值
数目	0.50	0.45	0.40	0.40	0.55	0.60	0.60	0.1429
增长率	0.55	0.50	0.40	0.45	0.60	0.55	0.55	0.1467
目的资产	0.60	0.60	0.50	0.55	0.60	0.55	0.55	0.1643
危害性	0.60	0.55	0.45	0.50	0.65	0.60	0.60	0.1633
可清除性	0.45	0.40	0.40	0.45	0.50	0.55	0.55	0.1334
隐蔽性	0.40	0.45	0.45	0.40	0.45	0.50	0.50	0.1252
可利用性	0.40	0.45	0.45	0.40	0.45	0.50	0.50	0.1252

4.2 运行实例分析

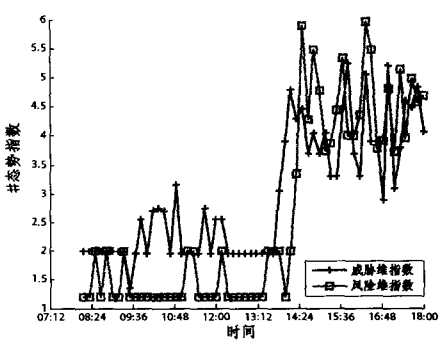

图 4 4 月 6 日指数曲线图

在系统实际部署运行过程中，由于该公司内部某台机器遭受木马入侵，被攻陷主机在内部网络中利用 CVE-2001-0876 漏洞继续进行传播，在一段时间内对内部网络造成了一次 DDOS 攻击，NIDS 检测到相应的攻击事件为：MISC UPnP malformed advertisement，如在 2010 年 4 月 06 日早上 8 点到晚上 18 点该公司内部网络的威胁维和风险维指数变化情况如图 4 所示。因为网络基础运行维和脆弱维指数变化不明显，在图中没有绘制，所有指数的取值范围为 0～10，越大表明网络安全态势越差。从图 4 可以看出，网络安全态势指数在下午两点左右出现了一个较大的跃迁，威胁维指数增大表明网络遭受某种攻击，风险指数增大表明系统中存在该攻击

针对的漏洞，整个网络安全风险增大。而在同一时间该公司网络中出现了大量针对 239.255.255.250:1900 的 UDP 数据包，导致整个网络传输延时增大，服务器响应变慢，说明指数和该公司网络实际运行情况完全吻合，它客观反应了网络安全态势的变化情况。

4 月 10 日，在该公司采取一些列安全措施后，威胁维和风险维指数都相继回落到攻击未发生时的水平，如图 5 所示。进一步验证了本文提出的网络安全态势感知模型能够很好地体现网络安全态势的变化情况。

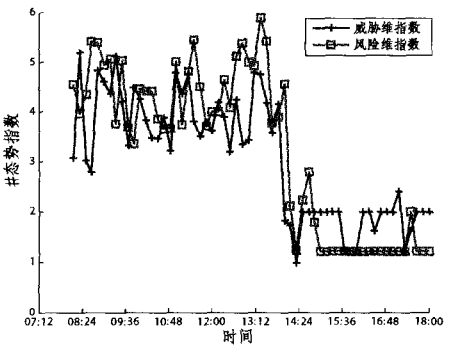

图 5　4 月 10 日指数曲线图

4.3　模拟实验验证

为了验证所提模型的合理性和有效性，设计了 DDoS 模拟实验。在实验过程中，采用了 TFN2K 的 DDoS 攻击工具对位于 DMZ 区域的服务器进行 DDoS 攻击。TFN2K 攻击工具能够在瞬间产生大量的 SYN 和 ICMP 请求，是一款广泛使用的 DDoS 工具。在设计的实验中，采用 TFN2K 产生大量的 ICMP 请求到 Web 服务器，导致 Web 服务的资源被耗尽，无法响应合法的 HTTP 请求。实验过程中对 Web 服务器进行了 20 分钟的攻击，在前十分钟逐渐增加攻击强度，后十分钟逐渐减弱到最终停止攻击。图 6 为 DDoS 攻击下各指数的曲线图，其中每 6 秒钟计算一次指数。图中各维度指数在第八分钟后急剧下降，通过服务器流量和资源使用情况可知：在第八分钟 DDoS 攻击流量已经超过服务器的负载能力，导致无法对任何请求作出响应。综上，本文所提网络安全态势感知模型能够比较客观全面地反应网络的实际运行状态。

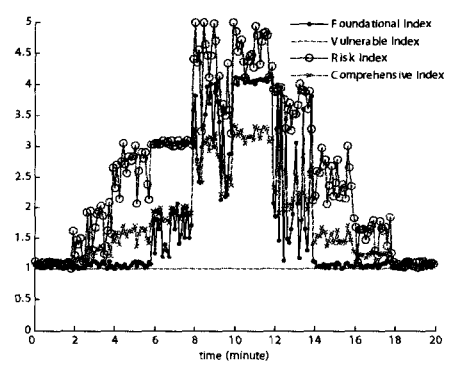

图 6　DDoS 攻击下的指数图

结束语　通过网络安全态势感知发现网络中主要风险，才能采取有效的网络安全防御措施，实现网络安全监管。现有的网络安全态势感知方法大都针对小规模网设计，难以适应大规模网络实时态势感知的要求。本文在层次化网络安全态势指标体系的指导下，通过数据融合、关联分析、属性数据量化、权值计算、多指标综合评价，最后得出网络安全整体态势指数，并通过实际系统验证了模型的有效性和合理性。该指标体系已经形成国内标准，并开始在 CNCERT/CC 进行试用，取得了良好的效果。

参 考 文 献

[1] Tim B. Intrusion Detection Systems and Multi sensor Data Fusion: Creating Cyberspace Situational Awareness [J]. Communications of the ACM, 2000, 43(4): 99-105

[2] Yin X, Yurcik W, Slagell A. The design of VisFlowConnect-IP: A link analysis system for IP security situational awareness [C]// IEEE International Workshop on Information Assurance (IWIA). Washington DC: IEEE Computer Society Press, 2005

[3] Manadhata P, Wing M J. Measuring a System's Attack Surface [C] // USENIX Security Symposium. Washington DC: USENIX, 2004

[4] Arnes A, Valeur F, Vigna G, et al. Using Hidden Morkov Models to Evaluate the Risk of Intrusions [C]// International Symposium on the Recent Advances in Intrusion Detection (RAID). Berlin: Springer-Verlag, 2006: 145-164

[5] Yurcike W, Abad C, Hasan R. UCLog+: A security Data Management System for Correlation Alerts, Incidents, and Raw Data From Remote Logs [C] // Computing Research Repository. Washington DC: ACM Press, 2006

[6] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化感知方法[J]. 软件学报，2006，17(4)：885-897

[7] 张海霞，苏璞睿，冯登国. 基于攻击能力增长的网络安全分析模型[J]. 计算机研究与发展，2007，44(12)：2012-2019

[8] 韦勇，连一峰，冯登国. 基于信息融合的网络安全态势感知模型[J]. 计算机研究与发展，2009，46(3)：353-362

[9] Axelsson S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection [J]. ACM Transaction on Information and System Security, 2000, 3(3): 186-205

[10] Zhou C V, Lechie C, Karunasekera S. A survey of coordinated attacks and collaborative intrusion detection [J]. Elsevier Computers&Security Journal, 2010, 29(1): 124-140

[11] Valdes A, Shinner K. Probabilistic alert correlation [C]// International symposium on recent advances in intrusion detection (RAID). Berlin: Springer-Verlag, 2001: 54-68

[12] Dain O, Cunningham R. Fusing a heterogeneous alert stream into scenarios [C]// ACM workshop on data mining for security application. Washington DC: ACM Press, 2001: 1-13

[13] Cuppens F, Miege A. Alert correlation in a cooperative intrusion detection framework [C] // IEEE symposium on security and privacy(S&P). Washington DC: IEEE Computer Society Press, 2002: 202-15

[14] Ron G. Correlating IDS alerts with vulnerability information [R]. Tenable Network Security, 2002

[15] Valeur F, Vigna G, Kruegel C, et al. A Comprehensive Approach to Intrusion Detection Alert Correlation [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(3): 146-169

[16] Saaty T L. Modeling unstructured decision problems-the theory of analytical hierarchies [J]. Mathematics Computer Simulation, 1978, 20: 147-158

[17] 张吉军. 模糊层次分析法(FAHP)[J]. 模糊系统与数学，2000，14(2)：80-88