DS融合知识的网络安全态势评估及验证

唐成华[1,2] 汤申生[3] 强保华[1]
(桂林电子科技大学广西可信软件重点实验室 桂林 541004)[1]
(桂林电子科技大学广西信息科学实验中心 桂林 541004)[2]
(西密苏里州立大学电子工程学院 美国斯普林菲尔德 64507)[3]

摘 要 网络安全态势评估过程具有大量不确定性的复杂影响因素。针对态势评估中存在的正确性和合理性质疑等问题,利用DS证据理论建立了态势指标的识别空间和评估准则,通过专家知识融合的推理,提出了基于DS融合知识的网络安全态势评估方法,同时结合三层网络主机脆弱性指数的计算实验对态势评估的分析实例进行了验证。实验结果表明,该方法具有较好的态势评估效果,为态势评估提供了一种可行的解决方案。

关键词 网络安全,态势评估,DS证据理论,态势熵,脆弱性
中图法分类号 TP393.08 **文献标识码** A

Assessment and Validation of Network Security Situation Based on DS and Knowledge Fusion

TANG Cheng-hua[1,2] TANG Shen-sheng[3] QIANG Bao-hua[1]
(Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China)[1]
(Guangxi Experiment Center of Information Science, Guilin University of Electronic Technology, Guilin 541004, China)[2]
(Department of Engineering Technology, Missouri Western State University, St. Joseph, MO 64057, USA)[3]

Abstract Network security situation assessment process has a large number of complex and uncertain influence factors. Aiming at the problem of lack of correctness and rationality in situation assessment, the situation index identification space and evaluation criteria based on the DS evidential theory were set up. The network situation assessment method based on DS and Knowledge Fusion was proposed through expert knowledge fusion reasoning, and the situation assessment case analysis was verified, combining the computation of three-layer network host vulnerability index. Experimental results show that the method has good effect in situation assessment, and thus provides a feasible solution for situation assessment.

Keywords Network security, Situation assessment, DS evidential theory, Situation entropy, Vulnerability

态势评估是近年来网络安全领域的一个研究热点,主要是运用认知模型方法,实现高层次的决策级信息融合过程[1],属于一种动态的安全风险评估技术[2]。目前人们已运用众多的理论和方法寻求建立有效的评估模型,如贝叶斯网络[2]、模糊推理[3]、博弈论[4]、图模型[5]等。由于攻击信息的不确定性和多变性等特点,在态势评估的方法论上仍存在诸多争论点,评估结果的正确性和合理性更饱受质疑。Kirillov[6]将态势评估归为多假设分类问题,该假设可分解成由各子任务按一定逻辑关系组成的层次结构,一些子任务的输出可以作为其他子任务的输入,这种对于任务产生的假设条件尚值得商榷。Maio[7]认为态势评估主要是一个诊断的过程,他将态势看作假设原因,所发生的事件看作结果,诊断任务在于建立明确的信念网络结构来表示决策者关于态势估计的思维模式,并将其运用于核电站运营系统的态势计算模型,但以事件反推态势的过程存在因果关系强证明上的质疑。Haidong[8]对态势知识进行提炼,提出了网络安全态势知识的提取模型,并建立了层次性的安全风险,包括目标细化、态势细化和威胁评估等过程,主要是针对已确定的态势知识进行挖掘,该方法受限于复杂动态网络环境的影响。Holsopple[9]从认知角度进行分析,通过对威胁和活动影响的评估实现态势感知过程,并分析了目标对象行为会带来评估缺陷的可能。

网络安全态势评估结果的合理性和真实性是问题的关键,对于安全策略的制定和应用具有深刻的影响,即安全决策的制定和实施效果严重依赖于评估的可信程度。评估可信度本身是模糊的定性概念,一般以权威者对评估结论的信任等级来表示,从底层指标支持数据开始,逐层进行可信度评估,直到得出最高层的可信等级,从而为各层网络安全态势值进行验证。这种复杂的和重复的评估过程有很多不确定因素,

到稿日期:2013-06-26 返修日期:2013-10-21 本文受国家自然科学基金(61163057,60970146),广西可信软件重点实验室项目(kx201111),广西信息科学实验中心基金项目(20130329)资助。
唐成华(1974—),男,博士后,副教授,硕士生导师,主要研究方向为数据挖掘、信息安全,E-mail:tch@guet.edu.cn;汤申生(1969—),男,博士,主要研究方向为智能信息处理、网络行为分析;强保华(1972—),男,博士后,教授,主要研究方向为智能信息处理。

较适用于应用多专家属性的评判方法[10]，充分发挥各领域专家的经验和知识对评估目标进行评判。DS证据推理[11]可以看作是Bayes推理的一种扩展，能有效地处理在不确定和未知条件下的一致性推理问题，尤其是采用置信函数而不是概率作为度量，能满足比Bayes概率更弱的条件，在表达“不确定”、“无知”和进行不确定推理上具有独特的优势。王春雷[12]基于DS证据理论构建了适用于度量网络安全态势的形式模型，并将其用于支持态势数据关联分析，起到了很好的态势知识发现的效果。将DS证据理论与知识进行融合，应用在网络安全态势评估验证中，能有效地融合多专家在各层次态势评估指标上的意见，对态势评估结果进行可靠验证。

本文针对态势评估的正确性和合理性等问题，将DS证据推理引入态势评估，在深入研究评估准则和专家意见融合的基础上，提出基于DS融合的专家网络安全态势推理方法，并结合网络分层的脆弱性指数的计算实验对其进行验证。

1 基本定义

定义1 识别框架Θ为所有可能的观测结果范围的完备集，设$\Theta=\{\theta_1,\theta_2,\cdots,\theta_n\}$，在这个集合中，只能有一个假设是最后观测的正确结果，Θ的所有子集构成的集合是Θ的幂集，记为：2^{Θ}。

定义2 在Θ上的基本概率分配函数m为2^{Θ}到[0,1]上的函数，对$\forall A_i\subseteq\Theta$，满足：

$$\begin{cases} m(\varnothing)=0, m(A_i)\geqslant 0 \\ \sum\limits_i (Ai)=1 \end{cases} \tag{1}$$

其中，Θ为非空子集，A_i为焦点元素，m函数也称为在信任测度上的质量函数。

如果识别框架内仅有元素A_i被分配到概率$m(A_i)$，那么其余的基本概率就分配给Θ，用来描述“不确定”的情况，即不确定概率值，用θ来表示。

定义3 信任函数Bel用来描述获得的证据在识别框架Θ上对事件B的总支持度，定义为：

$$Bel(B)=\sum_{A\subseteq B} m(A) \tag{2}$$

定义4 似然函数Pls描述了获得的证据不能拒绝事件B的程度，定义为：

$$Pls(B)=\sum_{A\cap B=\varnothing} m(A) \tag{3}$$

如果m_1和m_2是由2个独立的证据源导出的基本概率分配函数，则合并后的概率分配函数为：

$$m(A)=m_1\oplus m_2=\frac{\sum\limits_{A_i\cap B_i\neq\varnothing} m_1(A_i)\cdot m_2(B_i)}{1-K} \tag{4}$$

其中，K为正交化常数，也称冲突权值，是独立于任一特定集合的归一化因子，计算为：

$$K=\sum_{A_i\cap B_i=\varnothing} m_1(A_i)\cdot m_2(B_i) \tag{5}$$

2 子网三层评估模型及分级描述

设由3台主机(H_1、H_2、H_3)构成了子网L三层评估模型。仅以脆弱性评估为例，为了评估L的脆弱性，首先建立其态势评估模型，如图1所示。

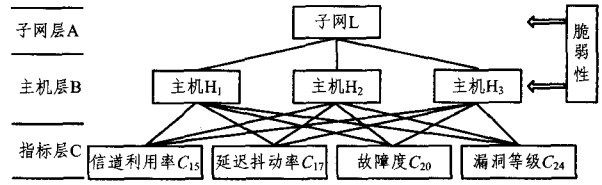

图1 子网L三层脆弱性评估模型

仅考虑评估子网L的脆弱性，以约简后的4个指标作为评估模型的底层指标(与脆弱性相关的态势指标约简已另文阐述)，信道利用率、延迟抖动率和故障度概念参见文献[13]。

定义5 漏洞等级是指网络主机所存在漏洞的危害级别。

一般预先设定漏洞等级的范围，数值越大，等级越高，危害性就越高，安全性也越差。设在时间序列上前后测得的漏洞等级为G_1和G_2，则漏洞等级的态势熵差计算为：

$$\begin{aligned}\Delta H_G &= -\log_2(G_2/\sum_{g=1}^{m} g)-(-\log_2(G_1/\sum_{g=1}^{m} g)) \\ &= -\log_2(G_2/G_1)\end{aligned} \tag{6}$$

其中，$G_1/\sum\limits_{g=1}^{m} g$和$G_2/\sum\limits_{g=1}^{m} g$分别是对$G_1$和$G_2$归一化。

事先已指定3台主机的相对重要性，利用层次法[14]计算得到C_{15}，C_{17}，C_{20}，C_{24} 4个态势指标在整个子网中的综合权值，分别为0.0625，0.1875，0.3125，0.4375。

定义6 给定单位分析时间窗口Δt，t时刻主机H_i的脆弱性指数为：

$$\begin{aligned}F_{H_i}(t) &= f(\overrightarrow{U_i}(t),\overrightarrow{J_i}(t),\overrightarrow{F_i}(t),\overrightarrow{G_i}(t),\overrightarrow{W_i}) \\ &= \overrightarrow{W_i}(\Delta\overrightarrow{H_{U_i}}(t)+\Delta\overrightarrow{H_{J_i}}(t)+\Delta\overrightarrow{H_{F_i}}(t)+(\sum_{k=1}^{m} V_k \\ &\quad \cdot\alpha^k\cdot C_k)e^{\Delta\overrightarrow{H_{G_i}}(t)})\end{aligned} \tag{7}$$

其中，$i=1,2,\cdots,n$，n为主机数；$\overrightarrow{W_i}$是各态势指标关于主机H_i的归一化计算权值；$\overrightarrow{U_i}(t)$是t时刻关于主机H_i的信道利用率向量；$\overrightarrow{J_i}(t)$是t时刻关于主机H_i的延迟抖动率向量；$\overrightarrow{F_i}(t)$是t时刻关于主机H_i的故障度向量；$\overrightarrow{G_i}(t)$是t时刻关于主机H_i的漏洞等级向量，以上向量均采用态势熵差法(Δ)计算[13]。m为Δt的数量，V_k是漏洞危害性权重，C_k是漏洞出现的数量，α为调节系数。

F_{H_i}的值越大，表明网络主机系统H_i的脆弱性越高，安全性能越低，其更大意义在于能反映两相邻时间窗口上的态势保持与趋势情况。

各层态势指数是对安全态势的定量描述，并在一定程度上反映了安全态势的发展趋势，态势指数的大小变化与所反映的网络安全态势保持一致。因此，可根据态势指数值对各层网络安全态势进行分级描述，将主机脆弱性安全态势按照其脆弱性指数F_H所在的区间划为5个等级，如表1所列。

表1 主机脆弱性安全态势分级描述

F_H值范围	脆弱性描述
>3.35	极危险
1～3.35	较危险
0.35～1	一般(中)
0.06～0.35	较安全
<0.06	很安全

3 评估准则及指标量化

事先给定一个参照等级，即目标识别框架 Θ，将它作为评判和识别的准则。设 $\Theta=\{$优(O_1)，良(O_2)，中(O_3)，差$(O_4)\}$，将其作为网络安全态势评估指标的评估准则。为了描述评估准则内各目标的可信程度，专家对各层评估指标进行评判，这种评判多依赖于专家的经验和知识，常采用“高”、“较低”、“很低”等模糊评语来表达对各指标安全性能的理解。设模糊评语集 $U=\{$很高，比较高，高，一般，比较低，低，很低$\}$，按七段构造来表达各模糊评语的量化七元组 $V=\{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$，$v_i\in[0,1]$。

定义 7 专家 x 对态势评估指标 C_m 的模糊评语到 Θ 每个目标识别对象等级的隶属度函数为：

$$\mu_x^{(C_m)(O_k)}=\frac{\sum_{i=1}^{7}\mathrm{Min}(\mu_{ij}^{(C_m)},\mu_j^{(O_k)})}{\sum_{j=1}^{7}\mathrm{Max}(\mu_{ij}^{(C_m)},\mu_j^{(O_k)})} \tag{8}$$

其中，$x=1,2,\cdots,n$，$k=1,2,3,4$，$i=1,2,\cdots,7$。

对 $\mu_x^{(C_m)(O_k)}$ 进行归一化：

$$\mu_x^{(C_m)(O_k)'}=\frac{\mu_x^{(C_m)(O_k)}}{\sum_{k=1}^{4}\mu_x^{(C_m)(O_k)}} \tag{9}$$

式(9)表示专家 x 对于指标 C_m 的模糊评语和 Θ 中每个等级对象的匹配程度，记为：

$$\mu_x^{(C_m)}=\{\mu_x^{(C_m)(O_1)'}(O_1),\mu_x^{(C_m)(O_2)'}(O_2),\mu_x^{(C_m)(O_3)'}(O_3),\mu_x^{(C_m)(O_4)'}(O_4)\} \tag{10}$$

4 融合知识的推理

通常不同的专家在知识、理解上存在差异，其权威、经验也不尽相同。因此，根据权威及其经验，预先给定 n 个专家可靠性系数：$w_1, w_2, \cdots, w_n$，一般取 $0.8\leqslant w_i\leqslant 1$，其中 $i=1,2,\cdots,n$。

因为专家的评判意见具有一定的不可靠性，并且专家的评判权重描述了不同专家的意见重要性，因此可以将其看作是他们评判意见的可信程度，所以专家的评判意见的隶属度并不全是确定的，即专家 x 对于态势评估指标 C_m 的评判意见的可信度或确定的部分可描述为：

$$\mu_x^{(C_m)^*}=w_x\cdot\mu_x^{(C_m)} \tag{11}$$

其中，$x=1,2,\cdots,n$，$m=1,2,\cdots,33$。

专家 x 对于态势评估指标 C_m 的评判意见的不确定的部分可描述为：

$$1-\sum_{k=1}^{4}w_x\cdot\mu_x^{(C_m)(O_k)'} \tag{12}$$

根据以上分析和定义 2 可知，上述具有不确定性的态势评估指标专家意见表达形式满足基本概率分配 m 函数的性质，因此，进行 m 函数的构造，将态势评估指标的验证准则集 $\Theta=\{$优(O_1)，良(O_2)，中(O_3)，差$(O_4)\}$作为目标识别空间，专家 x 对于评估指标 C_m（共 33 个评估指标）评判意见的 m 函数为：

$$m_x^{(C_m)}(O)=\begin{cases}w_x\cdot\mu_x^{(C_m)(O_1)'}O=\{O_1\}\\ w_x\cdot\mu_x^{(C_m)(O_2)'}O=\{O_2\}\\ w_x\cdot\mu_x^{(C_m)(O_3)'}O=\{O_3\}\\ w_x\cdot\mu_x^{(C_m)(O_4)'}O=\{O_4\}\\ 1-\sum_{k=1}^{4}w_x\cdot\mu_x^{(C_m)(O_k)'}O=\Theta\end{cases} \tag{13}$$

其中，$x=1,2,\cdots,n$，$C_m=C_1, C_2,\cdots, C_{33}$。

m 函数体现了专家对态势评估指标和目标识别空间中各等级对象匹配程度的信任度分布，记为：

$$m_x^{(C_m)}=\{m_x^{(C_m)}(O_1),m_x^{(C_m)}(O_2),m_x^{(C_m)}(O_3),m_x^{(C_m)}(O_4),m_x^{(C_m)}(\Theta)\} \tag{14}$$

由于专家对态势评估指标具有不确定的评判成分，而且各专家的意见是相互独立的，考虑到态势评估指标专家意见表达符合 m 函数性质，因此可以采用 DS 合成公式进行综合。在式(4)基础上，给出 m 函数合成规则定义：

定义 8 设 $Bel_1, Bel_2,\cdots,Bel_n$ 是目标识别空间 Θ 上的信任函数，$m_1, m_2,\cdots,m_n$ 分别是 $Bel_1, Bel_2,\cdots,Bel_n$ 的质量函数，用 DS 规则合成后的信任函数记为 $\bigoplus_{i=1}^{n}Bel_i$，则对应的质量函数由下式确定：

令 $A\subset\Theta$，$A\neq\varnothing$，则

$$m(A)=m_1(A_1)\oplus m_2(A_2)\oplus\cdots\oplus m_n(A_n)=\frac{\sum_{\bigcap_{i=1}^{n}A_i\neq\varnothing}m_1(A_1)\cdot m_2(A_2)\cdot m_n(A_n)}{1-K} \tag{15}$$

其中，$K=\sum_{\bigcap_{i=1}^{n}A_i=\varnothing}m_1(A_1)\cdot m_2(A_2)\cdot\cdots\cdot m_n(A_n)$。

对于式(15)，如果 n 个证据信息完全不能确定，此时分母为零，证据信息无法合成，但在部分不能确定的条件下，能使合成结果中的不确定信息减少，可产生新的质量函数，并作为更高层次的证据对象，从而适用于多层次的网络安全态势评估模型，将多专家针对多层次的态势评估指标评判知识进行 DS 融合推理。

根据式(13)和式(14)，对 n 个专家的评判意见进行融合后的结果记为：

$$m^{(C_m)}=\{m^{(C_m)}(O_1),m^{(C_m)}(O_2),m^{(C_m)}(O_3),m^{(C_m)}(O_4),m^{(C_m)}(\Theta)\} \tag{16}$$

式(16)体现了综合多专家对态势评估指标和目标识别空间中各等级对象的匹配程度的信任度分布，要进一步得出专家对上一层(即主机层)的评判意见，需考虑各指标对目标的重要性问题。

定义 9 设态势评估指标 C_m 的重要性权重为 w_{C_m}，则各评估指标的相对重要度定义为：

$$\eta_{w_m}=w_{C_m}/\max_{1\leqslant i\leqslant m}(w_{C_m}) \tag{17}$$

其中，$m=1,2,\cdots,33$，设有 33 个相关态势指标。

η_{w_m} 反映了各指标间的重要性差异。指标的重要性权重也具有一定的不可靠性，即各指标在验证准则集中各参考等级上的信任程度也不全是确定的，即在评估主机 H_i 的安全

态势时，专家评判意见的可信度或确定的部分可描述为：

$$m^{(C_m)^*}=\eta_{w_m}\cdot m^{(C_m)} \tag{18}$$

其中，$C_m=C_1,C_2,\cdots,C_{33}$，$w_m=w_1,w_2,\cdots,w_{33}$。

而专家对于主机 H_i 的态势评判意见的不确定的部分可描述为：

$$1-\sum_{k=1}^{4}\eta_{w_m}\cdot m^{(C_m)}(O_k) \tag{19}$$

于是，使用相对重要度修正后的质量函数为：

$$m^{(C_m)^*}=\{m^{(C_m)^*}(O_1),m^{(C_m)^*}(O_2),m^{(C_m)^*}(O_3),m^{(C_m)^*}(O_4),m^{(C_m)^*}(\Theta)\} \tag{20}$$

由于各评估指标、各主机、专家评判过程都是相互独立的，可再次利用式(15)进行融合，得到上一层，即主机层的态势评判意见的质量函数：

$$m^{(H_i)}=\{m^{(H_i)}(O_1),m^{(H_i)}(O_2),m^{(H_i)}(O_3),m^{(H_i)}(O_4),m^{(H_i)}(\Theta)\} \tag{21}$$

按同样的方法，可对更上一层即子网层的态势进行专家评判，依次可得最高层的融合评判结果。

定义 10 设 $\exists O_1,O_2\subset\Theta$，并在预先给定的门限值 ε_1 和 ε_2 条件下，满足

$$\begin{cases}m(O_1)=\max\{m(O_i),O_i\subset\Theta\}\\ m(O_2)=\max\{m(O_i),O_i\subset\Theta\text{ 且 }O_i\neq O_1\}\end{cases} \tag{22}$$

并且

$$\begin{cases}m(O_1)-m(O_2)>\varepsilon_1\\ m(\theta)<\varepsilon_2\\ m(O_1)>m(\theta)\end{cases} \tag{23}$$

那么，O_1 为验证准则的决策。

5 网络安全态势评估实例分析

设专家评判指标体系以图 1 给出的分层模型为依据，选择 $n=3$ 个专家组成评判群体，首先对底层各评估指标进行定性的评判。以主机 H_1 为例，结合专家经验和知识，根据模糊评语集 U，针对主机 H_1 的信道利用率 C_{15}、延迟抖动率 C_{17}、故障度 C_{20} 和漏洞等级 C_{24} 指标对各评估指标给出相关评判意见，如表 2 所列。

表 2 主机 H_1 评估指标专家评判意见

专家 x	C_{15}	C_{17}	C_{20}	C_{24}
x=1	高	高	一般	比较高
x=2	比较高	比较高	比较低	比较高
x=3	比较高	一般	比较低	一般

为了保证对态势评估指标的模糊评语和验证准则上的一致性，将表 2 中的评判意见统一转换成有利于网络安全态势的角度描述，如表 3 所列。

表 3 转换后的主机 H_1 评估指标专家评判意见

专家 x	C_{15}	C_{17}	C_{20}	C_{24}
x=1	高	低	一般	比较低
x=2	比较高	比较低	比较高	比较低
x=3	比较高	一般	比较高	一般

根据专家权威和经验确定其意见重要性，即建立可靠性系数：$w_x=(0.85,0.90,0.95)$。验证过程是，首先按照式(13)和式(14)建立各专家关于各指标的评判意见的 m 函数，然后进行融合得到评估指标的多专家综合评判意见的 m 函数，继而对关于主机 H_1 不同指标间的意见进行合成，得到关于主机 H_1 的综合评判意见的 m 函数。

主机 H_1 的各专家关于各评估指标的评判意见的 m 函数如表 4 所列。

表 4 各专家评判意见的 m 函数

指标	x	O_1	O_2	O_3	O_4	θ
$m^{(C_{15})}$	1	0.4922	0.3576	0	0	0.1502
	2	0.0584	0.7158	0.1258	0	0.1000
	3	0.0617	0.7556	0.1328	0	0.0499
$m^{(C_{17})}$	1	0	0	0.4250	0.4250	0.1500
	2	0	0.1258	0.7158	0.0584	0.1000
	3	0	0.4750	0.4750	0	0.0500
$m^{(C_{20})}$	1	0	0.4250	0.4250	0	0.1500
	2	0.0584	0.7158	0.1258	0	0.1000
	3	0.0617	0.7556	0.1328	0	0.0499
$m^{(C_{24})}$	1	0	0.1188	0.6760	0.0552	0.1500
	2	0	0.1258	0.7158	0.0584	0.1000
	3	0	0.4850	0.4750	0	0.0500

按照式(15)进行融合，得到多专家综合评判意见的 m 函数，如表 5 所列。

表 5 多专家综合评判意见的 m 函数

指标	O_1	O_2	O_3	O_4	θ
$m^{(C_{15})}$	0.0303	0.9521	0.0155	0	0.0021
$m^{(C_{17})}$	0	0.0638	0.9193	0.0142	0.0028
$m^{(C_{20})}$	0.0047	0.9364	0.0573	0	0.0019
$m^{(C_{24})}$	0	0.0836	0.9319	0.0023	0.0020

采用第 3 节给出的指标综合权值，并根据式(17)和式(20)计算各指标相对重要度，得到修正后的多专家综合评判意见的 m 函数，如表 6 所列。

表 6 修正后的多专家综合评判意见的 m 函数

指标	O_1	O_2	O_3	O_4	θ
$m^{(C_{15})*}$	0.0043	0.1361	0.0022	0	0.8574
$m^{(C_{17})*}$	0	0.0273	0.3940	0.0061	0.5276
$m^{(C_{20})*}$	0.0034	0.6689	0.0409	0	0.2868
$m^{(C_{24})*}$	0	0.0836	0.9319	0.0023	0.0020

继续融合，得到主机 H_1 的专家综合评判意见的 m 函数：

$$m^{(H_1)}=\{0(O_1),0.1404(O_2),0.7581(O_3),0.0009(O_4),0.0008(\Theta)\} \tag{24}$$

如果给定 $\varepsilon_1=0.6$ 和 $\varepsilon_2=0.001$，则根据定义 10 可以判定主机 H_1 的安全态势为 O_3，即属于“中”性安全态势，这与原网络主机层的主机脆弱性指数实验计算值的分级描述级别绝大部分相符合。

6 实验结果及分析

在对照实验中仅对配置有 Linux Ubuntu 8.04 LTS /Intel Core 2 Duo E7200/2G/250G 主机 H_1 的网络安全态势进行脆弱性评估，实验环境中还有其他服务器、防火墙等设备，取时间序列为 12 小时，基于文献[13]的方法，采集并分析与该主机有关的信道利用率、延迟抖动、故障及漏洞等信息，即首先取得各时间窗口主机 H_1 的信道利用率态势熵差向量

(下转第 125 页)

[4] AlZain M A, Soh B, Pardede E. MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing[C]//DASC. Sydney, Australia, 2011: 784-791

[5] Trostle J. Protecting Against Distributed Denial of service attacks Using Distributed Filtering[C]//Securecomm and Workshops. Baltimore, USA, 2006: 1-11

[6] Bhaskaran M, Natrarajan A M, Sivanandam S N. Tracebacking the Spoofed IP Packets in Multi ISP Domains with Secured Communication[C]//ICSCN. Chennai, India, 2007: 579-584

[7] Joshi B, Vijayan A S, Joshi B K. Securing Cloud Computing Environment Against DDoS Attacks[C]//ICCCI. Coimbatore, India, 2012: 1-5

[8] 陈亚睿，田立勤，杨扬. 云计算环境下基于动态博弈论的用户行为模型与分析[J]. 电子学报，2011，8：1818-1823

[9] Niyato D, Vasilakos A V. Resource and Revenue Sharing with Coalition Formation of Cloud Providers: Game Theoretic Approach[C]//CCGrid. Newport Beach, CA, USA, 2011: 215-224

[10] Karnwal T, Sivakumar T, Aghila G. A Comber Approach to Protect Cloud Copmputing against XML DDoS and HTTP DDoS attack[C]//SCEECS, Bhopal, India, 2012: 1-5

[11] Chen Qi, Lin Wen-min, Dou Wan-chun, et al. CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment [C]//DASC. Sydney, Australia, 2011: 427-434

[12] 谢立军，朱智强，孙磊，等. 基于隶属度理论的云服务行为信任评估模型研究[J]. 计算机应用研究，2012，30(4)：1051-1054

[13] Niyato D, Wang P, Hossain E, et al. Game Theoretic Modeling of Cooperation among Service Providers in Mobile Cloud Computing Environments[C]//WCNC. Shanghai, China, 2012: 3128-3133

[14] 张维迎. 博弈论与信息经济学[M]. 上海：上海人民出版社，2004

(上接第 110 页)

7 $\Delta\vec{H}_{U_{ij}}$ $(j=1,2,\cdots,m)$、延迟抖动率态势熵差向量 $\Delta\vec{H}_{I_{ij}}$ $(j=1,2,\cdots,m)$、故障度态势熵差向量 $\Delta\vec{H}_{F_{ij}}$ $(j=1,2,\cdots,m)$和漏洞等级态势熵差向量 $\Delta\vec{H}_{G_{ij}}$ $(j=1,2,\cdots,m)$，m 为单位分析时间窗口的数量，再按式(6)计算对应的主机脆弱性指数值变化序列，如图 2 所示。

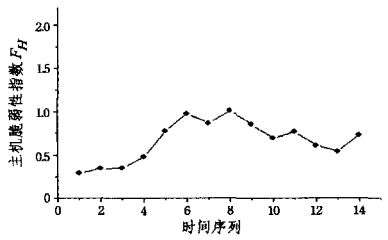

图 2 主机 H_1 脆弱性安全态势

图 2 表明该主机的脆弱性处于较稳定的状态，变化平稳，主机系统受到的攻击或威胁不是很剧烈。根据表 1 提供的描述分级，可以认定该主机在分析时间序列范围内，脆弱性态势处于“一般”状态，这与基于 DS 融合的态势评估值保持一致。

结束语 通过建立网络安全态势指标的识别空间和评估准则，并基于专家意见融合的推理过程，实现了一种基于 DS 证据融合理论的专家网络安全态势评估方法，并通过脆弱性指数实验对其进行了验证，二者可以相互印证。实验表明该方法能克服复杂网络中大量不确定因素的影响，可很好地解决态势评估中存在的正确性和合理性质疑等问题。本文主要以脆弱性评估为例进行描述，对于其他评估角度(如稳定性、威胁性和容灾性等)也有相同的评估效果。而利用态势评估值对态势进行预测，建立有效的网络安全态势预警系统是下一步要进行的工作。

参 考 文 献

[1] Farinelli A, Nardi D, Pigliacampo R, et al. Cooperative situation assessment in a maritime scenario[J]. International Journal of Intelligent Systems, 2012, 27(5): 477-501

[2] 付钰，吴晓平，叶清. 基于改进 FAHP-BN 的信息系统安全态势评估方法[J]. 通信学报，2009，30(9)：135-140

[3] Zhao Jin-hui, Zhou Yu, Shuo Liang-xun. A situation awareness model of system survivability based on variable fuzzy set[J]. Telkomnika, 2012, 10(8): 2239-2246

[4] 姜伟，方滨兴，田志宏，等. 基于攻防博弈的网络安全测评和最优主动防御[J]. 计算机学报，2009，32(4)：817-827

[5] Jakobson G. Mission cyber security situation assessment using impact dependency graphs[C]//Proceedings of the International Conference on Information Fusion (FUSION). Chicago, IL, USA: IEEE, 2011

[6] Kirillov V P. Constructive stochastic temporal reasoning in situation assessment[J]. IEEE Transactions on Systems, Man and Cybernetics, 1994, 24(8): 1099-1113

[7] Miao A X, Zacharias G L, Shih-ping K. Computational situation assessment model for nuclear power plant operations[J]. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 1997, 27(6): 728-742

[8] Xiao Hai-dong, Li Jian-hua. Analysis of security situation of networks based on knowledge base[J]. WSEAS Transactions on Electronics, 2006, 3(1): 34-39

[9] Holsopple J, Sudit M, Nusinov M, et al. Enhancing situation awareness via automated situation assessment[J]. IEEE Communications Magazine, 2010, 48(3): 146-152

[10] Zhao Jin-jing, Wen Yan, Wang Dong-xia. A network security evaluation method framework based on multiple criteria decision making theory[C]//Proceedings of the 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Seoul, Korea: IEEE Comput. Soc, 2011: 371-375

[11] Feng Xue-wei, Wang Dong-xia, Ma Guo-qing, et al. Security situation assessment based on the DS theory[C]//Proceedings of the 2nd International Workshop on Education Technology and Computer Science. Wuhan, China: IEEE Comput. Soc, 2010: 352-356

[12] 王春雷，方兰，王东霞，等. 基于知识发现的网络安全态势感知系统[J]. 计算机科学，2012，39(7)：11-17，24

[13] 唐成华，王鑫，张瑞霞，等. 基于态势熵的网络安全态势评估指标体系研究[J]. 桂林电子科技大学学报，2011，31(4)：270-274

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