基于 WOWA-FAHP 的网络安全态势评估

吕镇邦[1,2] 周 波[1]

(中国航空计算技术研究所 西安 710068)[1] (西安电子科技大学计算机学院 西安 710071)[2]

摘 要 从入侵响应决策与安全管理的实际需求出发,提出了基于 WOWA 合成的模糊层次分析法(WOWA-FAHP)和基于 WOWA-FAHP 的网络安全态势评估模型。WOWA-FAHP 方法在继承模糊层次分析法优点的基础上兼顾属性间的客观、主观关联性,能够适应各种决策偏好。基于 WOWA-FAHP 的评估模型把动态评估与静态评估相结合,充分利用系统安全风险评估、入侵警报融合关联、异常监测与安全审计所提供的多种信息,综合考虑警报类、异常类、脆弱性、后果性等多方面的评价指标,并依据不同安全策略,通过 WOWA-FAHP 方法处理诸如评价要素间的复杂关系。网络应用服务系统安全态势评估实例证明了方法与模型的有效性。

关键词 网络安全,态势评估,WOWA 算子,模糊层次分析法,决策偏好

中图法分类号 TP393.08 **文献标识码** A

Network Security Situation Assessment Based on WOWA-FAHP

LU Zhen-bang[1,2] ZHOU Bo[1]

(Aeronautics Computing Technique Research Institute, Xi'an 710068, China)[1]

(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)[2]

Abstract For the practical purposes of intrusion response decision-making and security management, a Fuzzy Analytic Hierarchy Process approach based on Weighted Ordered Weighted Averaging aggregation(WOWA-FAHP) and a network security situation assessment model based on WOWA-FAHP were proposed. Besides preserving the merits of the FAHP, the WOWA-FAHP approach takes into account both objective and subjective associations among the attributes, and is able to adapt various decision preferences. The assessment model based on WOWA-FAHP combines static and dynamic assessments; utilizes multiple information sources, such as system security risk evaluation, intrusion alert fusion and correlation, anomaly monitor and security audit; considers multiple aspects, such as intrusion alerts, anomalies, vulnerabilities, and attack effects; and handles the complex relations among the factors with the WOWA-FAHP approach according to different security policies. The effectiveness of the proposed approach and model is illustrated via an actual security situation assessment for a network application service system.

Keywords Network security, Situation assessment, Weighted ordered weighted averaging operator, Fuzzy analytic hierarchy process, Decision preference

网络安全态势评估是信息安全研究领域的一个新方向,是贯穿信息系统生命周期的重要技术手段。切实有效的网络安全态势评估可以使安全管理人员准确及时地把握网络安全状况及其发展趋势,为其决策提供支持。现有安全态势评估研究工作主要集中在系统风险评估和攻击后果评估。系统风险评估依据一定的标准,基于威胁、脆弱性和资产价值 3 个指标定性或定量地评估网络的安全风险状况[1],属于宏观性的静态的认知方法。攻击后果评估则是在获得入侵信息及相关知识的基础上,通过入侵场景重建或入侵警报关联来动态评估安全状况[2],这种专注于攻击本身的态势评估方法具有明显的局限性。文献[3]利用 IDS 警报并结合系统运行指标,基于服务、主机的重要性,构建了层次化网络安全威胁态势评估模型并提出了相应的量化计算方法,使该领域的研究推进了一大步。但其不足在于未将态势评估与具体的网络环境信息相结合,并且使用传统的加权平均方法合成评估结果,其对安全要素的关联受到算法本身的限制。

总之,信息源单一、评价指标片面以及忽略主观/客观关联性与决策偏好是现有安全态势评估方法的两大缺陷。在安全态势评估中需要考虑诸多的客观、主观因素。一般来说,客观因素能够反映出系统安全状态和攻击威胁情况,而主观因素更能够反映系统安全策略和管理员的决策意向。在网络层次化安全态势评估中,对处于底层的应用服务系统安全态势的恰当评估成为整个评估模型的基础和关键。应用服务安全态势评估涉及的因素很多,具有相当的复杂度和不确定性。本文将其归结为复杂系统的多属性决策问题,提出了基于 WOWA 合成的模糊层次分析法并将其应用于安全态势评

到稿日期:2008-08-07 返修日期:2008-11-02 本文受国家自然科学基金资助项目(60573036),航空基础科学基金资助项目(03F31007)资助。

吕镇邦(1976—),男,博士研究生,主要研究方向为模糊计算、信息安全,E-mail:lvzhenbang@tom.com;周 波(1959—),男,研究员,主要研究方向为系统工程、信息安全。

估。基于 WOWA-FAHP 的网络安全态势评估方法把动态评估与静态评估相结合，利用系统安全风险评估、入侵警报融合关联、异常检测与安全审计所提供的多种信息，综合考虑了关于应用服务的警报类指标信息、异常类指标信息、脆弱性指标信息以及后果性指标信息，并能够处理诸评价指标间的复杂关系，同时适应各种决策偏好，较好地解决了这一难题。

1 预备知识

1.1 模糊层次分析法(FAHP)

层次分析法(Analytic Hierarchy Process，AHP)是美国著名运筹学家 Satty 于 20 世纪 70 年代中期提出的一种经典的多属性决策分析方法。它从系统的观点出发，把复杂的问题分解为各个组成因素，将这些组成因素按照一定的关系进行分组，形成有序的递阶层次结构，通过两两比较确定每一层次中各因素的相对重要性，进而得到决策因素相对于目标的重要性分值。针对 AHP 在一致性检验方面的问题与复杂性，文献[4]把模糊思想和方法引入层次分析法中，提出了模糊层次分析法(Fuzzy Analytic Hierarchy Process，FAHP)。

模糊层次分析法[4]是在层次分析法的基础上，结合模糊综合评判法，在权重集的构建上引入模糊一致判断矩阵进行评价的一种层次化决策分析方法，其核心是构建满足一致性要求的模糊判断矩阵。利用模糊层次分析法计算评价指标的权数分配，与模糊综合评判法相比可以有效地减少主观因素。FAHP 是一种定性与定量相结合、综合化程度较高的评价方法，它与传统 AHP 的区别在于判断矩阵的模糊性。它简化了人们判断属性相对重要性的复杂程度，借助模糊判断矩阵实现决策由定性向定量方便、快捷的转换，直接由模糊判断矩阵构造模糊一致性判断矩阵，使判断的一致性问题得到有效解决。

1.2 WOWA 合成算子

加权平均(Weighted Mean，WM)算子和有序加权平均(Ordered Weighted Averaging，OWA)算子是两类重要的加权集结算子，广泛应用于信息融合与数据合成[5,6]。WM 算子考虑不同数据源的可靠性或重要性，权值对应于固定的数据源；OWA 算子则考虑各数据源之间的相互关系，权值与各数据源本身的重要性无关。WOWA(Weighted Ordered Weighted Averaging，Weighted OWA)算子基于 OWA 算子并综合了 WM 算子，用两组权同时考虑这两方面的因素，并可从两组权计算一组新的权[7]。

定义 1 设 $F:R^n\to R$，若：

(1) $p=[p_1,p_2,\cdots,p_n]^T$，$\sum_{i=1}^{n}p_i=1$，$p_i\in[0,1]$，$i=1,2,\cdots,n$

(2) $w=[w_1,w_2,\cdots,w_n]^T$，$\sum_{i=1}^{n}w_i=1$，$w_i\in[0,1]$，$i=1,2,\cdots,n$

(3) $a_\sigma=[a_{\sigma(1)},a_{\sigma(2)},\cdots,a_{\sigma(n)}]^T$ 是任意 n 维实向量 $a=[a_1,a_2,\cdots,a_n]^T$ 中元素以降序排列组成的向量

(4) $\omega=[\omega_1,\omega_2,\cdots,\omega_n]^T$，$\omega_i=w^*\left(\sum_{j\leqslant i}p_{\sigma(j)}\right)-w^*\left(\sum_{j<i}p_{\sigma(j)}\right)$，其中 w^* 是对点集$\{(0,0)\}\cup\{(\frac{i}{n},\sum_{j\leqslant i}w_j)\}$插值得到的单调递增函数

(5) $F(a_1,a_2,\cdots,a_n)=\omega^Ta_\sigma=\sum_{j=1}^{n}\omega_ja_{\sigma(j)}$

则称 F 为 n 维 WOWA 算子。

当 WM 权向量 $p=p_{avg}=[\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n}]^T$ 时，$\omega=w$，WOWA 算子退化为 OWA 算子；当 OWA 权向量 $w=w_{avg}=[\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n}]^T$ 时，$\omega=p$，WOWA 算子退化为 WM 算子。

2 基于 WOWA 合成的模糊层次分析法

与 AHP 一样，FAHP 中的合成运算通常取为最大-最小型 $\Delta=(\wedge,\vee)$，最大-积型 $\Delta=(\cdot,\vee)$及加权平均型 $\Delta=(\cdot,\oplus)$等。这些合成运算很难同时反映各要素的客观属性和主观上的决策偏好，其中最常用的加权平均合成运算实质上忽略了属性间的关联性。由 Torra 提出的 WOWA 算子综合了 WM 和 OWA，能够很好地满足这一需求。因此本文将 WOWA 合成运算引入 FAHP，提出基于 WOWA 合成的 FAHP 评判方法。

基于 WOWA 合成的 FAHP 与传统基于 WM 合成的 FAHP 最主要的区别在于 WOWA 算子同时包括两组权重：反映客观属性的重要性权向量 p 和反映主观属性的关联性权向量 w。

WOWA 算子基于 OWA 算子并综合了 WM 算子，兼顾各数据源的重要性与相互关系，本质上是一种特殊的 Choquet 模糊积分[7,8]。OWA 算子是泛化的析取/合取运算，当各原因节点的重要性相当时，WOWA 算子退化为 OWA 算子。WOWA/OWA 算子的与或度可由如下定义的 orness 测度衡量。利用具有不同 orness 的权向量，WOWA/OWA 算子能够模拟各种确定的或模糊的与或关系[5-8]。

定义 2 $orness(w)=\frac{1}{n-1}\sum_{j=1}^{n}(n-j)w_j$

如下所示为一组简单的合成规则：

(1) If orness is low then $w=w_{min}=[0,0,\cdots,1]^T$；

(2) If orness is medium then $w=w_{avg}=[\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n}]^T$；

(3) If orness is high then $w=w_{max}=[1,0,\cdots,0]^T$。

基于 WOWA 合成的 FAHP 方法的基本步骤和算法如下：

(1)构建层次化评价指标体系

将复杂问题概念化，找出研究对象所涉及的主要因素。通过分析各因素的关联、隶属关系，构建有序的多层次结构模型。层次模型的构造是基于分解法的思想，进行对象的系统分解，目的是基于系统基本特征建立系统的评估指标体系，其基本层次有 3 类：目标层、准则层和指标层。

(2)设定 FAHP 各层的因素集和评判集

将评价目标看成是由多种因素组成的模糊集合(称为因素集)，再设定这些因素所能选取的评审等级，组成评语的模糊集合(称为评判集)。$U=\{u_1,u_2,\cdots,u_n\}$为准则层或指标层中评判对象的各因素组成的集合，称为因素集，其中 u_i 为 FAHP 中的一个准则或指标($1<i<n$)。$V=\{v_1,v_2,\cdots,v_m\}$为多种决断评语构成的集合，称为评判集。

(3)建立 U 到 V 的模糊关系矩阵

构造模糊映射 $f:U\to F(V)$，$u_i\to f(u_i)=(r_{i1},r_{i2},\cdots,r_{im})\in F(V)$。$F(V)$是 V 上的模糊集全体，映射 f 表示因素对评

判集中各评语的支持程度。令 $R_i=\{r_{i1},r_{i2},\cdots,r_{im}\}$，$i=1,2,\cdots,n$，于是得到 U 到 V 的模糊关系矩阵：

$$R=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix}$$

称 R 为隶属度矩阵。

(4)建立模糊判断矩阵

模糊判断矩阵 F 表示针对上一层某元素，本层次与之有关元素(子属性)之间相对重要性的比较。模糊一致判断矩阵可表示为

$$F=\begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{bmatrix}$$

f_{ij} 指本层次第 i 个元素对第 j 个元素具有模糊关系"…比…重要得多"的隶属度，可采用文献[4]中的 0.1～0.9 标度表给予数量标度。

(5)将模糊判断矩阵 F 一致化，确定重要性权重向量 p。

首先对模糊判断矩阵 F 按行求和：

$$s_i=\sum_{j=1}^{n} f_{ij},\ i=1,\cdots,n;$$

然后进行线性变换：

$$\overline{f}_{ij}=\frac{s_i-s_j}{2n}+0.5;$$

如此得到模糊一致判断矩阵：

$$\overline{F}=\begin{bmatrix} \overline{f}_{11} & \overline{f}_{12} & \cdots & \overline{f}_{1n} \\ \overline{f}_{21} & \overline{f}_{22} & \cdots & \overline{f}_{2n} \\ \vdots & \vdots & & \vdots \\ \overline{f}_{n1} & \overline{f}_{n2} & \cdots & \overline{f}_{nn} \end{bmatrix}$$

确定重要性权重向量 $p=[p_1,p_2,\cdots,p_n]^T$，其中

$$p_i=\frac{2\sum_{\substack{j=1\\ j\neq i}}^{n}\overline{f}_{ij}}{n(n-1)}。$$

(6)根据决策偏好，确定关联性权重向量 w

OWA 合成算子的关键在于其权值向量 w 的取值。通过选择适当的权向量 w，我们可以获得各式各样的聚合算法。如果 w 支持值较大的证据，称为乐观(Optimistic)融合，典型的如 Max 算子；如果 w 支持值较小的证据，称为悲观(Pessimistic)融合，典型的如 Min 算子；而所谓的折衷或近中原则偏向于支持中间值证据。在 FAHP 中引入 OWA 合成算子，使得决策者能够按照具体的安全策略和决策偏好(乐观/悲观度)来协调安全态势评估。

Yager 所定义的 orness 测度，即是用来度量 OWA 合成算子的乐观度/悲观度。对于给定的 $orness(w)$，可通过求解最大熵规划模型[9]或最小方差规划模型[10]来确定权向量 w。此外，也可以基于"some，at most，at least"等模糊语言量词来构造 OWA 集结权向量 w。这些模糊语言量词本身就直观地反映了决策偏好[5,6]。

(7)由 WM 权向量和 OWA 权向量合成 WOWA 权向量 ω

根据 WOWA 算子的定义，WOWA 权向量 ω 是由 WM 权重向量 p 和 OWA 权重向量 w 通过对点集 $\{(0,0)\}\cup\{(\frac{i}{n},\sum_{j\leqslant i}w_j)\}$ 插值，构造单调递增的函数 w^* 而得到的。插值函数 w^* 可以有多种。本文采用由二次 Bernstein 多项式曲线构成的分段插值方法[11]。

(8)自下而上，基于 WOWA 合成算子逐级综合评判。

3 网络安全态势评估实例

本节以某实际的网络应用服务系统为对象，应用基于 WOWA 合成的 FAHP 方法实施网络安全态势评估。

(1)构建评估指标体系、因素集

建立基于 WOWA 合成的 FAHP 安全态势评估模型，如图 1 所示，包括目标层、准则层和指标层共 3 个层次。目标层元素为某待评应用服务系统的风险指数。准则层包括警报、脆弱性、异常和后果。警报类指标包括警报数量、警报种类、警报的置信度和相关性，相关数据可由 IDS 与警报融合关联系统得到。脆弱性指标包括服务开放度、攻击容易度、攻击隐蔽性(攻击者无风险度)，相关数据可由脆弱性与威胁评估得到；异常类指标包括用户异常、服务异常、系统异常，相关数据可由异常监测和安全审计得到；后果类指标包括机密性、完整性和可用性，相关数据可由信息资产评估得到。

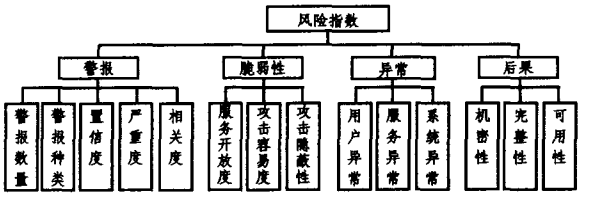

图 1 基于 WOWA 合成的 FAHP 安全态势评估模型

(2)确定评判集、建立底层指标评判矩阵

为简便计算，本例选用四级评语判断集 $V=\{Severe,High,Medium,Low\}$，依次建立警报类指标、脆弱性指标、异常类指标、后果类指标评判矩阵如下：

$$R_1=\begin{bmatrix} 0.3 & 0.4 & 0.2 & 0.1 \\ 0.2 & 0.5 & 0.2 & 0.1 \\ 0.5 & 0.4 & 0.1 & 0.0 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.5 & 0.1 & 0.1 \end{bmatrix}$$

$$R_2=\begin{bmatrix} 0.4 & 0.2 & 0.3 & 0.1 \\ 0.3 & 0.5 & 0.1 & 0.1 \\ 0.5 & 0.3 & 0.1 & 0.1 \end{bmatrix}$$

$$R_3=\begin{bmatrix} 0.2 & 0.2 & 0.5 & 0.1 \\ 0.1 & 0.2 & 0.3 & 0.4 \\ 0.5 & 0.4 & 0.1 & 0.0 \end{bmatrix}$$

$$R_4=\begin{bmatrix} 0.1 & 0.4 & 0.4 & 0.1 \\ 0.3 & 0.4 & 0.2 & 0.1 \\ 0.2 & 0.5 & 0.2 & 0.1 \end{bmatrix}$$

(3)建立模糊判断矩阵，确定 WM 权重向量

根据 0.1～0.9 标度，建立准则层模糊矩阵：

$$F=\begin{bmatrix} 0.5 & 0.6 & 0.7 & 0.9 \\ 0.4 & 0.5 & 0.7 & 0.8 \\ 0.3 & 0.3 & 0.5 & 0.8 \\ 0.1 & 0.2 & 0.2 & 0.5 \end{bmatrix}$$

模糊一致化矩阵：

$$\bar{F}=\begin{bmatrix}0.500 & 0.538 & 0.600 & 0.713\\ 0.462 & 0.500 & 0.562 & 0.675\\ 0.400 & 0.438 & 0.500 & 0.613\\ 0.287 & 0.325 & 0.387 & 0.500\end{bmatrix}$$

求得准则层 WM 权重向量：

$p=[0.309 \quad 0.283 \quad 0.241 \quad 0.167]^T$

同样方法求得指标层 WM 权重向量：

$P_1=[0.201 \quad 0.249 \quad 0.289 \quad 0.159 \quad 0.102]^T$；

$P_2=[0.267 \quad 0.367 \quad 0.366]^T$

$P_3=[0.466 \quad 0.267 \quad 0.267]^T$

$P_4=[0.500 \quad 0.167 \quad 0.333]^T$

(4)根据决策偏好确定 OWA 权重向量

OWA 权向量直接反映评估者的决策偏好或乐观度/悲观度。为便于比较本方法跟普通 FAHP 方法的合成评估结果，本例仅对准则层采用非退化 WOWA 算子合成。

采用“轻两头重中间”的(橄榄球型)决策偏好，得到准则层 OWA 权重向量：

$w=[0.125 \quad 0.375 \quad 0.375 \quad 0.125]^T$。

对指标层的合成则采用完全折衷的决策取向。OWA 权重向量：

$W_1=[0.2 \quad 0.2 \quad 0.2 \quad 0.2 \quad 0.2]^T$

$W_2=[0.333 \quad 0.333 \quad 0.333]^T$

$W_3=[0.333 \quad 0.333 \quad 0.333]^T$

$W_4=[0.333 \quad 0.333 \quad 0.333]^T$

(5)由 WM 权向量和 OWA 权向量合成 WOWA 权向量

由准则层 OWA 权向量 $w=[0.125 \quad 0.375 \quad 0.375 \quad 0.125]^T$，采用 Bernstein 插值方法，得到插值函数：

$$w^*(x)=\begin{cases}1-2(1-x)^2, & x\geqslant 0.5\\ 2x^2, & x<0.5\end{cases}$$

根据 WOWA 算子定义中的权向量合成公式 $\omega_i=w^*\left(\sum_{j\leqslant i}p_{\sigma(j)}\right)-w^*\left(\sum_{j<i}p_{\sigma(j)}\right)$，由准则层 WM 权向量 $p=[0.309 \quad 0.283 \quad 0.241 \quad 0.167]^T$，求得准则层 WOWA 算子权向量：

$\omega=[0.191 \quad 0.476 \quad 0.277 \quad 0.056]^T$

在本例中，由于指标层 OWA 权向量退化为算术平均算子，指标层 WOWA 合成算子退化为 WM 算子：

$\omega_1=P_1=[0.201 \quad 0.249 \quad 0.289 \quad 0.159 \quad 0.102]^T$

$\omega_2=P_2=[0.267 \quad 0.367 \quad 0.366]^T$

$\omega_3=P_3=[0.466 \quad 0.267 \quad 0.267]^T$

$\omega_4=P_4=[0.500 \quad 0.167 \quad 0.333]^T$

(6)基于 WOWA 的逐级综合评判

$A_1=\omega_1{}^T\cdot R_1=[0.333 \quad 0.419 \quad 0.177 \quad 0.071]$

$A_2=\omega_2{}^T\cdot R_2=[0.400 \quad 0.347 \quad 0.153 \quad 0.100]$

$A_3=\omega_3{}^T\cdot R_3=[0.253 \quad 0.253 \quad 0.340 \quad 0.154]$

$A_4=\omega_4{}^T\cdot R_4=[0.167 \quad 0.433 \quad 0.300 \quad 0.100]$

$$A=\begin{bmatrix}A_1\\ A_2\\ A_3\\ A_4\end{bmatrix}=\begin{bmatrix}0.333 & 0.419 & 0.177 & 0.071\\ 0.400 & 0.347 & 0.153 & 0.100\\ 0.253 & 0.253 & 0.340 & 0.154\\ 0.167 & 0.433 & 0.300 & 0.100\end{bmatrix}$$

$R=\omega^T\circ A=[0.191 \quad 0.476 \quad 0.277 \quad 0.056]\circ$

$$\begin{bmatrix}0.333 & 0.419 & 0.177 & 0.071\\ 0.400 & 0.347 & 0.153 & 0.100\\ 0.253 & 0.253 & 0.340 & 0.154\\ 0.167 & 0.433 & 0.300 & 0.100\end{bmatrix}$$

$=[0.191 \quad 0.476 \quad 0.277 \quad 0.056]$

$$\begin{bmatrix}0.400 & 0.433 & 0.340 & 0.154\\ 0.333 & 0.419 & 0.300 & 0.100\\ 0.253 & 0.347 & 0.177 & 0.100\\ 0.167 & 0.253 & 0.153 & 0.071\end{bmatrix}$$

$=[0.314 \quad 0.392 \quad 0.265 \quad 0.109]$

注意到 WOWA 合成中涉及排序操作，因此合成结果通常不再是归一化向量。在本例中 R 的各分量都得到了不同程度的加强。按最大隶属度原则，得到该应用服务系统的风险指数为 High。若指标层也采用普通的平均算子合成，即假定有序平均加权算子的权向量 $w=[0.25 \quad 0.25 \quad 0.25 \quad 0.25]^T$，则有 $R=\omega^T\circ A=p^TA=[0.305 \quad 0.361 \quad 0.230 \quad 0.104]$。按最大隶属度原则，得到该应用服务系统的风险指数仍然为 High，结论一致。这是因为本例中的决策偏好采用的是折衷原则，比较接近 WM 算子，同时也说明基于 WM 合成的普通 FAHP 方法为基于 WOWA 合成的 FAHP 方法的特例。但基于 WOWA 合成的 FAHP 方法赋予评估者根据实际安全策略调整决策偏好的便利，因此更具灵活性和适用性。

结束语 网络安全态势评估属于前沿性研究领域，目前包括在指标体系、决策算法等许多方面的工作仍处于探索阶段。本文将其归结为复杂系统的多属性决策问题，评估实例旨在说明 WOWA-FAHP 方法的特点和有效性，其网络安全态势评估模型与算法比较粗糙，并缺乏对未来一段时间内网络安全状况变化趋势的感知与预测能力。对于复杂多变的网络安全环境，决策者要求得到多种不同的合成权重信息，即需要建立较为丰富的权重信息知识库。随着实验数据和经验知识的不断积累，在本文工作的基础上，正在实现和逐步完善基于可变权概率模糊认知图[12]的安全态势评估系统。该系统能够根据不同的环境条件和指标特性动态调整重要性权因子与关联性权因子，充分利用风险评估、安全审计与攻击关联认知结果，提高多源信息与评估指标的完备性、态势评估的有效性和实时性，并最终实现网络安全态势的持续性实时动态评估，以有效支持入侵响应决策与系统安全管理。

参 考 文 献

[1] 吴亚非，李新友，禄凯. 信息安全风险评估[M]. 北京：清华大学出版社，2007

[2] Siraj A，Vaughn R. A Dynamic Fusion Approach for Security Situation Assessment[A]//Proceedings of the 4th IASTED International Conference on Communication，Network，and Information Security(CNIS 2007)[C]. Berkeley，California，2007：77-82

[3] 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

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

[5] Calvo T，Mesiar R，Yager R R. Quantitative Weights and Aggregation[J]. IEEE Transactions on Fuzzy Systems，2004，12(1)：

62-69

[6] Yager R R. On Ordered Weighted Averaging Aggregation Operators in Multicriteria Decision Making[J]. IEEE Transactions on Systems, Man, and Cybernetics, 1988, 18(1): 183-190

[7] Torra V. The Weighted OWA Operator[J]. International Journal of Intelligent Systems, 1997, 2(12): 153-166

[8] Torra V. Empirical Analysis to Determine Weighted OWA Orness[A]// Proceedings of the 4th International Conference on Information Fusion[C]. Montreal, Canada, 2001: 11-16

[9] Fullér R, Majlender P. An Analytic Approach for Obtaining Maximal Entropy OWA Operator Weights[J]. Fuzzy Sets and Systems, 2001, 124(1): 53-57

[10] Fullér R, Majlender P. On Obtaining Minimal Variability OWA Operator Weights[J]. Fuzzy Sets and Systems, 2003, 136(2): 203-215

[11] Chen J E, Otto K N. Constructing Membership Functions Using Interpolation and Measurement Theory[J]. Fuzzy Sets and Systems, 1995, 73(3): 313-327

[12] 吕镇邦,周利华. 基于有序加权平均算子的概率模糊认知图[J]. 计算机科学, 2008, 35(12)

(上接第 62 页)

LLC 层包格式如表 3 所列。

表 3 LLC 层包格式

2byte	2	1	0-113
目的网络地址	目的节点地址	负载长度指示	负载

LLC 层信息包包括目的网络地址、目的节点地址、负载长度、负载,用于 LLC 与应用层进行数据交互。

LLC 层采用 POLL 轮询机制,node 节点 LLC 层启动一个 Timer 函数,定时向 coordinator 发送 POLL,coordinator 收到 POLL 后,在 MaxWaitTime 内向 node 发送 ACK,建立通信链接,进行数据包传送。当超时没有 ACK 返回时,node 节点 LLC 层重发 POLL 轮询。超过最大次数 MaxPollNum 而没有 ACK 返回时,LLC 层向应用层发送 POLL-FAIL. confirm 指示,应用层进行相应处理。

1.3 底层模块

底层驱动模块主要有 UART 模块、Timer 模块、ADC 模块和 LED 模块等。UART 模块主要是收发不同格式的数据;Timer 模块主要完成任务调度和定时;ADC 模块主要用于传感器采集数据并转化以及信道侦听,ADC 转换完成调用中断。Node433 通信节点设计有红、绿和黄 3 个 LED,用来指示各种状态。

2 实验验证

在由 50 个节点组成的温湿度环境监测网络条件下进行本文协议的有效性和实用性实验验证。节点硬件采用 Atmega128L[5]作为主控芯片,CC1000[6]作为射频收发模块芯片。

网络系统中,设置一个 coordinator 节点,通过 RS232 串口与上位机相连,与各 node 节点组成星型网络。串口调试助手显示 coordinator 收发数据。由数据帧的规定,可判断串口调试助手收发数据正确与否,如图 6 所示。

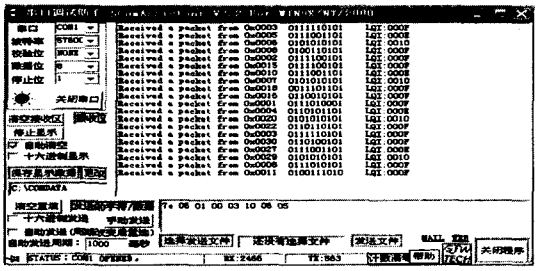

图 6 串口调试助手收发数据

在测试过程中,通过改变发送速率,观看收发效果。当发送速率不高于 10kbps 时,数据收发正确。此速率满足大多数应用需求。各节点采用 POLL 轮询机制,均能先后接入信道。在 2h 时间段内对节点数据收发进行统计,丢包率低于 1% 。

在温湿度监测系统中,node 节点采用 5 号镍氢充电电池供电,初始电量 1500mAH,Atmega128L 工作电压 3.3V,工作频率 8MHz,平均工作电流 10mA[5](包括 ADC 采集模块和温湿度传感器模块)。CC1000 射频收发芯片,频率选为 433MHz 时,接收状态平均电流损耗约 7.4mA,发射状态平均电流损耗约 15mA,睡眠模式(晶振关闭)平均电流损耗约 0.2μA,从睡眠模式唤醒需 5ms[6]。设定数据发送频率 120s 一次(ADC 转换一次数据,输入时钟为 100kHz,射频发送一次数据),对 node 节点进行能耗测算,node 节点可工作 200 天左右。

结束语 本文基于 IEEE802.15.4 协议标准,参照 802.11 MAC 层规范[10,11],设计实现了一种高效、低功耗的无线传感器网络 MAC 协议。网络节点分为 node 和 coordinator,大量的 node 节点通过物理层对无线收发机睡眠管理实现低功耗,极少量的 coordinator 节点射频处于常开状态,实时处理并协调节点消息。实验数据表明,coordinator 和 node 节点构成的系统高效工作,node 节点实现了低功耗。本文协议可用于节点总量不多、通信实时性要求不高的应用系统,如温湿度监测系统等。

参 考 文 献

[1] 孙利民,李建中,陈渝,等. 无线传感器网络[M]. 北京:清华大学出版社, 2005

[2] 李晓维,徐勇军,任丰原. 无线传感器网络技术[M]. 北京:北京理工大学出版社, 2007

[3] Kristofer S, Pister J. Tracking vehicles with a UAV-delivered sensor network[OL]. http://robotics.eecs.berkeley.edu/~pister/29Palms0103/

[4] Butler Z, Corke P, Peterson R, et al. Networked Cows: Virtual Fences for Controlling Cows[C]// Proc. WAMES2004. Boston, USA

[5] Atmega128L DataSheets[OL]. http://www.atmel.com

[6] CC1000 DataSheet[OL]. http://www.chipcn.com/files/CC_1000_DataSheet_2_2.pdf

[7] Ye W, Heidemann J, Estrin D. Medium Access Control with Coordinator Adaptive Sleeping for Wireless Sensor Networking[J]. IEEE /ACM Transactions on Networking, 2004, 12(3): 493-506

[8] IEEE Std 802.15.4[B]-2003. pdf. 142-144

[9] IEEE 802.15.4[B]-2006/2003

[10] Wu Haitao, Cheng Shiduan, Peng Yong. IEEE 802.11 Distributed Coordination Function (DCF) Analysis and Enhancement [J]. IEEE Magazine, 2002

[11] Demirkol I, Ersoy C, Alagoz F. MAC protocols for wireless sensor networks: a survey[J]. Communications Magazine, IEEE, 2006, 44(4): 115-121