基于专家综合评判的叛逆追踪效能评估研究*

韩金森，张龙军，邹　涛
（武警工程大学 信息工程系，西安 710086）

摘　要：针对追踪的效能评估显得尤为必要但至今尚缺，首次系统地通过理论方法结合实例模型，设计了对叛逆追踪效能进行评估的方法。首先实施专家咨询确定对影响叛逆追踪效能的因素分别从有效性、安全性、开销、完善性、应用性等五方面进行分析；然后层次分析确定各项的等级描述并构建叛逆追踪效能评估指标体系；最后综合评判某个叛逆追踪算法的效能。通过实例模型验证了其可操作性和优越性，且谓之专家综合评判。

关键词：专家分析；层次分析；综合评判；叛逆追踪；效能评估
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2012)10-3835-03
doi:10.3969/j.issn.1001-3695.2012.10.061

Research on expert comprehensive evaluation for traitor tracing effectiveness

HAN Jin-sen, ZHANG Long-jun, ZOU Tao
(*Dept. of Information Engineering, Engineering University of CAPF, Xi'an* 710086, *China*)

Abstract: Combining with theoretical method and actual example scientifically, this paper designed an evaluation method of traitor tracing effectiveness grade for the first time. It ascertained to analyze the effectiveness of one traitor tracing scheme from availability, security, overhead, integrity, and applicability by implementing Delphi firstly. Then it made sure their various grade descriptions and set up effectiveness valuation index sign system of traitor tracing by AHP. And finally it synthesized the effectiveness grade of adjudicating the current traitor tracing scheme. The method has been proved its maneuverability and superiority by actual example which is called as expert comprehensive evaluation.

Key words: experts analyze; AHP; comprehensive evaluation; traitor tracing; effectiveness evaluation

信息网络已成为国家和地区各行业各领域关键性基础性设施，各种数字信息、个人隐私信息、数字服务在物联网上传播和应用越来越频繁，其信息安全、权限保障和版权保护问题也越来越受到单位和个人的重视[1]；大量盗版和侵权等问题的出现，严重侵犯了合法使用者和提供商的知识产权。叛逆追踪技术的应用，就能有效地针对网络中的间谍账户窃密、叛逆用户泄密问题，追踪叛逆者，提供证据，撤销使用密钥和权限安全。而层出不穷的叛逆追踪方案[2~8]在某些性能方面各有其优势，但都是描述性地评价某个方案的某项效能如何，不能综合算法的各项指标；如何合理可行地进行综合评判，为叛逆追踪技术的有效应用制定策略提供依据，是尚未解决而需要解决的问题[9~12]。目前现有的评估方法种类繁多，但大部分缺乏对事物事实、逻辑的考虑，可行但可操作性不够，也不曾有学者利用某种理论来对叛逆追踪的效能进行评判。本文以某实际算法为例，首次综合 Delphi 咨询、层次分析和模糊评判等理论[13]，介绍了通过一种实际操作性强的评估方法——专家综合评判，对叛逆追踪算法的效能情况进行综合性的评价。

1　建立叛逆追踪效能评价指标

不同的叛逆追踪算法有其不同的性能指标，而且各个性能指标都有其各自的特点和预设目标，这就需要一种综合性高的指标确定方法。本文根据叛逆追踪算法理论性强、适用性复杂的特点，本着易操作的原则，通过 Delphi 咨询法来确定评估的指标项目[14]。

通过实施 Delphi 咨询，分析得叛逆追踪算法的效能主要由有效性、安全性、开销、完善性和应用性五个方面来衡量。具体指标如下（建立叛逆追踪效能评价指标体系如图 1 所示）：

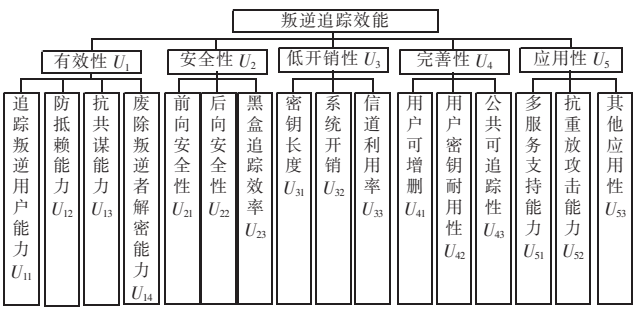

图 1　叛逆追踪效能评价指标体系

a）有效性，指该算法追踪叛逆者、提供叛逆证据、遏制叛逆行为的能力，主要包括防抵赖能力、抗共谋能力、废除叛逆者解密能力等。

b）安全性，指该算法通过语义分析和理论策略分析上满足的安全性能，主要包括前向安全性、后向安全性和黑盒追踪效率等。

c）低开销性，指该算法下所需的计算开销和信道资源占用等，包括密钥长度、系统开销和信道利用率等。

d）完善性，指该算法实现其功能的完善程度，主要包括用户可增加和撤销、用户密钥耐用性和公共可追踪性等。

收稿日期：2012-03-15；**修回日期**：2012-04-25　　**基金项目**：武警工程大学基础研究基金资助项目（WJY201111）

作者简介：韩金森（1988-），男，浙江海宁人，硕士研究生，主要研究方向为信息安全（306874033@qq.com）；张龙军（1964-），男，教授，博士（后），主要研究方向为信息安全；邹涛（1961-），男，副教授，硕士，主要研究方向为无线数据通信.

e)应用性,指该算法对于实际环境的应用性,主要包括多服务支持能力、抗重放攻击能力和其他应用性。

2 量化叛逆追踪效能指标权重

建立效能指标体系后,对其进行层次分析[15],结合由 Delphi 法得到的效能指标,量化各层次各指标的评估值,计算出权重向量;然后根据模糊综合评判思想,结合各指标的权重求出叛逆追踪算法的效能。

2.1 权重量化方法

a)量化评判矩阵 A。

按照已得的指标体系,应用 1 ~ 9 比例标度方法[16],按层量化各指标。

b)归一化 A 的列 $w_{ij}=a_{ij}/\sum_{i=1}^{n}a_{ij}$。

c)按行对 w_{ij} 求和,得 $w_{ij}=\sum_{j=1}^{n}w_{ij}$。

d)归一化 $w_i=w_i/\sum_{i=1}^{n}w_i$,得近似特征向量 $w=(w_1,w_2,\cdots,w_n)^{\mathrm{T}}$。

e)计算最大特征值 $\lambda_{\max}\approx\frac{1}{n}\sum_{i=1}^{n}\frac{(Aw)_i}{w_i}$。

以上已完成了指标权重量化的过程,但为了使计算所得数据的可靠性和可操作性更强、更具说服力,还需继续对所计算得到的矩阵作进一步的检验,其方法很传统,易操作。

f)利用 e)中所得数据求得随机一致性 $CI=\frac{\lambda_{\max}-n}{n-1}$。

g)查表 1 得相应阶数的平均随机一致性指标值 RI。

表 1 平均随机一致性指标

n	1	2	3	4	5	6	7	8
RI	0	0	0.52	0.89	1.12	1.26	1.36	1.41

h)计算随机比例系数 $CR=CI/RI$。

i)评判 CR 是否小于 0.1(偏差容忍范围)。若 $CR\leqslant 0.1$,则数据可用;反之则数据不可用,必须重新调整初始数据再进行,直至满足 $CR\leqslant 0.1$。

2.2 计算各层矩阵

根据上述方法,按层求得关于叛逆追踪效能的评判矩阵,如表 2 ~ 7 所示。

表 2 评判矩阵 A_U 及一级指标权重 w

A_U	U_1	U_2	U_3	U_4	U_5	w
U_1	1	2	3	5	4	0.438
U_2	1/2	1	2	4	3	0.245
U_3	1/3	1/2	1	3	2	0.146
U_4	1/5	1/4	1/3	1	1/2	0.067
U_5	1/4	1/3	1/2	2	1	0.095

表 3 评判矩阵 A_{U_1} 及二级指标权重 w_1

A_{U_1}	U_{11}	U_{12}	U_{13}	U_{14}	w_1
U_{11}	1	4	2	3	0.480
U_{12}	1/4	1	1/3	1/2	0.100
U_{13}	1/2	3	1	2	0.261
U_{14}	1/3	2	1/2	1	0.154

表 4 评判矩阵 A_{U_2} 及二级指标权重 w_2

A_{U_2}	U_{21}	U_{22}	U_{23}	w_2
U_{21}	1	3	2	0.545
U_{22}	1/3	1	1/2	0.167
U_{23}	1/2	2	1	0.286

表 5 评判矩阵 A_{U_3} 及二级指标权重 w_3

A_{U_3}	U_{31}	U_{32}	U_{33}	w_3
U_{31}	1	1/3	2	0.222
U_{32}	3	1	5	0.652
U_{33}	1/2	1/5	1	0.125

表 6 评判矩阵 A_{U_4} 及二级指标权重 w_4

A_{U_4}	U_{41}	U_{42}	U_{43}	w_4
U_{41}	1	3	2	0.545
U_{42}	1/3	1	1/2	0.167
U_{43}	1/2	2	1	0.286

表 7 评判矩阵 A_{U_5} 及二级指标权重 w_5

A_{U_5}	U_{51}	U_{52}	U_{53}	w_5
U_{51}	1	1/4	1/2	0.143
U_{52}	4	1	3	0.632
U_{53}	2	1/3	1	0.222

计算可得随机比例系数 $CR\leqslant 0.1$,属于偏差范围之内,数据可用。

3 叛逆追踪效能的专家综合评判

3.1 拟定因素指标

叛逆追踪算法效能 U 按照图 1 所确定的体系方法,可表示为 $U=\{U_1,U_2,\cdots,U_5\}$,且 $U_i\cap U_j=\varnothing(i\neq j)$。

任意 $U_i(i=1,2,\cdots,5)$ 均有 $U_{ik}(i=1,2,\cdots,5;k=1,2,\cdots,n_i,n_i$ 为 U_i 下的因素的个数),即 $U_1=\{U_{11},U_{12},U_{13},U_{14}\}$,$U_2=\{U_{21},U_{22},U_{23}\}$,$U_3=\{U_{31},U_{32},U_{33}\}$,$U_4=\{U_{41},U_{42},U_{43}\}$,$U_5=\{U_{51},U_{52},U_{53}\}$,且 $U_{ik}\cap U_{i1}=\varnothing(k\neq 1)$。

3.2 一级评价实施

依次对 U_{ik} 实施量化评价。为了得到操作性强且符合实际的数据,一般建立 P 等评价级 $V=\{V_1,V_2,\cdots,V_p\}$。本文以 7 级评价为例,$V=\{V_1,V_2,\cdots,V_7\}=\{$很差,差,较差,一般,较好,好,很好$\}$。

综合运用专家法,对每个 $U_{ik}(i=1,2,\cdots,5;k=1,2,\cdots,n_i,n_i$ 为 U_i 下的因素的个数)进行评判,得到 $r_{ik,j}$。以八位专家为例,先由专家们各自对每个指标单独评判,假如有五位专家对指标 U_{ik} 评判为一般,则相应的 $r_{ik,3}=5/8$。依此类推,可得所有指标 U_i 的专家综合评判矩阵 $R_i=(r_{ik,j})_{n\times 7}(i=1,2,\cdots,5;k=1,2,\cdots,n_i;j=1,2,\cdots,7)$,进而可以得到首级评判的向量 $B_i=w_i\cdot R_i$。

鉴于叛逆追踪算法的理论和实际应用环境比较复杂,涉及因素多,本文留用 20 位专家席位实施专家综合评判的方法,具体评价结果如表 8 所示。

表 8 评价表

指标	很差	差	较差	一般	较好	好	很好
追踪叛逆用户能力	0	0	0	2	7	8	3
防抵赖能力	0	0	2	9	8	1	0
抗共谋能力	0	0	3	7	8	2	0
废除叛逆者解密能力	0	1	3	6	9	1	0
前向安全性	0	0	1	2	10	7	0
后向安全性	0	0	0	3	7	9	1
黑盒追踪效率	0	0	0	1	10	7	2
开销包括密钥长度	0	1	2	9	8	0	0
系统开销	1	1	8	7	3	0	0
信道利用率	0	2	9	8	1	0	0
用户可增加和撤销	0	0	1	1	10	6	2
用户密钥耐用性	0	0	0	6	9	5	0
公共可追踪性	1	1	3	10	5	0	0
多服务支持能力	1	5	7	7	0	0	0
抗重放攻击能力	0	0	2	10	8	0	0
其他应用性	1	1	3	9	6	0	0

所以:

$$R_1=\begin{pmatrix}0 & 0 & 0 & 0.1 & 0.35 & 0.4 & 0.15\\ 0 & 0 & 0.1 & 0.45 & 0.4 & 0.05 & 0\\ 0 & 0 & 0.15 & 0.35 & 0.4 & 0.1 & 0\\ 0 & 0.05 & 0.15 & 0.3 & 0.45 & 0.05 & 0\end{pmatrix}$$

$$R_2=\begin{pmatrix}0 & 0 & 0.05 & 0.1 & 0.5 & 0.35 & 0\\ 0 & 0 & 0 & 0.15 & 0.35 & 0.45 & 0.05\\ 0 & 0 & 0 & 0.05 & 0.5 & 0.35 & 0.1\end{pmatrix}$$

$$R_3=\begin{pmatrix}0 & 0.05 & 0.1 & 0.45 & 0.4 & 0 & 0\\ 0.05 & 0.05 & 0.4 & 0.35 & 0.15 & 0 & 0\\ 0 & 0.1 & 0.45 & 0.4 & 0.05 & 0 & 0\end{pmatrix}$$

$$R_4=\begin{pmatrix}0 & 0 & 0.05 & 0.05 & 0.5 & 0.3 & 0.1\\ 0 & 0 & 0 & 0.3 & 0.45 & 0.25 & 0\\ 0.05 & 0.05 & 0.15 & 0.5 & 0.25 & 0 & 0\end{pmatrix}$$

$$R_5=\begin{pmatrix}0.05 & 0.25 & 0.35 & 0.35 & 0 & 0 & 0\\ 0 & 0 & 0.1 & 0.5 & 0.4 & 0 & 0\\ 0.05 & 0.05 & 0.15 & 0.45 & 0.3 & 0 & 0\end{pmatrix}$$

进一步计算首级综合评判:

$$B_1=w_1\cdot R_1=(0\quad 0.0077\quad 0.0723\quad 0.2306\quad 0.3817\quad 0.2308\quad 0.072)$$

$$B_2=w_2\cdot R_2=(0\quad 0\quad 0.0273\quad 0.0939\quad 0.474\quad 0.366\quad 0.037)$$

$$B_3=w_3\cdot R_3=(0.0326\quad 0.0562\quad 0.3393\quad 0.3781\quad 0.1929\quad 0\quad 0)$$

$$B_4=w_4\cdot R_4=(0.0143\quad 0.0143\quad 0.0702\quad 0.2204\quad 0.4192\quad 0.2053\quad 0.0545)$$

$$B_5=w_5\cdot R_5=(0.0183\quad 0.0469\quad 0.1466\quad 0.466\quad 0.3194\quad 0\quad 0)$$

3.3　二级评价实施

按照同样的方法,记 B_i 为 U 的专家评判向量,可以计算得:评判矩阵 $R_U=(B_1,B_2,\cdots,B_5)^{\mathrm{T}}$;$U_i$ 权重 $w=(w_1,w_2,\cdots,w_5)$,$\sum_{i=1}^{5}w_i=1$。则 $B_{二级}=wR=(b_1,b_2,\cdots,b_7)$。其中:

$$R=(B_1,B_2,\cdots,B_5)^{\mathrm{T}}=$$

$$\begin{pmatrix}0 & 0.0077 & 0.0723 & 0.2306 & 0.3817 & 0.2308 & 0.072\\ 0 & 0 & 0.0273 & 0.0939 & 0.474 & 0.366 & 0.037\\ 0.0326 & 0.0562 & 0.3393 & 0.3781 & 0.1929 & 0 & 0\\ 0.0143 & 0.0143 & 0.0702 & 0.2204 & 0.4192 & 0.2053 & 0.0545\\ 0.0183 & 0.0469 & 0.1466 & 0.466 & 0.3194 & 0 & 0\end{pmatrix}$$

从而可得到:

$$B=w\cdot R=(0.0075\quad 0.017\quad 0.1065\quad 0.2382\quad 0.3699\quad 0.2045\quad 0.0443)$$

按照既定的评价方法可得,第 5 级(较好)的评价系数最高(为 0.369 9),所以该叛逆追踪算法的效能评价为较好。

4　结束语

本文结合专家咨询法、模糊综合评估法、层次分析法等理论的思想,多方面地综合叛逆追踪算法的各项技术指标,结合实际的模型,介绍了一种集多种方法所长的综合性方法,暂且叫做专家综合法。之前的学者对于叛逆追踪方案的评价都局限于某个方面,未曾有过综合性的应用理论方法来评价。通过本文的研究,首次采用科学的理论和方法来综合性地评价叛逆追踪算法的效能:按照专家咨询的意见逐步建立影响信息系统安全的因素体系,涉及面全、贴合实际、考虑全面;借助层次分析法的精髓,化难为易,层层剖析,按权分配;量化指标进行模糊综合评价,科学合理,得出结论也贴合实际的反应。不足之处在于:专家综合法的精确度依赖于专家的专业水平,可以通过增加专家数或者增加专家来源来提高。

参考文献:

[1] 王甲生, 付钰, 吴晓平. 基于改进 FAHP 法的信息系统安全风险评估[J]. 火力与指挥控制, 2011,36(4):33-36.

[2] NAOR D, NAOR M, LOTSPIECH J B. Revocation and tracing schemes for stateless receiver[C]//Proc of the 21st Annual International Conference on Advances in Cryptotogy. London: Springer-Verlag,2001:41-62.

[3] 杨岚,李乔良,周波清,等. 基于群的公钥叛逆者追踪方案[J]. 计算机工程, 2011,37(4):161-162.

[4] BONEH D,GENTRY C,WATERS B. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]//Proc of the 25th Annual International Conference on Advances in Cryptology. Berlin: Springer-Verlag,2005:258-275.

[5] 齐亚莉,徐秀花. 基于广播加密的对称叛逆者追踪方案分析[J]. 北京印刷学院学报,2011,19(4):46-50.

[6] 张学军,曾志强,周利华. 一种新的基于大数分解困难问题的叛逆者追踪方案[J]. 计算机科学,2006,33(7):131-133.

[7] 吕锡香,张卫东,杨文峰. 基于双线性映射的非对称公钥叛逆者追踪[J]. 计算机工程,2009,35(3):4-6.

[8] 冯慧娟,马华,杨波. 一种新的基于 RSA 加密算法的叛逆者追踪方案[J]. 计算机应用研究,2007,24(5):135-136.

[9] 张多林,刘胜,吴智辉. 基于模糊综合评判的防空信息战效能评估[J]. 空军工程大学学报:自然科学版,2003,4(5):75-77.

[10] MON Don-lin,CHENG C H,LIN J C. Evaluating weapon system using fuzzy analytic hierarchy process based on entropy weight[J]. Fuzzy Sets and Systems,1994,62(2):127-134.

[11] TANG Hong,ZHANG Jie. Study on fuzzy AHP group decision-making method based on set-valued statistics[C]//Proc of the 4th International Conference on Fuzzy Systems and Knowledge Discovery. Washington DC:IEEE Computer Society,2007:689-693.

[12] 陈光. 信息系统信息安全风险管理方法研究[D]. 长沙:国防科学技术大学,2006.

[13] 王菊花,吴晓平. 基于模糊综合评判的舰载通信安全设备效能评估[J]. 舰船科学技术,2009, 31(4):103-106.

[14] 吴晓平,汪玉. 舰船装备系统综合评估的理论与方法[M]. 北京:科学出版社, 2007.

[15] 王莲芬,许树柏. 层次分析法引论[M]. 北京: 中国人民大学出版社,1990.

[16] 费军,余丽华. 基于模糊层次分析法的计算机网络安全评价[J]. 计算机应用与软件, 2011,28(10):120-123.