文章编号:1674-7070(2014)01-0058-05

李杰[1] 谢慧[1] 王甲生[1]

基于知识约简的无线网络脆弱性评价指标体系构建

摘要

针对无线网络脆弱性评价指标体系中影响因素众多、层次结构复杂且指标间存在相关性的问题,提出了一种基于知识约简算法的脆弱性指标体系构建方法.首先,初步建立无线网络脆弱性评价的指标体系,在此基础上构造脆弱性评价决策表;其次,运用知识约简算法对决策表进行简化,其中非核指标的重要性排序采用特征向量法进行确定,该方法以保证评价结果的准确性为前提,较AHP权重判断法更具客观性;最后,将该方法和AHP权重判断法进行了分析比较,说明了其有效性.

关键词

指标体系;决策表;知识约简;特征向量法;无线网络

中图分类号 TP393

文献标志码 A

收稿日期 2012-10-14

资助项目 全军军事学研究生课题(2012JY002-480)

作者简介

李杰,男,硕士生,研究方向为网络对抗.JalyTZ@126.com

谢慧(通信作者),女,副教授,研究方向为网络信息安全.aohanzh2007@163.com

1 海军工程大学 信息安全系,武汉,430033

0 引言

无线网络应用广泛,面临的安全威胁更为复杂.面对动态、复杂的无线网络环境,网络管理者必须借助对无线网络脆弱性的评价来反映当前网络的安全状态,才能准确做出决策[1].在对无线网络进行脆弱性评价时,选择合适的评价指标体系是基础,没有一套科学、可行、可信的指标体系,就无法客观地开展评价工作[2].目前,指标体系的建立方法主要有头脑风暴法、专家会议法、德尔菲法、聚类分析法等,这些方法的应用过程中大都包含各种不确定性、随机性和模糊性,且评价指标的多少、层次的多寡也包含着大量的主观因素.针对上述问题,国内外学者已经进行了一些相关研究,提出了一些指标体系的构建方法.如赵锋等[3]将ANP应用于无线自组织网络,从复杂的网络指标中有效筛选出了典型指标,但仿真结果显示各指标的复相关系数ρ相差不大,且临界值D的选取也缺乏科学依据.刘毅[4]构建了网络舆情预警指标体系,但是各指标之间的联系不紧密,并且有些指标间存在含义交叉,不能全面具体地对网络舆情进行预警.马亚龙等[5]采用极大不相关和权重判断相结合的方法对指标进行简化,有效解决了指标体系过于庞大、评估过程过于复杂的难题.针对无线网络脆弱性评价影响因素众多、层次结构复杂且指标间存在相关性的问题,本文提出了一种基于知识约简算法的脆弱性指标体系构建方法,将粗糙集理论中的决策表[6]应用于无线网络脆弱性指标体系的构建中,在保证评估有效性的基础上,筛选出典型的评价指标,为脆弱性评价提供了基础.

1 基于知识约简的指标体系构建步骤

指标体系的构建是一个从具体到抽象,再到具体的过程.首先通过脑力风暴法和德尔菲法初步建立递阶层次指标体系,具体有效地获得了初步评价指标,在此基础上,依据专家对脆弱性评价的一些权威数据建立属性决策表,并利用知识约简算法,在保证评价效能不变的前提下,删去冗余指标,最终得出科学准确的指标体系.其过程如图1所示.

1.1 初步建立无线网络脆弱性评价的递阶层次结构模型

无线网络攻击手段层出不穷、威胁形式日新月异,其脆弱性评价影响因素也随之增多.综合利用脑力风暴法和德尔菲法,提出课题要

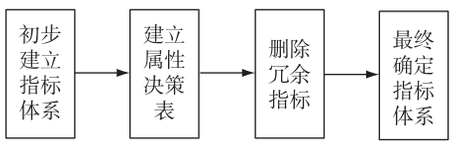

图 1 指标体系构建步骤

Fig. 1 Steps of target system construction

求,请专家对无线网络的脆弱性进行分解,将其分解为由多个元素组成的几部分,再将这些元素按属性分成若干组,形成不同层次,同一层次的元素作为准则层对下一层次的元素起支配作用,同时又受到上一层次元素的支配.最高层是目标层,给出了评价的总体目标;中间两层是准则层和子准则层,给出评价的准则;底层是指标层,即进行脆弱性评价的具体评价指标,表示影响目标实现的各种因素.典型的递阶层次结构模型如图 2 所示.

1.2 建立属性决策表

粗糙集理论中的属性决策表分为条件属性和决策属性 2 大块.将无线局域网准则 B_i 的各评价指标和其对 B_i 的脆弱性评估结果分别作为条件属性和决策属性,各评价指标的等级根据实际状况可分为好、中、差 3 个等级,分别赋值 3、2、1,脆弱性评估结果则划分为很高、高、中、低、很低 5 个等级,分别赋值 5、4、3、2、1.选取该领域专家,对其进行专家评估,得出合理权威的评估结果,并选取一定数量且具有代表性的评估案例作为论域.

选定 P 个评价指标 $R_1,R_2,\cdots,R_p$,N 个具有权威性的评估结果 $x_1,x_2,\cdots,x_n$,以此建立如表 1 所示的无线局域网准则 B_i 的脆弱性评估决策表.

表 1 无线局域网准则 B_i 的脆弱性评估决策

Table 1 Decision table of vulnerability evaluation for B_i in WLAN

论域	条件属性				B_i 的脆弱性
	R_1	R_2	…	R_p	决策属性
x_1	a_{11}	a_{12}	…	a_{1p}	b_1
x_2	a_{21}	a_{22}	…	a_{2p}	b_2
…	…	…	…	…	…
x_n	a_{n1}	a_{n2}	…	a_{np}	b_n

由此可得条件属性矩阵 $\boldsymbol{A}=(a_{ij})_{n\times p}$,决策属性矩阵 $\boldsymbol{B}=(b_1,b_2,\cdots,b_n)^{\mathrm{T}}$.这里 $a_{ij}(i=1,2,\cdots,n,j=1,2,\cdots,p)$ 分别取值 1,2,3,而 $b_i(i=1,2,\cdots,n)$ 取值分别为 1,2,3,4,5.

1.3 知识约简算法[7-8]

粗糙集中的知识约简是指在保持系统决策能力不变的前提下,删除其中不相关或不重要的冗余属性,获得最佳属性.本文在对非核指标的重要性排序时采用特征向量法[9]进行确定,得出指标约简模型.

定义 1 设 U 是论域,R_i 是 U 上的一个等价关系,U/R_i 表示 R_i 的所有等价类(U 上的分类)构成的集合.

定义 2 令 R 和 D 是论域 U 中的等价关系,R 相对于 D 的关系称为 D 的 R 正域,记为 $\mathrm{pos}_R(D)$,其中 $\mathrm{pos}_R(D)=\bigcup\limits_{X\in U/D}\underline{RX},\underline{RX}=\bigcup\{Y\in U/R\mid Y\subseteq X\}$.即 U

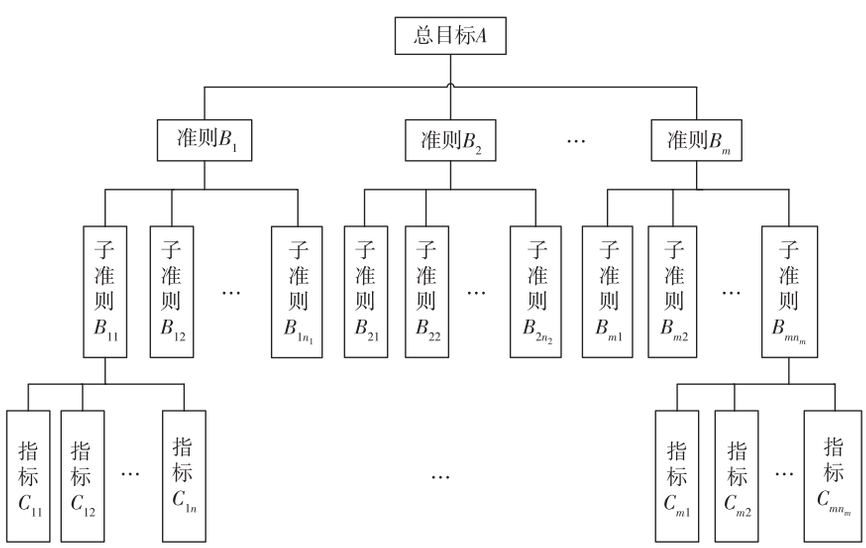

图 2 层次结构模型

Fig. 2 Structure of hierarchical model

中所有根据分类 U/R 的信息可以准确地划分到关系 D 的等价类去的对象集合.

通过 1.2 所建立的属性决策表,令 $U=\{x_1,x_2,\cdots,x_n\}$ 表示论域,评价指标 R_i 是 U 上的一个等价关系,决策属性中 B_i 的脆弱性为论域 U 中的另一个等价关系 D,则可建立指标约简模型[6].

2 无线网络脆弱性评价指标体系的构建

2.1 知识约简:特征向量法指标约简的计算

首先通过脑力风暴法和德尔菲法初步建立递阶层次指标体系.其中,脆弱性的评价主要从技术和管理两个方面进行分类[9],涉及物理层、网络层、系统层、应用层、管理层等各个层面的安全问题.在技术方面主要通过远程和本地两种方式进行系统扫描、对无线网络设备和主机等进行人工抽查,以保证技术脆弱性评价的全面性和有效性;管理脆弱性评价方面可以参照 BS7799 等标准[10]的安全管理要求对现有的安全管理制度及执行情况进行检查,发现其中的管理漏洞和不足.图 3 给出了初步的无线网络脆弱性评价指标体系.

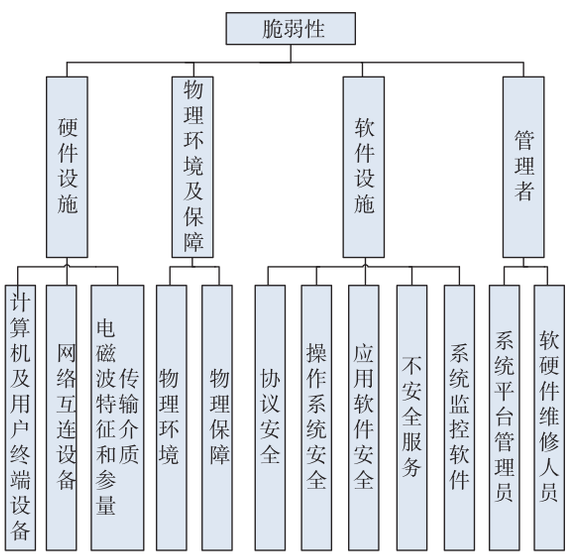

图 3 初步无线网络脆弱性评价指标体系

Fig. 3 Primary target system of vulnerability evaluation in WLAN

图 3 中,对于子准则下的各指标还可进一步细化列出:

1) 计算机及用户终端设备指标包括天线性能情况、无线打印和 PDA 等无线终端设备性能情况;

2) 网络互连设备指标包括 AP 连接情况和有线设备连接情况;

3) 传输介质、电磁波特征和参量指标包括 5G/2.4G 工作频段使用情况、对障碍物的穿透能力和天气影响;

4) 物理环境指标包括有线网络的拓扑情况及无线网络的覆盖范围情况;

5) 物理保障指标包括厂家之间的兼容性情况、无线网络系统物理管理制度的制定情况以及无线网络安全策略制定情况;

6) 协议安全指标包括密钥管理协议(安全信道)安全情况,加密算法鲁棒性,WEP、WPA 漏洞利用情况,各种协议漏洞(如 TCP/IP 协议等)利用情况;

7) 操作系统安全指标包括软件压缩资料库的漏洞(Linux)利用情况、Windows 操作系统漏洞利用情况;

8) 应用软件安全指标包括软件更新情况和网卡驱动更新情况;

9) 不安全服务指标包括复杂的认证情况及端口漏洞利用情况;

10) 系统监控软件指标包括蜜罐性能情况、防火墙更新情况和 IDS(入侵检测系统)性能情况;

11) 系统平台管理员指标包括非授权访问情况,用户以设置无线网卡为 P2P 与外部员工联系情况,密码、SSID 安全情况,SSID 广播情况,DHCP 开放情况,纪律、管理意识,责任心;

12) 软硬件维修人员指标包括思想纪律及技术情况.

以子准则 B_{35} 系统监控软件为例,选取该领域专家,对其进行专家评估,得出合理权威的评估结果,并选取一定数量且具有代表性的评估案例作为论域.建立条件属性矩阵 $\boldsymbol{A}=(a_{ij})_{6\times3}$,其中指标 R_1 为蜜罐,指标 R_2 为防火墙更新,指标 R_3 为 IDS 性能.决策属性矩阵 $\boldsymbol{B}=(b_1,b_2,\cdots,b_6)^{\mathrm{T}}$,如下所示:

$$\boldsymbol{A}=\begin{bmatrix}1&2&1\\3&3&2\\1&2&3\\2&1&3\\1&1&2\\3&2&1\end{bmatrix},\boldsymbol{B}=(1\quad4\quad2\quad3\quad2\quad1)^{\mathrm{T}}.$$

利用 1.3 中的算法模型对上述系统监控软件指标决策表进行计算处理,设 $U=\{x_1,x_2,\cdots,x_6\}$,$R=\{R_1,R_2,R_3\}$,R_1 为蜜罐的性能情况,R_2 为防火墙的更新情况,R_3 为 IDS 的性能情况,依据前文的指标约简模型,给出本例中评价指标约简过程:

1) $U/R_1=\{\{x_1,x_3,x_5\},\{x_2,x_6\},\{x_4\}\}$,
$U/R_2=\{\{x_1,x_3,x_6\},\{x_4,x_5\},\{x_2\}\}$,
$U/R_3=\{\{x_1,x_6\},\{x_2,x_5\},\{x_3,x_4\}\}$,
$U/\{R-R_1\}=\{\{x_1,x_6\},\{x_2\},\{x_3\},\{x_4\},\{x_5\}\}$,
$U/\{R-R_2\}=\{\{x_1\},\{x_2\},\{x_3\},\{x_4\},\{x_5\},\{x_6\}\}$,
$U/\{R-R_3\}=\{\{x_1,x_3\},\{x_2\},\{x_4\},\{x_5\},\{x_6\}\}$;

2) 进而知
$U/R=\{\{x_1\},\{x_2\},\{x_3\},\{x_4\},\{x_5\},\{x_6\}\}$,
$U/D=\{\{x_1,x_6\},\{x_3,x_5\},\{x_2\},\{x_4\}\}$;

3) 因为
$\mathrm{pos}_R(D)=\{x_1\}\cup\{x_2\}\cup\{x_3\}\cup\{x_4\}\cup\{x_5\}\cup\{x_6\}=\{x_1,x_2,x_3,x_4,x_5,x_6\}$,
$\mathrm{pos}_{|R-R_1|}(D)=\{x_1\}\cup\{x_2\}\cup\{x_3\}\cup\{x_4\}\cup\{x_5\}\cup\{x_6\}=\{x_1,x_2,x_3,x_4,x_5,x_6\}=\mathrm{pos}_R(D)$,
$\mathrm{pos}_{|R-R_2|}(D)=\{x_1\}\cup\{x_2\}\cup\{x_3\}\cup\{x_4\}\cup\{x_5\}\cup\{x_6\}=\{x_1,x_2,x_3,x_4,x_5,x_6\}=\mathrm{pos}_R(D)$,
知 R_1 与 R_2 都不是 R 中必要的,
$\mathrm{pos}_{|R-R_3|}(D)=\{x_2\}\cup\{x_4\}\cup\{x_5\}\cup\{x_6\}=\{x_2,x_4,x_5,x_6\}\neq\mathrm{pos}_R(D)$,
故 R_3 是 R 中必要的;

4) 由 3) 可得核为 R_3,又 $\mathrm{pos}_{R_3}(D)=\{x_1,x_6\}\neq\mathrm{pos}_R(D)$,所以 R_3 不为 R 的约简;

5) 再利用特征向量法,可得到 R_1,R_2 权重并归一化为(0.75,0.25),将 R_1 加入进核中,$\mathrm{pos}_{|R-R_2|}(D)=\mathrm{pos}_R(D)$,所以(IDS 性能、蜜罐) 是系统监控软件的一个约简;

6) 显然约去(R_1,R_3) 中的非核元素 R_1 不满足约简条件,故(蜜罐、IDS 性能)为系统监控软件的最佳约简,从而可以用“IDS 性能”、“蜜罐性能”这 2 个指标代替系统监控软件的 3 初始个指标.

2.2 评价指标体系的构建

通过 2.1 中对各 3 级指标的决策表的计算,可以得出它们对应各 4 级指标的重要性,从而删除不重要的指标:

1) 物理保障指标去除“厂家之间的兼容性情况”得最佳约简;

2) 协议安全指标去除“加密算法鲁棒性”,“WEP、WPA 漏洞利用情况”得最佳约简;

3) 系统监控软件指标去除“防火墙更新情况”得最佳约简;

4) 系统平台管理员指标去除“密码、SSID 安全情况”,“SSID 广播情况”,“DHCP 开放情况”得最佳约简.

其余指标均为最佳约简,不需删减指标.

2.3 与 AHP 权重判断法的比较

在优化、约简指标的问题上,也可以运用 AHP 权重判断法来进行指标删减.指标的权重是指标在决策问题中相对重要程度的一种主观评估和客观反映的综合度量,因此可以根据指标权重的大小决定指标的取舍,去除权数很小的指标.下面就以系统监控软件为例,选取专家对 R_1,R_2,R_3 构造判断矩阵 $\boldsymbol{A}=(a_{ij})_{3\times3}$,然后计算特征向量与特征值,最后再进行一致性的检验,从而得到 R_1,R_2,R_3 权重并归一化为(0.273,0.091,0.636).

设取舍权重为 λ_k,$\lambda_k\in[0,1]$,当指标权重大于 λ_k 时,则保留该指标,当指标权重小于或等于 λ_k 时,则筛选掉该指标.一般地,取舍权数取 0.1 较合适,指标权重小于等于 0.1 时可认为该指标影响较小,不足以考虑.也就是认为当其中一个指标的权重比其他小 1 个数量级时,应当剔除掉.当然研究者为了简化问题,对其取舍权重取大,或者根据问题的需要 λ_k 取小一些,都是可行的.这里取 $\lambda_k=0.1$,则删除指标 R_2,与前文约简的结果相符.但是,如若指标较多,且最后权重结果相差不大,则 λ_k 将难以选择,故而指标删除存在一定主观性,不能保证评估效能没有改变,不能达到科学、准确地构建指标体系的要求. 而知识约简方法通过权威的数据进行科学计算,所得约简结果主观性不强,能够科学全面地反映无线网络的脆弱性.

3 总结

评价指标体系不是所有相关指标的罗列,而应抓住重要性指标,抓住能反映本质特性的指标.本文针对无线网络复杂冗余的指标,采用对粗糙集中决策表的知识约简算法进行简化指标的方法,删除冗余指标,保留必要的指标,客观、科学地构建了详实完备的无线局域网脆弱性评价指标体系.最后,通过与 AHP 判断法进行比较,进一步说明本文所使用方法的科学准确.

参考文献

References

[1] 傅建新,黄联芬,姚彦.基于层次分析法-灰色聚类的无线网络安全风险评估方法[J].厦门大学学报:自然科学版,2010,49(5):622-626
FU Jianxin,HUANG Lianfen,YAO Yan.Risk evaluation of wireless network security based on AHP-grey

clustering method[J].Journal of Xiamen University:Natural Science,2010,49(5):622-626
[2] 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,2007:69-74
WU Xiaoping,WANG Yu.Assessment theory and method for warship equipment system [M]. Beijing: Science Press,2007:69-74
[3] 赵锋,郭爱瑄.基于网络层次分析法的无线自组网性能评估指标研究[J].传感技术学报,2011,24(1):111-115
ZHAO Feng,GUO Aihuang.The research of wireless Ad Hoc networks evaluation index system based on ANP[J]. Chinese Journal of Sensors and Actuators,2011,24(1):111-115
[4] 刘毅.基于三角模糊数的网络舆情预警指标体系构建[J].统计与决策,2012(2):11-14
LIU Yi.The early warning system construction for internet public opinion based on triangle fuzzy number [J]. Statistic & Decision,2012(2):11-14
[5] 马亚龙,孙明,朱敏洁.评估指标体系的简化研究与应用[J].火力与指挥控制,2009,34(7):155-157
MA Yalong,SUN Ming,ZHU Minjie.Research and application of the simplification of evaluation index system [J]. Fire Control & Command Control, 2009, 34 (7): 155-157
[6] 苗夺谦,李道国.粗糙集理论、算法与应用[M].北京:清华大学出版社,2008
MIAO Duoqian,LI Daoguo.Theory,arithmetic and application of rough set [M]. Beijing: Tsinghua University Press,2008
[7] Hu F,Fan X H,Yang S X,et al.A novel reduction algorithm based decomposition and merging strategy[J].Lecture Notes in Control and Information Sciences, 2006, 344:790-796
[8] 杨传健,葛浩,汪志圣.基于粗糙集的属性约简方法研究综述[J].计算机应用研究,2012,29(1):16-20
YANG Chuanjian,GE Hao,WANG Zhisheng.Overview of attribute reduction based on rough set [J]. Application Research of Computers,2012,29(1):16-20
[9] 吴晓平,付钰.信息系统安全风险评估理论与方法[M].北京:科学出版社,2011:100-111
WU Xiaoping,FU Yu.Security risk assessment theory and methods for information systems [M]. Beijing: Science Press,2011:100-111
[10] 吴晓平,付钰.信息安全风险评估教程[M].武汉:武汉大学出版社,2011:139-141
WU Xiaoping,FU Yu.The tutorial of information security risk assessment [M]. Wuhan: Wuhan University Press, 2011:139-141

Target system construction of vulnerability evaluation for wireless network based on knowledge reduction

LI Jie[1] XIE Hui[1] WANG Jiasheng[1]
1 Department of Information Security,Naval University of Engineering,Wuhan 430033

Abstract Aspects such as multiple influencing factors,complicated hierarchical structure,and relation between indicators perplexed the vulnerability evaluation target system for wireless network.This paper proposes a method to construct target system of vulnerability evaluation based on knowledge reduction.Firstly,a primary target system of vulnerability evaluation for wireless network is established,hence the decision table of vulnerability evaluation is constructed.Secondly,the knowledge reduction is employed to simplify the decision table,and arithmetic of character vector is used to sort the significance of non-core targets.Premised on high accuracy of evaluation result,this proposed method is more objective than AHP weight judgment method.Finally,this knowledge reduction based method is comparatively analyzed with AHP weight judgment method to validate its feasibility.

Key words targets system;decision table;knowledge reduction;arithmetic of character vector;wireless network