基于数据场的网络安全风险融合模型

傅建明[1,3] 余乔莉[1] 杨 灿[1,2]
(武汉大学计算机学院 武汉 430079)[1] (中国人民解放军 96411 部队 宝鸡 721006)[2]
(武汉大学软件工程国家重点实验室 武汉 430072)[3]

摘 要 针对目前网络安全风险评估中基于全局信息评估策略的不足,建立一种先局部后整体的网络安全风险融合模型。该方法在主机节点模糊评判统计分析的基础上,利用网络全局定位(GNP)实现网络拓扑的坐标化,通过对重要节点以及节点间关联性因子进行加权,然后采用数据场思想实现关联节点的风险融合。通过风险场的构建,该模型能够准确反映风险的融合规律和网络安全风险态势,为管理员提供直观的安全态势视图,方便风险阻断和策略制定。

关键词 风险评估,全局网络定位,风险场,安全态势
中图法分类号 TP393 **文献标识码** A

Network Security Risk Fusion Model Based on Data Field

FU Jian-ming[1,3] YU Qiao-li[1] YANG Can[1,2]
(School of Computer Science, Wuhan University, Wuhan 430079, China)[1]
(Chinese People's Liberation Army 96411 Armies, Baoji 721006, China)[2]
(State Key Lab of Software Engineering, Wuhan University, Wuhan 430072, China)[3]

Abstract As there are shortcomings of current network security risk evaluation based on global information, a new security risk evaluation was presented to describe network security risk fusion on the basis of data field. Based on the fuzzy evaluation and statistical analysis, a new network security risk fusion model in the risk field was implemented using GNP(Global Network Position). Through building the risk field, our experimental results demonstrate that the model could reflect the rule of security risk fusion and the security risk situation correctly, and provide intuitionistic graph for security situation in order to block risk propagation and make security policies.

Keywords Risk evaluation, Global network position, Risk field, Security tendency

1 引言

网络安全风险评估作为制定安全策略的基础,贯穿于整个网络系统生命周期。传统评估方式主要立足于现有模型对网络中个体进行评估,探求网络个体之间相互关联以及风险的叠加影响和融合规律方面。陈秀真等[1]提出采用自下而上、先局部后整体评估策略的层次化安全威胁态势量化评估模型及其相应的计算方法。张永铮[2]提出了网络节点关联性(NNC)的概念,并用于网络风险评估和网络风险传播。李涛[3]教授提出了基于人工免疫系统的网络安全风险定量评估模型,该模型首先根据攻击强度实时计算主机的风险值,然后利用各主机的风险值聚合成网络风险值,并给出了理论分析。这些研究都没有深入研究风险动态传播,或者考虑了利用自动弱点扫描工具[4]等获得弱点,然后实施量化后进行简单的风险累加。这些方法往往忽略了风险的动态传播和风险的反馈、叠加等特性。

考虑到风险评估应与整体环境相结合,本文以风险传播中的网络距离为切入点,以数据场和网络全局定位(NGP)理论为指导,把高维的网络数据映射到数据场,在对主机脆弱性和威胁性评估的基础上,构建网络安全风险场,研究场空间下数据的采集和风险融合机制。其特点是既考虑了网络的拓扑结构,又把目标网络作为一个整体,从全局角度看待风险评估,为网络安全风险评估提供了一种新的思路。

2 风险场和网络安全风险融合模型

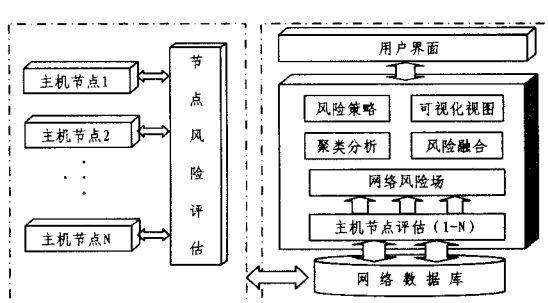

图1 网络安全风险评估实验系统体系图

根据风险评估的实际需求,从评估角度,实验主要由节点

到稿日期:2008-06-24 本文受863国家重点基金项目(2007AA01Z411),国家自然科学基金(90718005)资助。
傅建明(1969-),男,博士,副教授,主要研究方向为网络安全和软件行为,E-mail:jmfu@whu.edu.cn;余乔莉(1986-),女,硕士生,主要研究方向为网络安全与可信软件;杨 灿(1978-),男,硕士生,主要研究为网络安全与风险评估。

评估以及风险融合两个模块组成(如图 1 所示),其中数据采集和主机评估属于节点风险评估范畴,本实验主要采用模糊数学评判方法来实现。风险融合模块主要利用 GNP(全局网络定位)方法[7,13]对各个主机节点实施网络空间坐标化,从而构成网络空间风险场。通过场运算,利用各主机提供的网络风险值和网络拓扑可以绘制出风险场的可视化态势图。

2.1 主机节点模糊评估

现有的评估方法通常使用一个简单的数字指标作为分界线,界限两边是截然不同的两个级别。同时,因为风险要素的赋值是离散的、非连续的,所以对于风险要素的确定和评估本身也有很大的主观性和不精确性。模糊综合评价[10]是以模糊数学为基础,采用模糊数学方法对风险评估进行研究和分析,能较好地解决评估的模糊性。

运用隶属度来刻画风险评估中的模糊界限,而隶属度可用隶属函数来表达。为了确定模糊运算,需要为每一个评估因子确定一种隶属函数。如漏洞隶属函数可以定义为:当漏洞级别为 30 时,漏洞隶属二级风险级别的程度为 10%,隶属三级风险级别的程度为 80%,隶属四级风险级别的程度为 10%。资产因子和威胁因子也可以根据评估对象定义。

对各单项指标(评估因素)分别进行评价。可取 U 为各单项指标的集合,$U=\{$资产,漏洞,威胁$\}$;V 为风险级别的集合,$V=\{$低,较低,中,较高,高$\}$。对 U 上的每个单项指标 U_{ij},通过各自的隶属函数分别求出其对于评价集 V 上 5 个风险级别的隶属度。例如,漏洞因子 U_{ij} 的评估值为 T,就可以分别求出属于各个风险级别的隶属度,得出一组 5 个数$\{0,0,0.1,0.8,0.1\}$。同样其余资产、威胁因子也可以得出一组数,组成一个模糊矩阵 3 * 5,记为关系模糊矩阵 R_{ij}。

一般来说,风险级别比较高的因子对于综合风险的影响也是比较大的。换句话说,高的综合风险往往来自于那些高风险级别的因子,因此各单项指标中那些风险级别比较高的因子应该得到更大的重视,即权重也应该较大。设每个单项指标的权重值为 β_i,得到一个模糊矩阵,记为权重模糊矩阵 B,$B=\{\beta_1,\beta_2,\beta_3\}$。

进行单项评价并配以权重后,可以得到两个模糊矩阵,即关系模糊矩阵 R 和权重模糊矩阵 B,则模糊综合评价模型为 $Y=B*R$,$Y=\{y_1\ y_2\ y_3\ y_4\ y_5\}$代表最后的综合评估结果隶属于第 i 个风险级别的程度。这样,最后的模糊评估形式的量化值为 $P_i=1*y_1+2*y_2+3*y_3+4*y_4+5*y_5$,作为一个最终的数值结果。

本实验涉及评估节点 50 个,根据资产评估、威胁评估和脆弱性评估的结果,导入评价模型中,进行模糊算法综合评估,最后根据等级库和综合评估结果生成风险报告。

主机风险值表如表 1 所列。

表 1 主机风险值表

编号	GNP 空间坐标		节点值
	x	y	
…	…	…	…
10	180	13	33.4
11	156	122	69.9
12	106	118	83.2
13	120	102	32.8
14	170	140	15.2
…	…	…	…

2.2 风险场环境构建

通过风险场来展现网络拓扑中节点风险融合规律,可以分为以下 3 个方面:

(1)确定数据对象。把复杂网络拓扑看成一个数据集合,按照节点之间的空间点映射为一个数据对象。

(2)确定场分布。根据 GNP 思想计算网络空间节点的网络坐标,按照节点之间的空间位置、分布位置确定节点之间的场空间位置。

(3)确定势函数及其表达式。利用数据场公式和等势线算法,便可以得到与该网路拓扑结构相对应的数据场视图。

根据 GNP 思想将实验网络系统抽象成为一个风险网络坐标空间(如图 2 所示),其中纵、横坐标表示评估节点在风险场空间的坐标位置。通过高维的网络数据映射到风险场,在描述风险场的特性时,引入标量函数——势函数来计算单个节点对场中其他节点的影响。因此风险场空间每一个节点都会对场中任何一个点的势值有贡献,且贡献的大小与距离的平方成反比。

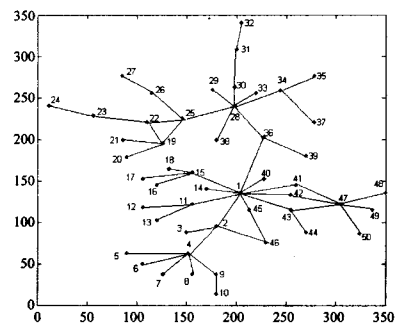

图 2 实验网络坐标空间

事实上,风险节点利用网络路径进行风险攻击和传播牵涉到多方面的因素,考虑到网络中节点的风险传递的强度不但与节点空间位置有关,而且与网络的传播路径、风险类型、节点的抗风险强度息息相关,所以传播概率也是不同的。为了突出本文的实验效果,必须考虑到风险传递概率,这样对给定 n 个数据节点,$D=\{d_1,d_2,\cdots,d_n\}$ 在 X 上的势函数被改进为

$$f(x)=\sum_{i=1}^{n}p_i m_i e^{-\frac{d^2(x,d_i)}{2\sigma^2}} \tag{1}$$

其中,m_i 为该点 d_i 质量大小。由于本文研究是以主机节点为单元研究风险的传播规律,故拟用节点的风险值表示节点的质量。一般而言,单个节点风险值越大,它在网络中的辐射面越广,传播性越强,向外传播的概率就越高。风险值越大的节点,它在风险场的影响力也就越大,在网络空间就越"重要"。而风险越低的节点,则认为该节点抵抗风险能力就越强,被感染的概率就越低。而 p_i 为节点间关联性因子,与实际传播路径有关,主要描述风险传递的可能性。$d(x,d_i)$为节点 d_i 与对象 x 间的距离,σ 为辐射因子。通过多次迭代和相互作用,就可以计算出风险场中各节点的势。势越大的点,其风险越高。

为了验证实验效果,以一个有 50 个节点和 56 条边组成的网络拓扑[11]为例,通过全局网络定位获取网络中每个节点的网络坐标。在节点评估的基础上,利用改进后的风险场势函数计算网络空间节点的融合效果。

融合算法如下:

```
输入:m[n]  //主机节点 n 风险值
      p[n][n]  //节点间的风险传播概率
      x[n],y[n]  //节点 n 的坐标空间位置
输出:z[i,j]空间位置的风险势值
s=2 * σ^2;
For(int i=0;i<=L;i++)  // L 为空间分布长度
{
  For (int j=0;j<=W;j++)  // W 为空间分布宽度
  {
    z[i][j]=0;
    For (int k=1;k<=n;k++)
  {
      z[i][j]= z[i][j]+ p[i][j] * m(k) *
      exp(-abs(sqr(i-x [k])+sqr(j-y [k]))/ s);
    }
  }
}
```

通过对风险网络在某个时间 $T1$ 的数据进行采样，得到场空间中前 20 个节点的风险融合数据，运算得出等势平面图和三维效果(如图 3 和图 4 所示)，其中红、黄颜色表示风险程度的高低处于危险和警戒状态，从中可以直观寻找出最具威胁的节点和安全节点。

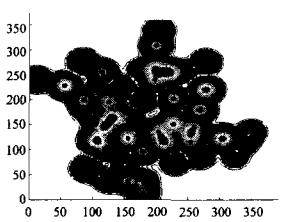

图 3　网络风险场平面图($T=T1,\sigma=10.24$)

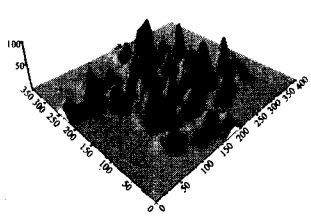

图 4　网络风险场三维图

2.3　风险的转移和阻断

由于网络的传播特性，病毒或者恶意代码能够利用节点漏洞或者缺陷实施风险传播，而这种风险传递通过不同时间的观测可以利用风险场实时显示。当风险经过一段时间传播到 $T2$ 时刻时，分别对 $T1$ 和 $T2$ 时刻的网络风险进行实施监控并比对(如表 2 所列)，从而展现网络风险的动态变化和传播趋势。图 5 显示出了网络中的风险转移后的风险视图。倘若在 $T3$ 时刻对风险源实施阻断，或者根据风险特征实施网络加固，则可以降低网络总风险。图 6 显示出了对网络实施风险阻断之后的风险视图，明显看出高风险源被抑制。

表 2　不同时刻风险融合数据表

节点编号	网络位置		T1 时刻	T2 时刻	T3 时刻
	X	Y			
1	204	135	70.174	70.174	65.128
2	180	95	41.236	41.241	41.199
3	150	88	21.854	23.339	22.948
4	152	62	12.871	50.495	40.495
5	90	62	25.263	25.263	25.263
6	106	50	10.491	10.492	10.492
7	126	37	17.033	17	16.98
8	156	37	40.529	34.317	33.846
9	180	37	26.312	25.845	25.833
10	180	13	34.95	34.917	34.917
11	156	122	71.382	71.402	71.392
12	106	118	88.027	88.027	37.419
13	120	102	42.584	42.584	36.784
14	170	140	23.134	24.289	24.285
15	156	160	37.578	57.378	54.371
16	120	145	92.553	92.567	37.46
17	106	152	39.318	39.318	22.569
18	132	164	90.017	91.194	36.695
19	126	195	63.195	63.556	63.145
20	90	178	17.677	17.677	17.669

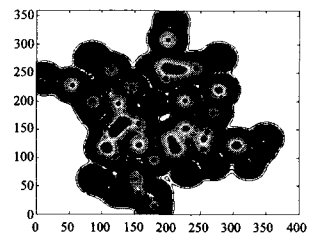

图 5　风险转移图($T=T2,\sigma=10.24$)

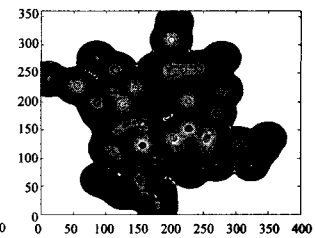

图 6　阻断后风险图($T=T3,\sigma=10.24$)

3　数据分析

3.1　融合风险呈上扬趋势

多次实验通过对不同时刻网络主机进行节点评估，并利用风险融合模型进行风险融合，得到风险融合后的结果(如表 3 所列)。其中，节点编号表示风险场空间中各个网络节点，节点的坐标与表 2 中编号相同的节点的坐标一致，场前场后数据代表了风险融合前的节点模糊评判结果和融合后的节点风险值。

表 3　节点风险对比

节点	实验一			实验二		
编号	场前	场后	增幅	场前	场后	增幅
1	60.4	70.174	16.2%	64.5	75.456	17.0%
2	40.8	41.236	1.1%	25.2	26.109	3.92%
3	20.6	21.854	6.1%	31.8	31.85	0.2%
4	10.2	12.871	26.2%	23.2	30.893	33.2%
5	24.4	25.263	3.5%	24.4	25.248	3.5%
6	5.8	10.491	80.9%	62.6	65.633	4.8%
7	16.1	17.033	5.8%	5.7	10.438	83.1%
8	38.3	40.529	5.8%	33.2	36.707	10.6%
9	21.7	26.312	21.3%	32.2	53.285	65.5%
10	33.4	34.95	4.6%	75.4	76.222	1.1%
11	69.9	71.382	2.1%	30	30.253	0.8%
12	83.2	88.027	5.8%	22.8	26.841	17.7%
13	32.8	42.584	29.8%	60.5	77.265	27.7%
14	15.2	23.134	52.2%	16.8	17.69	5.3%
15	31.8	37.58	18.2%	32.2	38.267	18.8%
16	80.5	92.553	15%	70.1	78.367	11.8%
17	12.2	39.318	222.3%	43.2	43.414	0.5%
18	80.1	90.017	12.4%	30.6	33.798	10.5%
19	62.2	78.43	26.1%	60.2	74.58	24.3%
20	12.6	17.677	40.3%	28.3	33.096	16.9%

从表 3 可以看出，每次实验中，各个节点的风险值经过风险场的运算后，总是保持一定上扬的趋势，没有出现抵消甚至自动降低的可能。分析原因表明，风险的融合对单个主机只会增加由于动态传播的影响产生非线性叠加的效果，如果不主动采取阻断措施和风险策略，不会出现风险自动消除的现象。

3.2　骨干节点融合风险增幅较大

网络中节点所处位置不同导致不同的节点在风险融合方面有不同的融合效果。为了挖掘融合规律，如果结合网络拓扑运用数据挖掘知识进行骨干网重要节点挖掘，依据网络的

拓扑特征，如节点度数、节点介数、边介数和聚焦系数等，发现重要节点，并将节点连接重构为新的虚拟骨干网络(如图 7 所示)。取 $N=20$，表示预定的挖掘节点数目及挖掘粒度。

根据实验一、实验二、实验三和实验四的数据，得到节点风险增幅图(如图 8 所示)，其中横坐标是网络节点编号，纵坐标是节点在各个实验中的风险值增幅。

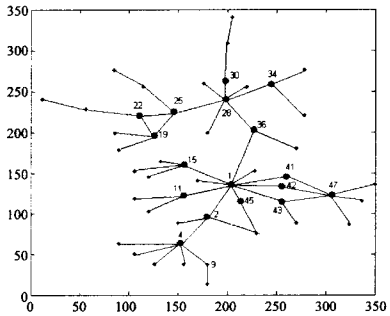

图 7　网络拓扑骨干网图

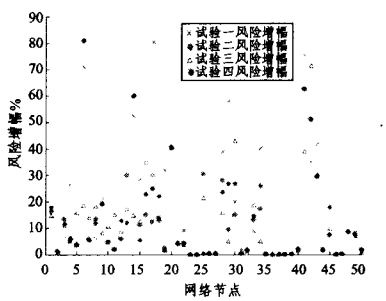

图 8　节点风险增幅图

实验得到各自测验中风险增幅>15%的网络节点占骨干节点的百分比，如表 4 所列。

表 4　风险增幅与骨干节点($N=20$)关系图

实验	增幅大于 15%节点数	属于骨干节点比重(%)
1	19	52.6
2	13	53.8
3	16	56.3
4	14	57.1
5	16	54.3
6	18	60.1
7	14	53.4
8	15	57.2
9	17	58.1
10	16	57.5

根据表 4 不难发现，风险增幅靠前的节点大部分也是网络中的重要骨干节点[11]。换句话说，骨干节点的风险增幅较之场空间其他节点普遍要高。

3.3　网络总风险均值增幅平缓

经研究发现，如果对通过场融合后网络所有节点风险值进行汇总求均值，作为衡量总体风险的一个指标，通过多次实验得出结论，如表 5 所列，网络总风险的增幅保持一定幅度，并且稳定。由此，得到网络中主机节点静态风险值之后，可以根据增幅规律大致得到融合后的网络叠加总量。

表 5　风险场总风险均值增幅

实　验	场前均值	场后均值	增幅(%)
1	40.6	45.4	11.9
2	42.4	47.0	10.8
3	35.8	39.2	9.61
4	35.3	38.9	10.1
5	37.3	41.4	10.9
6	36.1	40.3	11.6
7	41	45.8	11.6
8	45.4	50.9	11.9
9	43.2	48.3	11.8
10	42.0	47.0	11.7

结束语　为了研究评估网络中的风险融合规律，借鉴数据场，提出了网络安全风险场的概念，并用实验阐明了风险场的风险融合机制。与传统的风险评估相比，该模型具有以下特点：(1)利用 GNP 思想建立风险网络，采用模糊评判实现网络节点评估，从全局角度研究风险的融合机制，既考虑个体，又兼顾全局。(2)具备直观的风险态势图，能快捷、便利查找出最具威胁风险源和安全节点，为决策者实施风险阻断和策略制定提供高效依据。(3)通过对风险融合的态势研究，掌握融合的趋势与规律，能使防护策略具有针对性，从而采取主动防御的策略，降低风险的传递速度，使得风险的传播和破坏作用仅局限在有限的范围。如何更准确地描述节点风险和节点之间的关联度，是未来的研究工作之一。

参 考 文 献

[1]　陈秀真，郑庆华，管晓宏，等. 网络化系统安全态势评估的研究[J]. 西安交通大学学报，2004，38(4)：404-407

[2]　张永铮，方滨兴，迟悦，等. 网络风险评估中网络节点关联性的研究[J]. 计算机学报，2007，30(2)：234-240

[3]　Li T. An immunity based network security risk estimation[J]. Science in China Series E-Information Sciences，2005，35(8)：798-816

[4]　Jajodia S，Noel S，O'Berry B. Topological analysis of network attack vulnerability//Kumar V，Srivastava J，Lazarevic A，eds. Managing Cyber Threats：Issues，Approaches and Challenges. Springer-Verlag，2005：248-266

[5]　陈桂生，李德毅. 基于数据场的复杂网络级联失效传播模型[C]//全国复杂网络学术会议. 2006

[6]　李德毅. 不确定性人工智能[M]. 北京：国防工业出版社，2005：195-205

[7]　Ng T S E，Zhang Hui. Predicting Internet Network Distance with Coordinates-Based Approaches[C]//Proceedings of INFOCOM'2002. New York，USA，2002：170-179

[8]　张增斌，陈阳，邓北星，等. 基于邻近原则的 BitTorrent 实验研究[J]. 厦门大学学报：自然科学版，2007，46(2)：213-215

[9]　Shavitt Y，Tankel T. Big-Bang Simulation for embedding network distances in Euclidean space[C]//Proc. of INFOCOM. San Francisco，CA，June 2003

[10]　汪楚娇，蒋志雄，王拓. 基于模糊数学的网络安全风险评估模型[J]. 网络安全技术与应用，2005：22-25

[11]　李德毅，韩明畅，孙岩. 复杂网络与网络安全[J]. 军队指挥自动化，2005

[12]　李德毅，淦文燕，朱熙. 复杂网络中重要性节点发掘综述[J]. 计算机科学，2007，34(12)：1-17

[13]　陈阳，邓北星，李星. 基于坐标的网络节点聚类在 Internet 中的实验研究[J]. 大连理工大学学报，2005，45(21)：41-43