文章编号:1673-9469(2009)02-0086-03

基于SPA的攻击模型BBFPAN双枝集对分析模型

任大勇[1],黄光球[2]
(1.渭南师范学院,陕西 渭南 714000;2.西安建筑科技大学 管理学院,陕西 西安 710055)

摘要:针对以双枝模糊决策和模糊Petri网为基础的攻击模型BBFPAN在描述网络攻击进展情况方面存在的问题,提出了一种BBFPAN双枝集对分析模型。该模型发掘了网络攻击模型BBFPAN中对层次的集对关系,并对这些集对进行了双枝集对分析,用联系度表示攻击模型BBFPAN中因素对网络攻击效果的支持程度,用贴近度表示决策分量与攻击和防御成功相对隶属度的接近程度,同时给出了BBFPAN双枝集对分析的基本步骤,为集对分析理论在攻击模型BBFPAN的推理过程中的应用奠定了基础。

关键词:集对分析;网络安全;攻击建模
中图分类号:TP393.08 **文献标识码**:A

A both-branch set pair analysis model based on set pair analysis to attack model BBFPAN

REN Da-yong[1], HUANG Guang-qiu[2]
(1.Weinan Teachers University, Weinan 714000, China; 2.School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: Attack model BBFPAN based on both-branch fuzzy decision-making and fuzzy Petri net has some drawback such as can not depicting the network attacks pictorially. Based on set pair analysis, a both-branch set pair analysis model is put forward to the attack model BBFPAN. The multilayer set pair of attack model BBFPAN has been discovered in the both-branch set pair analysis model. The relationship between the factors of the attack model BBFPAN and the network attack can be depicted as the connection degree. The relative degree of decision weight successes to attack and defense can be determined through the close-degree. The basic step of both-branch set pair analysis model on attack model BBFPAN is also proposed which can help the attack model reasoning with the Set Pair Analysis.

Key words: set pair analysis; network security; attack modeling

集对分析(Set Pair Analysis, SPA)是我国学者赵克勤于1989年提出的一种关于确定不确定系统同异反定量分析的系统分析方法[1]。自被提出以来已在科学研究与工程技术以及社会、经济、人文等领域得到了广泛的关注和应用。文献[2]运用集对分析理论建立了一个用于评价图书馆服务质量数学模型,并通过该模型对评价体系中各指标进行态势分析,对图书馆服务质量进行综合评价;文献[3]在不完备信息系统中,采用集对分析方法构建了一种基于联系度的二元关系,从而建立了新的基于联系度的粗集模型,使用决策矩阵讨论了不完备系统规则的生成方法;文献[4]将集对分析理论中的3元联系度拓展到5元联系度,综合考虑事物的确定和不确定因素,成功的将其应用于水质富营养化问题的综合评价;文献[5]结合态势评估的常用方法建立了一种综合距离优势、角度威胁因子、速度威胁因子的集对分析的态势评估模型,对在预警机指挥下的多机编队空战态势进行了评估。在集对分析的应用研究中,很少有涉及网络安全方面的相关文献,文献[6]提出了一

收稿日期:2009-02-17
作者简介:任大勇(1981-),男,陕西渭南人,硕士,从事电子商务与网络安全。

种基于节点的不确定性的 P2P 网络信誉度的安全机制,并采用集对分析理论对信誉度进行了定量分析。

我们在文献[7]中,以双枝模糊决策[8-9]和模糊 Petri 网为基础,综合考虑对网络攻击起促进和抑制作用的两种因素,定义了一种新型网络攻击模型 BBFPAN,并提出了一种基于双枝模糊决策理论的 BBFPAN 双枝模糊决策分析模型。但同时,我们也发现该分析模型通过对 BBFPAN 中变迁输入库所集中的影响因素进行双枝模糊决策分析,只能单一的判断变迁输出库所集中库所属性,而无法反映变迁在算法执行的某一轮以及后继轮中的触发情况,进而也就无法反映网络攻击的进展情况。

文献[10]首次将集对分析理论与双枝模糊决策理论相结合,用集对分析的方法研究进行双枝模糊决策的方法,分别对双枝模糊决策因素域和双枝模糊决策的上枝、下枝和双枝进行了集对分析,提供了双枝模糊决策理论研究新的视角和方法。但是在文献[10]中,对于集对分析理论中很多重要参数的确定并不能很好的反应参数本身所代表的含义,同时也没有发掘集对分析理论和双枝模糊集深层次的关系。

本文将首先深入研究集对分析理论和双枝模糊集的关系,探求以双枝模糊集为基础的网络攻击模型 BBFPAN 中多层次的集对关系,首次将集对分析理论应用于攻击模型的分析研究,提出 BBFPAN 本身也是一个确定不确定系统。

1 BBFPAN 中的集对

集对分析理论研究的是由两个集合 A 和 B 所构成的既对立又统一的确定不确定系统,利用两个集合在指定问题背景下的同一度,差异度,对立度刻画了这种确定不确定性关系。而在双枝模糊集中,既存在对特定问题起绝对作用的因素域(U^+和 U^-),也存在着一些比较模糊的因素域(U^*)。

文献[7]定义攻击模型 BBFPAN 为 7 元组模型,其中 $\theta=(\theta_1,\cdots,\theta_n)^T$,$\theta_i$ 是命题 d_i 的逻辑状态,θ_i 为[-1,1]区间的双枝模糊集区间数。若 $\theta_i\in(0,1]$即表示命题 d_i 所对应的因素对网络攻击具有积极促进作用,同时令 $\theta_i\in U^+$;若 $\theta_i\in[-1,0)$则表示命题 d_i 所对应的因素对网络攻击具有消极抑制作用,则可令 $\theta_i\in U^-$;若 $\theta_i=0$ 表示命题 d_i 所对应的因素对网络攻击,既可能具有积极促进作用,又可能具有消极抑制作用,它是网络攻击的中间状态节点,可令 $\theta_i\in U^*$。按照此定义,可以得到如下的攻击模型 BBFPAN 因素关系分解图,如图 1 所示。

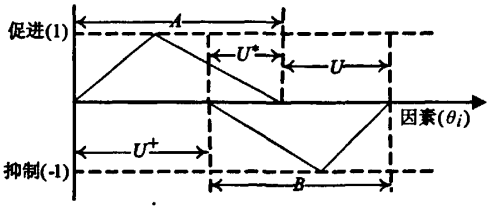

图1 BBFPAN因素关系分解图

Fig. 1 Relation decompose diagram of BBFPAN

图 1 中,因素域 U^+ 和 U^- 中的因素分别对网络攻击起着积极促进作用和消极抑制作用,因素域 U^* 中既存在着对网络攻击起积极促进作用的因素,同时也存在着对网络攻击的起消极抑制作用的因素,并且 U^* 中的因素会随着网络攻击过程的不断演变,而对网络攻击起着完全相反的作用。故而,以双枝模糊集为基础的 BBFPAN 也是一个确定不确定系统,若因素域 U^+ 和 U^* 组成集合 A,因素域 U^- 和 U^* 组成集合 B,则就将 BBFPAN 因素域分解为由集合 A 和 B 所构成的一个集对。

同时,对于由因素域 U^+ 和 U^* 组成的集合 A 中的因素来说,他们对网络攻击所起到的促进作用大小也是不一样的,以致有的因素可以达到相应的效果而有的则不可以,所以这些因素对于网络攻击的最终结果也是既确定又不确定的。依照集对分析理论,可以利用联系度来刻画集合 A 和 B 中因素对网络攻击最终结果的影响程度。

2 双枝集对分析模型

在双枝集对分析模型中,分别对因素域 U^+、U^* 和因素域 U^-、U^* 中的因素进行集对分析,利用同一度分别表示他们对网络攻击和网络防御的支持程度。

2.1 U^+ 和 U^* 上的集对分析模型

按照文献[7]的定义,得到 n 个决策因素关于 m 个决策的攻击相对隶属度矩阵为 $R^+=\{r_{ij}\}_{n\times m}$。

攻击成功的相对隶属度

$$h^+ = (h_1^+, h_2^+, \cdots, h_n^+)^T = (\bigvee_{j=1}^{m} r_{1j}, \bigvee_{j=1}^{m} r_{2j}, \cdots, \bigvee_{j=1}^{m} r_{nj})^T \quad (1)$$

攻击失败的相对隶属度

$$s^+ = (s_1^+, s_2^+, \cdots, s_n^+)^T = (\bigwedge_{j=1}^{m} r_{1j}, \bigwedge_{j=1}^{m} r_{2j}, \cdots, \bigwedge_{j=1}^{m} r_{nj})^T \quad (2)$$

对于决策 j 的向量 $r_j = (r_{1j}, r_{2j}, \cdots, r_{nj})^T$ 来说,攻击成功的相对隶属度 h^+ 和攻击失败的相对隶属度 s^+ 就构成了其比较空间。决策分量 r_{ij} 与攻击成功 h^+ 的状况的接近程度,可以用贴近度[11]表示,即

$$a_{ij}^+ = \frac{\min(h_j^*, r_{ij})}{\max(h_j^+, r_{ij})} = \frac{r_{ij}}{h_j^+} \quad (3)$$

相应的,他与攻击失败 s^+ 的状况的接近程度,也可以用贴近度[11]表示为

$$c_{ij}^+ = \frac{\min(s_j^+, r_{ij})}{\max(s_j^+, r_{ij})} = \frac{s_j^+}{r_{ij}} \quad (4)$$

由(3)、(4)两式可知,$a_{ij}^+, c_{ij}^+ \in [0,1]$,且他们分别表示在数值上 r_{ij} 与 h^+,r_{ij} 与 s^+ 的接近程度。其值越大,这种接近程度越大,而在确定区间 $[s^+, h^+]$ 中,r_{ij} 与 s^+ 的接近程度恰说明了 r_{ij} 与 h^+ 的远离,故可称 a_{ij}^+ 和 c_{ij}^+ 为集对 $\{r_{ij}, h^+\}$ 的同一度和对立度,则根据 $a_{ij}^+ + b_{ij}^+ + c_{ij}^+ = 1$[1]可得

$$b_{ij}^+ = 1 - (a_{ij}^+ + c_{ij}^+) = \frac{h_j^+ r_{ij} - r_{ij}^2 - h_j^+ s_j^+}{h_j^+ r_{ij}} \quad (5)$$

从而得到集对 $\{r_{ij}, h^+\}$ 的联系度为

$$\mu\{r_{ij}, h^+\} = \frac{r_{ij}}{h_j^+} + \frac{h_j^+ r_{ij} - r_{ij}^2 - h_j^+ s_j^+}{h_j^+ r_{ij}} I + \frac{s_j^+}{r_{ij}} j \quad (6)$$

进而可得,在比较空间 $[s^+, h^+]$ 中,集对 $\{r_j, h^+\}$ 的联系度

$$\mu\{r_j, h^+\} = a_j^+ + b_j^+ I + c_j^+ J \quad (7)$$

其中 $a_j^+ = \sum_{j=1}^{n} w_i a_{ij}^+$, $b_j^+ = \sum_{j=1}^{n} w_i b_{ij}^+$, $c_j^+ = \sum_{j=1}^{n} w_i c_{ij}^+$。

2.2 U^- 和 U^* 上的集对分析模型

按照文献[7]的定义,得到 n 个决策因素关于 m 个决策的防御相对隶属度矩阵为 $R^- = \{\overline{r_{ij}}\}_{n\times m}$。

防御成功的相对隶属度

$$h^- = (h_1^-, h_2^-, \cdots, h_n^-)^T = (\bigwedge_{j=1}^{m} \overline{r_{1j}}, \bigwedge_{j=1}^{m} \overline{r_{2j}}, \cdots, \bigwedge_{j=1}^{m} \overline{r_{nj}})^T \quad (8)$$

防御失败的相对隶属度

$$s^- = (s_1^-, s_2^-, \cdots, s_n^-)^T = (\bigvee_{j=1}^{m} \overline{r_{1j}}, \bigvee_{j=1}^{m} \overline{r_{2j}}, \cdots, \bigvee_{j=1}^{m} \overline{r_{nj}})^T \quad (9)$$

决策分量 $\overline{r_{ij}}$ 与防御成功 h^- 的状况的接近程度,可以表示为

$$a_{ij}^- = \frac{\max(h_j^-, \overline{r_{ij}})}{\min(h_j^-, \overline{r_{ij}})} = \frac{\overline{r_{ij}}}{h_j^-} \quad (10)$$

相应的,他与防御失败 s^- 的状况的接近程度,可以表示为

$$c_{ij}^- = \frac{\max(s_j^-, \overline{r_{ij}})}{\min(s_j^-, \overline{r_{ij}})} = \frac{s_j^-}{\overline{r_{ij}}} \quad (11)$$

由(10)、(11)式和 2.1 节可得,在比较空间 $[s^-, h^-]$ 中,集对 $\{\overline{r_{ij}}, h^-\}$ 的联系度

$$\mu\{\overline{r_{ij}}, h^-\} = a_j^- + b_j^- I + c_j^- J \quad (12)$$

其中 $a_j^- = \sum_{i=1}^{n} w_i a_{ij}^-$, $b_j^- = \sum_{i=1}^{n} w_i b_{ij}^-$, $c_j^- = \sum_{i=1}^{n} w_i c_{ij}^-$。

2.3 U 上的集对分析模型

通过对比由 U^+ 和 U^* 上的决策 j 的决策向量 r_j 与攻击成功 h^+ 的同一度 a_j^+ 与 U^- 和 U^* 上的决策 j 的决策向量 $\overline{r_j}$ 与防御成功 h^- 的同一度 a_j^-,可以得到 U 上的集对分析模型如下:

命题 1:若 $a_j^+ > a_j^-$,U 上的攻击集与防御集的集对分析是攻击因素集起主导作用,决策结论决定于攻击因素。

命题 2:若 $a_j^+ < a_j^-$,U 上的攻击集与防御集的集对分析是防御因素集起主导作用,决策结论决定于防御因素。

命题 3:若 $a_j^+ = a_j^-$,U 上的攻击集与防御集的集对分析是攻击因素与防御因素势均力敌。

2.4 双枝集对分析的基本步骤

步骤 1:构造相对隶属度矩阵 R^+, R^-。

步骤 2:分别按照公式(1)、(2)、(8)、(9)计算攻击成功、攻击失败、防御成功、防御失败的相对隶属度。

步骤 3:根据文献[7]中定义,计算决策因素权向量 w。

步骤 4:分别按照公式(3)、(4)、(10)、(11)计算 a_{ij}^+、c_{ij}^+、a_{ij}^-、c_{ij}^-。

步骤 5:分别根据公式(7)、(12)计算集对

(下转第 102 页)

处理的试验研究[J].天津工业大学学报,2007,26(4):12-15.
[29] MASAWAKI P, ARIBAS J I, HERNANDEZ A. Retention of proteins in cross-flow UF through asymmetric inorganic membrane[J]. American Institute of Chemical Engineers, 1994,40(11):1901-1910.
[30] 冯建立,许振良,王学军.超滤去除红霉素发酵液乳化现象的研究[J].中国抗生素杂志,2007,32(3):150-153.
[31] 张晓飞,刘光全,张建华.利用超滤膜技术处理油田含盐采出水研究[J].油气田环境保护,2007,(3):4-7.
[32] DEMADIS K D, NEOFOTISTOU E, MAVERDAKI E, *et al*. Inorganic foulants in membrane systems: chemical control strategies and the contribution of "green chemistry"[J]. Desalination, 2005,179(6):281-295.
[33] KIM D, JUNG S, SONH J, *et al*. Biocide application for controlling biofouling of SWRO membranes - an overview [J]. Desalination, 2009,238(3):43-52.
[34] 于奕峰,顾春雷,王广玉,等.有机超滤膜处理退浆废水实验研究[J].膜科学与技术,2008,28(1):72-76.
[35] FUGERè R, MAMERI N, GALLOT J E, *et al*. Treatment of pig farm effluents by ultrafiltration[J]. Journal of Membrane Science, 2005,255(6):225-231.

(责任编辑 刘存英)

(上接第88页){r_j, h^+}和集对{$\overline{r_{ij}}, h^-$}的联系度。

步骤6:根据命题1-3,对BBFPAN中变迁t_j的输入库所集t_j中因素的作用效果做出判断。

3 结语

本文深入研究集对分析理论和双枝模糊集的关系,探求以双枝模糊集为基础的网络攻击模型BBFPAN中多层次的集对关系,首次将集对分析理论应用于攻击模型的分析研究,提出了BBFPAN双枝集对分析模型,为集对分析理论在攻击模型BBFPAN的推理过程中的应用奠定了基础。本研究一方面丰富了攻击模型的分析研究方法,使攻击模型能够更好的描述网络攻击的演变情况;另一方面扩展了集对分析的研究领域。

参考文献:

[1] 赵克勤.集对分析及其初步应用[M],杭州:浙江科技出版社,2000.
[2] 郑 鹏,张弼云.基于集对分析的图书馆服务质量综合评价[J].情报杂志,2008,(1):145-158.
[3] 杨习贝,杨静宇.不完备信息系统中的集对分析方法[J].计算机科学,2007,34(4):171-174.
[4] 邱 林,冯晓波.集对分析发在湖泊水质富营养化评价中的应用[J].人民长江,2008,39(5):52-54.
[5] 郑东良,黄文卿,孙 亮.基于集对分析的预警机指挥多机编队空战态势评估[J].空军工程大学学报(自然科学版),2008,9(1):9-13.
[6] 胡 波,王汝传,王海艳.基于集对分析的P2P网络安全中的信誉度改进算法[J].电子学报,2007,35(2):244-247.
[7] 黄光球,任大勇.基于双枝模糊决策和模糊Petri网的攻击模型[J].计算机应用,2007,27(11):2689-2693.
[8] 史开泉,李岐强.双枝模糊决策与决策识别问题[J].中国工程,2001,3(1):71-77.
[9] SHI KAIQUAN, CUI YUQUAN. Both-Branch fuzzy decision and decision encryption authentication[J]. Science in China (Series F), 2003, 46(2): 90-103.
[10] 刘保相,张春英.基于SPA的双枝模糊决策分析[J].模糊系统与数学,2006,20(4):74-78.
[11] 刘 林.应用模糊数学[M].陕西科学技术出版社,1996.

(责任编辑 刘存英)