文章编号：2096-1618(2017)01-0001-07
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-1000428.html
发表时间：2016-09-02

安全通论(13)

——沙盘演练的最佳攻防对策计算

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：在文献[2]与[13]中，已经指出：在任何现实的网络空间安全对抗中，无论有多少个红客与黑客参战，无论大家的价值观是多么千差万别(当然一定要事先确定，不能边战边修改价值观)，也无论是多么复杂的混战，只要大家是理性的(即，以自身利益最大化为目标)，那么，就一定存在能够共赢的最佳结局(即，纳什均衡状态)。这个结果虽然已被严格的数学证明了，但是，由于它太抽象，以致安全界的许多人(特别是决策者们)根本不相信或者不理解，非要逼问更具说服力的证据。由于“纳什均衡状态”对树立正确的安全观念非常重要，所以，本文只好花大力气，从复杂的博弈论中抽丝剥茧，提炼出了专门针对网络攻防沙盘演练的，真正能够使矛盾双方都达到最佳结局(纳什均衡状态)的攻防策略计算方法。

doi：10.16836/j.cnki.jcuit.2017.01.001

0　引言

一说起网络安全对抗，大家马上想到的就是“你死+我活”或“水涨+船高”或“魔高一尺+道高一丈”等等。总之，都认为“安全就是零和”。在这一错误观念的引导下，强势一方，要坚决置对手于死地；弱势一方，则不惜鱼死网破，也要“狭路相逢勇者胜”。于是，敌我双方不惜耗费大量的人力、物力和财力等，永远无休止地“兵来将挡”或“水来土掩”，这样一来，将永远没有最后的赢家，直到最终把大家都“累死”为止。

在文献[2]与[13]中，我们已经指出：其实，除了你死、我活两个状态外，网络安全对抗还存在另一个更加重要的状态：纳什均衡，此时，攻守双方的自身利益都能够达到最大化，而且，谁若再妄动，谁就会遭受额外的损失。同时，文献[2]还指出，无论是攻方还是守方，无论其实力有多强，其攻防业绩都一定存在着不可突破的理论极限(即，攻击信道和防守信道的信道容量)，这也从另一个角度，警示了攻防对抗中的任性行为。因此，网络空间安全对抗中，一方面，在备战阶段，我们必须认真准备具有足够威慑力的攻防手段，避免低水平的重复(比如，传统三大件(防火墙、入侵检测、加密)中的若干落后手段，就该考虑适时淘汰了)；另一方面，在今后战时阶段，我们又反而必须理智行动，尽快将对方逼入“纳什均衡状态”，从而实现共赢，争取自身利益最大化。

但是，由于文献[2]与[13]中相关结论过于抽象，使得大家难以理解，甚至怀疑我们的安全对抗的纳什均衡存在性定理：针对任何有限系统(即，攻防终端数目有限、攻防用户数有限、攻防手段数目有限。因此，现实中的所有网络系统，其实都是有限系统)，无论各方的损益函数怎么定义，红客和黑客之间的安全对抗都一定存在纳什均衡。

所以，为了树立正确、全面的安全观念，为了让大家更加直观地理解网络空间安全对抗的纳什均衡状态，本文将从复杂的博弈论中抽丝剥茧，提炼出了专门针对网络攻防沙盘演练的，真正能够使矛盾双方都达到最佳结局(纳什均衡状态)的攻防策略计算方法。

本文结果的价值至少体现在如下几个方面：

首先，在知己知彼的沙盘演练场景下，以实际可行的算法和步骤，给出了达到攻防双方共赢，各自利益都最大化的、具体的最佳攻防策略(纳什均衡状态)。

其次，沙盘演练与实战虽然有一定的区别，但是，在随时关注对方实力情况下，就可在平常预备好最佳的攻防策略，从而，在战时有助于稳准狠地出招。

还有，充分掌握最佳攻防策略，可以使现有的手段发挥其最大的效用，避免不必要的争斗和牺牲。

最后，也是最重要的，有助于全民树立正确的网络空间安全观念，让大家一起努力，实现共赢的纳什均衡。

1 最佳攻防策略与武器库的丰富和淘汰原则

当前全球的核武器竞争,基本上已经自动进入纳什均衡状态了:任何一个核大国都不敢轻举妄动,否则,可能玉石俱焚。但是,全球的网络安全对抗,还处于一团混战阶段,别指望能够在短期内自动达到纳什均衡状态,甚至,许多人还根本不相信,在如此复杂的网络对抗中,还存在着某种最佳的共赢状态! 所以,在没有具体战例的情况下,我们只好用沙盘演练来陈述观点,就像打仗前将军们要推演沙盘一样。

设攻方有 m 种攻击手段,分别记为 $A=\{a_1,a_2,\cdots,a_m\}$;守方有 n 种防护手段,分别记为 $B=\{b_1,b_2,\cdots,b_n\}$。当攻方用手段 a_i 来攻,而守方用 b_j 来防时,记攻方此时所获得的收入为 d_{ij},$1\leqslant i\leqslant m$,$1\leqslant j\leqslant n$;当然,此时,守方的损失也为 d_{ij}(也可以说守方的收入为 $-d_{ij}$)。记 $m\times n$ 矩阵 $\boldsymbol{D}=[d_{ij}]$ 为攻方的收入矩阵,它当然也是守方的损失矩阵。

这种沙盘非常接近实战:1)虽然在实战中,也许无法准确掌握对方的全部手段,但是,可以在平常,通过日积月累,了解其大概(当然,越精准越好);2)虽然在政治对抗中,收入矩阵 $\boldsymbol{D}$ 难以达成共识,但是,在经济对抗中,就完全没有这个问题了,所以,此时的沙盘就能够很逼真了。

当攻守双方的收入(损失)矩阵确定后,它们的整体实力就确定了,余下的问题就是在如此实力的条件下,各方如何为自己争得最大的利益,即,攻方要想获得尽可能多的收入,而守方则想尽可能地减少损失。

下面,就来给出相关的攻防策略(称为最优策略),使得能够同时满足攻守双方的愿望。

在平时,攻守双方应该努力提高自己的本领,使得自己在收入(损失)矩阵中占据优势;在战时,攻守双方一定要理智,要以自己利益最大化为目标,而不做损人不利己的事情。

下面在攻守双方都是理智的前提下,来进行沙盘演练:

一方面,对于任意 $1\leqslant i\leqslant m$,假如攻方用手段 a_i 展开攻击,那么,守方一定会用使自己的损失 d_{ij} 达到最小(即,$\min\limits_{1\leqslant j\leqslant n}d_{ij}$)的那个手段 b_j 来进行防护;于是,在精明的守方不出差错的前提下,攻方所能够企望获得的最大收入是 $\max\limits_{1\leqslant i\leqslant m}[\min\limits_{1\leqslant j\leqslant n}d_{ij}]$。

另一方面,对于任意 $1\leqslant j\leqslant n$,假如守方用手段 b_j 来进行防护,那么,攻方一定会用使自己的收入 d_{ij} 达到最大(即,$\max\limits_{1\leqslant i\leqslant m}d_{ij}$)的那个手段 a_i 去展开攻击;于是,在精明的攻方不出差错的前提下,守方所能够企望的最小损失是 $\min\limits_{1\leqslant j\leqslant n}[\max\limits_{1\leqslant i\leqslant m}d_{ij}]$。

假如在收入矩阵 $\boldsymbol{D}$ 中,碰巧成立等式 $\max\limits_{1\leqslant i\leqslant m}[\min\limits_{1\leqslant j\leqslant n}d_{ij}]=\min\limits_{1\leqslant j\leqslant n}[\max\limits_{1\leqslant i\leqslant m}d_{ij}]=d_{st}$,这时就意味着,“攻方所企望的最大收入”=“守方所企望的最小损失”,即攻守双方都达到了自己的目的,这时攻击手段 a_s 和防护手段 b_t 当然就是各自的最佳手段了,因为,这些手段使他们的利益都最大化了,此时,称该对抗存在最佳纯策略(a_s,b_t)。当然,最佳攻防手段可能会有多组,但是,他们在收入矩阵中所对应的最佳收入值是相等的。

但是,并非所有收入矩阵 $\boldsymbol{D}$ 都能够碰巧满足等式 $\max\limits_{1\leqslant i\leqslant m}[\min\limits_{1\leqslant j\leqslant n}d_{ij}]=\min\limits_{1\leqslant j\leqslant n}[\max\limits_{1\leqslant i\leqslant m}d_{ij}]$,比如,若在攻防手段中存在封闭环(就像石头、剪刀、布游戏那样),那么,这个等式就不成立。不过,幸好有如下定理:

定理 1(最佳纯策略存在性定理):在收入矩阵为 $\boldsymbol{D}$ 的攻防对抗中,存在攻守双方的最佳策略的充分必要条件是:存在某组对抗(a_s,b_t)使得对一切 $1\leqslant i\leqslant m$,$1\leqslant j\leqslant n$ 成立 $d_{it}\leqslant d_{st}\leqslant d_{sj}$。

证明:先证充分性,由于 $d_{it}\leqslant d_{st}\leqslant d_{sj}$,

故 $\max\limits_{1\leqslant i\leqslant m}d_{it}\leqslant d_{st}\leqslant\min\limits_{1\leqslant j\leqslant n}d_{sj}$,

又因为 $\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}\leqslant\max\limits_{1\leqslant i\leqslant m}d_{it}$

和 $\min\limits_{1\leqslant j\leqslant n}d_{sj}\leqslant\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}$,

所以有,$\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}\leqslant d_{st}\leqslant\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}$。

另一方面,对任给 i 和 j,有 $\min\limits_{1\leqslant j\leqslant n}d_{ij}\leqslant d_{ij}\leqslant\max\limits_{1\leqslant i\leqslant m}d_{ij}$,所以,

$\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}\leqslant\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}$。

于是,综合起来便有 $\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}=\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}$,充分性证毕。

现在来证必要性。若有 s 和 t,使得 $\max\limits_{1\leqslant i\leqslant m}d_{it}=\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}$ 和 $\min\limits_{1\leqslant j\leqslant n}d_{sj}=\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}$,则由 $\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}=\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}$ 就有,

$$\max_{1\leqslant i\leqslant m}d_{it}=\min_{1\leqslant j\leqslant n}d_{sj}\leqslant d_{st}\leqslant\max_{1\leqslant i\leqslant m}d_{it}=\min_{1\leqslant j\leqslant n}d_{sj}$$

所以,对任意 i,j 都有:$d_{it}\leqslant\max\limits_{1\leqslant i\leqslant m}d_{it}\leqslant d_{st}\leqslant\min\limits_{1\leqslant j\leqslant n}d_{sj}\leqslant d_{sj}$ 证毕。

为便于深入研究,现引进关于二元函数鞍点的概念。

定义 1:设 $f(x,y)$ 为一个定义在 $x\in A$ 及 $y\in B$ 上的实值函数,如果存在 $a\in A$ 和 $b\in B$,使得对一切 $x\in A$ 和 $y\in B$,都有 $f(x,b)\leqslant f(a,b)\leqslant f(a,y)$,那么,称 (a,b) 为函数 f 的一个鞍点。

由定义 1 及定理 1 可知,在收入矩阵为 $\boldsymbol{D}$ 的情况

下,存在纯策略意义最佳解 d_{st}(即,攻防双方存在最佳策略 a_s 和 b_t)的充要条件是:d_{st} 是矩阵 $\boldsymbol{D}$ 的一个鞍点。下面,矩阵 $\boldsymbol{D}$ 的鞍点也称为攻防对策的鞍点。

上面的定理 1 还可以再直观解释为:如果 d_{st} 是收入矩阵 $\boldsymbol{D}$ 中第 s 行中最小值,同时也是第 t 列中最大值,则 d_{st} 即为攻防最佳对策的收入值,并且 (a_s,b_t) 就是攻防双方的最佳对策解,即,当攻方选取了攻击手段 a_s 后,守方为了使其所失最少,只有选择防护手段 b_t,否则就可能失得更多;反之,当守方选取了防护手段 b_t 后,攻方为了得到最大的收入,他也只能选取攻击手段 a_s,否则,就会赢得更少。于是,攻防双方的对抗在 (a_s,b_t) 处达到了一个平衡的共赢状态,任何一方若想打破这个状态,他都会自遭损失。

收入矩阵的最佳攻防对策可能不唯一,但是,其多组最佳攻防策略之间,满足如下性质。

性质 1(无差别性)。即若 (a_s,b_t) 和 (a_u,b_v) 是同一个收入矩阵 $\boldsymbol{D}$ 的两组最佳对策,那么,$d_{st}=d_{uv}$。即,收入矩阵最佳对策的值是唯一的。换句话说,攻防双方不必在各种最佳策略之间去做选择,反正,最终结果都一样。

性质 2(可交换性)。即若 (a_s,b_t) 和 (a_u,b_v) 是同一个收入矩阵 $\boldsymbol{D}$ 的两组最佳对策,那么,(a_s,b_v) 和 (a_u,b_t) 也都是最佳对策。由此可知,当攻方采用最佳攻击手段时,他一定能够赢得最佳收入,并不依赖于守方到底采用哪种最佳防护手段;同理,当守方采用最佳防护手段时,他一定能够最小损失,并不依赖于攻方到底采用哪种最佳攻击手段。

前面已经知道:收入矩阵为 $\boldsymbol{D}$ 时,攻方有把握至少赢得收入 $v=\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}d_{ij}$,守方有把握的至多损失是 $u=\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}d_{ij}$;一般,攻方赢得的收入不会多于守方的所失,即总有 $v\leqslant u$。当 $u=v$ 时,收入矩阵存在纯策略意义下的最佳解 $u=v$。然而,一般情形并不总是如此,实际中出现的更多情形是 $v<u$,于是,此时在攻防双方之间不存在纯策略意义下的最佳策略。这时,就必须引进所谓的混合攻防策略。

定义 2:设攻方的所有攻击手段之集为 $A=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$,守方的所有防护手段之集为 $B=\{\beta_1,\beta_2,\cdots,\beta_n\}$,收入矩阵 $\boldsymbol{D}=[d_{ij}]$ 为 $m\times n$ 矩阵。记随机变量集

$$S_1=\{x\in E^m\mid x_i\geqslant 0,\ i=1,\cdots,m,\ \sum_{i=1}^{m}x_i=1\}\text{ 和}$$

$$S_2=\{y\in E^n\mid y_j\geqslant 0,\ j=1,\cdots,n,\ \sum_{j=1}^{n}y_j=1\}$$

分别称为攻方和守方的混合攻防策略集(或策略集),其中的任何随机变量 $x\in S_1$ 和 $y\in S_2$ 分别称为攻方和守方的混合攻防策略(或策略),并称攻防手段对 (x,y) 为一组混合局势;在该局势中,攻方的收入函数记为:$E(x,y)=x^{\mathrm{T}}\boldsymbol{D}y=\sum\limits_i\sum\limits_j d_{ij}x_iy_j$。这样得到的一组新攻防对策 (x,y) 称为对策的混合扩充。

由定义 2 可知,前面的纯攻防策略是此处混合策略的特例。例如,攻方的纯策略 α_k 等价于混合策略 $x=(x_1,\cdots,x_m)$,$x_k=1$ 并且对所有 $i\neq k$ 取 $x_i=0$。

一个混合策略 $x=(x_1,\cdots,x_m)$ 可设想成攻防双方,基于收入矩阵 $\boldsymbol{D}$,进行的多次重复进对抗时,攻方分别采用攻击手段 $\alpha_1,\cdots,\alpha_m$ 的频率。若只进行一次攻防,则混合策略 $x=(x_1,\cdots,x_m)$ 可设想成攻方对各种攻击手段的偏爱程度。

下面讨论攻防对抗在混合策略意义下解的定义。

设攻防双方仍然进行理智的对抗。当攻方采取混合策略 x 时,他只能希望获得(最不利的情形)$\min\limits_{y\in S_1}E(x,y)$ 的收入,因此,攻方应选取 $x\in S_1$,使得该式取极大值(最不利当中的最有利情形),即攻方可保证自己的赢得期望值不少于

$$v_1=\max_{x\in S_1}[\min_{y\in S_2}E(x,y)]$$

同理,守方可保证自己所遭受损失的期望值至多是

$$v_2=\min_{y\in S_1}[\max_{x\in S_2}E(x,y)]$$

首先,注意到上面的公式 v_1 和 v_2 是有意义的。因为根据定义,攻方的赢得函数 $E(x,y)$ 是欧氏空间 E^{m+n} 内有界闭集 F 上的连续函数,其中

$$F=\{(x,y):x_i\geqslant 0,y_j\geqslant 0,1\leqslant i\leqslant m,1\leqslant j\leqslant n,\ \sum_i x_i=1,\ \sum_j y_j=1\}$$

因此,对固定的 x 来说,$E(x,y)$ 是 S_2 上的连续函数,故 $\min\limits_{y\in S_2}E(x,y)$ 存在,而且 $\min\limits_{y\in S_2}E(x,y)$ 也是 S_1 上的连续函数,故 $\max\limits_{x\in S_1}[\min\limits_{y\in S_2}E(x,y)]$ 也存在。同样可说明 $\min\limits_{y\in S_2}[\max\limits_{x\in S_1}E(x,y)]$ 也存在。

其次,仍然有 $v_1\leqslant v_2$,即,攻方的收入不超过守方的损失事实上。设

$$\max_{x\in S_1}[\min_{y\in S_2}E(x,y)]=\min_{y}E(x^*,y)$$

$$\min_{y\in S_2}[\max_{x\in S_1}E(x,y)]=\max_{x}E(x,y^*)$$

于是 $v_1=\min\limits_{y\in S_2}E(x^*,y)\leqslant E(x^*,y^*)\leqslant\max\limits_{x\in S_1}E(x,y^*)=v_2$

定义 3:如果攻防双方的混合扩充满足等式

$$\max_{x\in S_1}[\min_{y\in S_2}E(x,y)]=\min_{y\in S_2}[\max_{x\in S_1}E(x,y)]=V$$

则称该 V 值为攻防双方的最佳对策值,并称使该等式成立的混合局势 (x^*,y^*) 为对抗双方在混合策略意义

下的最佳对策解(或简称,最佳解),x^* 和 y^* 分别称为攻方的最佳混合攻击策略和守方的最佳混合防护策略(或简称,最佳策略)。

今后,当纯策略意义下,不存在最佳攻防策略(或解不存在)时,就自动认为讨论的是在混合策略意义下的解,相应的攻方的收入函数为 $E(x,y)$。

和定理1类似,在混合策略意义下,最佳攻防解也存在鞍点型的充要条件。

定理2(最佳混合攻防策略存在性定理):攻防双方都存在最佳混合策略的充要条件是:存在 $x^* \in S_1$ 和 $y^* \in S_2$,使 (x^*,y^*) 为函数 $E(x,y)$ 的一个鞍点,即对一切 $x \in S_1, y \in S_2$,有 $E(x,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,y)$。

本定理的证明同定理1,不再复述。

下面来讨论最佳攻防对策解的存在性及解的有关性质。

如前所述,一般情况下,在纯策略意义下,最佳攻防策略的解往往是不存在的。但是,在混合策略意义下的解却总是存在的,并且,我们将通过一个构造性的证明,引出求解最佳攻防对策的基本方法,即,线性规划方法。

先给出如下两个记号:

当攻方采取纯策略 a_i(即,采用攻击手段 a_i)时,记其相应的收入函数为 $E(i,y)$,于是,$E(i,y)=\sum_j d_{ij}y_j$。当守方采取纯策略 β_j(即,采用防护手段 β_j)时,记其相应的收入函数为 $E(x,j)$,于是,$E(x,j)=\sum_i d_{ij}x_i$。

于是有,$E(x,y)=\sum_i\sum_j d_{ij}x_iy_j=\sum_i(\sum_j d_{ij}y_j)x_i=\sum_i E(i,y)x_i$ 和 $E(x,y)=\sum_i\sum_j d_{ij}x_iy_j=\sum_j(\sum_i d_{ij}x_i)y_j=\sum_j E(x,j)y_j$,由此,可给出定理2的另一种等价表示。

定理3:设 $x^* \in S_1, y^* \in S_2$,则 (x^*,y^*) 是一对最佳(混合)攻防策略的充要条件是:对任意 $i=1,\cdots,m$ 和 $j=1,\cdots,n$,有 $E(i,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,j)$。

证明:设 (x^*,y^*) 是一组最佳攻防策略,则由定理2就有 $E(x,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,y)$。由于纯策略是混合策略的特例,故有 $E(i,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,j)$。反之,若有 $E(i,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,j)$,由 $E(x,y^*)=\sum_i E(i,y^*)x_i \leqslant E(x^*,y^*)\sum_i x_i=E(x^*,y^*)$ 和 $E(x^*,y)=\sum_j E(x^*,j)y_j \geqslant E(x^*,y^*)\sum_j y_j=E(x^*,y^*)$,可得,$E(x,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,y)$。证毕。

可以这样来理解定理3:在验证 (x^*,y^*) 是否为最佳攻防对策时,公式 $E(i,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,j)$ 把需要对无限多个不等式进行验证的问题,转化为只要对有限个(mn 个)不等式进行验证的问题,从而使后续的工作量大幅度减少。

不难证明,定理3还可表述为如下等价的形式,而这一形式在求解最佳攻防策略时特别有用。

定理4:设 $x^* \in S_1, y^* \in S_2$,则 (x^*,y^*) 为最佳攻防策略解的充要条件是:存在数值 v,使得 x^* 和 y^* 分别是下述不等式方程组(Ⅰ)和(Ⅱ)的解,并且这个 v 就是最佳攻防策略的收入值。

(Ⅰ) $\sum_i d_{ij}x_i \geqslant v,\ 1 \leqslant j \leqslant n;\ \sum_i x_i=1;\ x_i \geqslant 0,\ 1 \leqslant i \leqslant m$

(Ⅱ) $\sum_j d_{ij}y_j \leqslant v,\ 1 \leqslant i \leqslant m;\ \sum_j y_j=1;\ y_j \geqslant 0,\ 1 \leqslant j \leqslant n$。

下面给出攻防对策的基本定理,虽然我们早在[2]和[13]中就给出了该定理的更一般形式(即,纳什均衡定理),但是,此处的证明过程特别有实用价值,因为,它具体给出了一个可行的,能为攻防双方求出最佳攻防策略的计算方法。

定理5:攻防双方一定存在混合策略意义下的最佳攻防策略解。

证明:由定理3知,只要证明存在 $x^* \in S_1$ 和 $y^* \in S_2$,使得 $E(x,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,y)$ 成立就行了。为此,考虑如下两个线性规划问题:

(P) $\max(w):\sum_i d_{ij}x_i \geqslant w,\ 1 \leqslant j \leqslant n;\ \sum_i x_i=1;\ x_i \geqslant 0,\ 1 \leqslant i \leqslant m$

(Q) $\min(v):\sum_j d_{ij}y_j \leqslant v,\ 1 \leqslant i \leqslant m;\ \sum_j y_j=1;\ y_j \geqslant 0,\ 1 \leqslant j \leqslant n$

容易验证,问题(P)和(Q)是互为对偶的线性规划问题,而且,$x=(1,0,\cdots,0) \in E^m$,$w=\min_j d_{1j}$ 是问题(P)的一个可行解。$y=(1,0,\cdots,0) \in E^n$,$v=\max_i d_{i1}$ 是问题(Q)的一个可行解。由线性规划的对偶理论可知,问题(P)和(Q)分别存在最优解 (x^*,w^*) 和 (y^*,v^*),且 $v^*=w^*$。即,存在 $x^* \in S_1$ 和 $y^* \in S_2$ 和数 v^*,使得对任意 $i=1,\cdots,m$ 和 $j=1,\cdots,n$,有 $\sum_j d_{ij}y_j^* \leqslant v^* \leqslant \sum_i d_{ij}x_i^*$ 或 $E(i,y^*) \leqslant v^* \leqslant E(x^*,j)$。

又由 $E(x^*,y^*)=\sum_i E(i,y^*)x_i^* \leqslant v^*\sum_i x_i^*=v^*$ 和 $E(x^*,y^*)=\sum_j E(x^*,j)y_j^* \geqslant v^*\sum_j y_j^*=v^*$,得到 $v^*=E(x^*,y^*)$,故由 $E(i,y^*) \leqslant v^* \leqslant E(x^*,j)$ 就知道定理3中的公式 $E(i,y^*) \leqslant E(x^*,y^*) \leqslant E(x^*,j)$ 成立。证毕。

此处定理5的证明是一个构造性的证明,它不仅证明了攻防双方的最佳对策解的存在性,而且还给出了利用线性规划求出最佳攻防策略的方法。

下面的几个定理就来讨论最佳攻防对策的若干重要性质,以及它们在求解最佳攻防策略时的用途。

定理6:设 (x^*,y^*) 是一对最佳攻防策略解,其最佳收入值是 v,则

(1)若 $x_i^*>0$,则 $\sum_j d_{ij}y_j^*=v$。解释出来便是:若攻击手段 α_i 不可缺少,那么,攻方坚持不懈地只用 α_i 来攻击 n 次时,守方若出招最佳防护策略 y^*,那么,最后的收入之和刚好等于最佳收入值 v。

(2)若 $y_j^*>0$,则 $\sum_i d_{ij}x_i^*=v$。解释出来便是:若防护手段 β_j 不可缺少,那么,守方坚持不懈地只用 β_j 来防护 m 次时,攻方若出招最佳攻击策略 x^*,那么,攻方最后的收入之和刚好也等于最佳收入值 v。

(3)若 $\sum_j d_{ij}y_j^*<v$,则 $x_i^*=0$。解释出来便是:若攻方连续 n 次用攻击手段 α_i 来攻击时,而守方出招最佳防护策略 y^*,并且最后的收入之和小于最佳收入值 v,那么,攻击手段 α_i 便可以被淘汰了。

(4)若 $\sum_i d_{ij}x_i^*>v$,则 $y_j^*=0$。解释出来便是:若守方连续 m 次使用防护手段 β_j,而攻方出招最佳攻击策略 x^*,并且最后的收入之和小于最佳收入值 v,那么,防护手段 β_j 也可被淘汰了。

证明:按定义有 $v=\max_{x\in S_1}E(x,y^*)$,故,

$$v-\sum_j d_{ij}y_j^*=\max_{x\in S_1}E(x,y^*)-E(i,y^*)\geqslant 0$$

又因 $\sum_i x_i^*[v-\sum_j d_{ij}y_j^*]=v-\sum_i\sum_j d_{ij}x_i^*y_j^*=0$ 并且 $x_i^*\geqslant 0, i=1,\cdots,m$

所以,当 $x_i^*>0$ 时,必有 $\sum_j d_{ij}y_j^*=v$;当 $\sum_j d_{ij}y_j^*<v$ 时,必有 $x_i^*=0$。于是(1)和(3)得证。同理可证(2)和(4)。证毕。

该定理 6 的几个结论,可用于淘汰落后的攻防手段,使得攻防双方的效率更高。

若记最佳对抗的策略解集为 T,下面 3 个定理揭示了解集 T 的一些性质。

定理 7:设有两个收入矩阵 $\boldsymbol{D}_1$ 和 $\boldsymbol{D}_2$,并且 $\boldsymbol{D}_1=[d_{ij}]$,$\boldsymbol{D}_2=[d_{ij}+L]$,$L$ 为任一常数;则有(1) $V_2=V_1+L$,即,后者的最佳收入值也增加 L;(2) $T_1=T_2$,即,它们有相同的最佳策略解集。换句话说,如果黑客的攻击能力普遍都增加 L 的话,那么,他可以在沿用过去攻击策略的情况下,将其最佳攻击收入值也提高 L。

定理 8:设有两个收入矩阵 $\boldsymbol{D}_1$ 和 $\boldsymbol{D}_2$,并且 $\boldsymbol{D}_1=[d_{ij}]$,$\boldsymbol{D}_2=a[d_{ij}]$,$a>0$ 为任一常数;则有(1) $V_2=aV_1$;(2) $T_1=T_2$。换句话说,如果黑客的攻击能力普遍提高 a 倍的话,那么,他可以在沿用过去攻击策略的情况下,将其最佳攻击收入也提高 a 倍。

上面的定理 7 和定理 8 表明:平时的备战,确实是有用的。当然,如果守方通过备战,使得收入矩阵的值减少,也可类似地降低自己的损失。

定理 9:如果收入矩阵 $\boldsymbol{D}$ 是斜对称矩阵,即,$\boldsymbol{D}=-\boldsymbol{D}^{\mathrm{T}}$,则,(1)其最佳对抗策略的收入值为 0;(2) $T_1=T_2$,即,攻防双方的最优策略集是相同的。换句话说,此时攻守双方每次出招都相同,所以,最终输赢相等,总和为零。这时,也有类似于“以子之矛,攻子之盾”的情况。

上面的定理 7 至定理 9 都很容易验证,此处略去细节。在给出定理 10 之前,先给出攻防对抗的优超纯策略定义。

定义 4:设攻方手段集 $\boldsymbol{S}_1=\{\alpha_1,\cdots,\alpha_m\}$,守方手段集 $\boldsymbol{S}_2=\{\beta_1,\cdots,\beta_n\}$,收入矩阵 $\boldsymbol{D}=[d_{ij}]$,如果对一切 $j=1,\cdots,n$,都有 $d_{sj}\geqslant d_{tj}$,即矩阵 $\boldsymbol{D}$ 的第 s 行元素均不小于第 t 行的对应元素,则称攻方的纯策略 α_s 优超于 α_t(即,攻方的手段 α_s 始终比 α_t 厉害);同样,若对一切 $i=1,\cdots,m$,都有 $d_{is}\leqslant d_{it}$,即矩阵 $\boldsymbol{D}$ 的第 t 列元素均不小于第 s 列的对应元素,则称守方的纯策略 β_s 优超于 β_t(即,守方的手段 β_s 始终优于 β_t)。

定理 10:设攻方手段集 $S_1=\{\alpha_1,\cdots,\alpha_m\}$,守方手段集 $S_2=\{\beta_1,\cdots,\beta_n\}$,收入矩阵 $\boldsymbol{D}=[d_{ij}]$,如果纯策略 α_1 被其余纯策略 $\alpha_2,\cdots,\alpha_m$ 中的某个策略所优超,由 D 中去掉第一行,可得到一个新的 $(m-1)\times n$ 矩阵 $\boldsymbol{D}_1$,于是有:(1) $V=V_1$,即,基于 $\boldsymbol{D}$ 和 $\boldsymbol{D}_1$ 的最佳对抗策略的收入值是相同的;(2)无论是基于 $\boldsymbol{D}$ 还是 $\boldsymbol{D}_1$,守方的最优防护策略都是相同的;(3)若 $(x_2,\cdots,x_m)$ 是 $\boldsymbol{D}_1$ 中攻方的最优攻击策略,则 $(0,x_2,\cdots,x_m)$ 便是其在 $\boldsymbol{D}$ 中的最优攻击策略。

这个定理其实非常容易理解,即,如果攻方有一个手段很落后,以至于它完全可以被另一个攻击手段所替代,那么,攻方扔掉该手段对整合对抗局势不会产生任何影响,而守方也可以完全不必考虑如何来对付这种落后的武器。正如,攻方有了枪以后,还要刀干吗;守方既然能够对付枪了,又何必担忧刀呢。

证明:不妨设攻击手段 α_2 优超于 α_1,即,$d_{2j}\geqslant d_{1j}, j=1,\cdots,n$。若 $x=(x_2,\cdots,x_m)$ 和 $(y_1,\cdots,y_n)$ 是 $\boldsymbol{D}_1$ 的最佳攻防策略解,由定理 3,有,$\sum_{j=1}^{n}d_{ij}y_j\leqslant V_1\leqslant\sum_{i=2}^{m}d_{ij}x_i$ 对所有 $i=2,\cdots,m$ 和 $j=1,\cdots,n$;这里 V_1 是基于 $\boldsymbol{D}_1$ 的最佳攻击策略的收入值。

因为 α_2 优超于 α_1,所以,$\sum_{j=1}^{n}d_{1j}y_i\leqslant\sum_{j=1}^{n}d_{2j}y_j\leqslant V_1$。合并上面的两式,可得,$\sum_{j=1}^{n}d_{ij}y_j\leqslant V_1\leqslant\sum_{i=2}^{m}d_{ij}x_i+d_{1j}.\ 0$,对所有 $i=1,\cdots,m$ 和 $j=1,\cdots,n$。或者,

$E(i,y)\leqslant V_1\leqslant E(x,j)$,对所有 $i=1,\cdots,m$ 和 $j=1,\cdots,n$。由定理 4 便知,(x,y) 就是 $\boldsymbol{D}$ 的最佳对抗策略解,其中 $x=(0,x_2,\cdots,x_m)$,且 $V_1=V$,基于 $\boldsymbol{D}$ 的最佳攻击收入。证毕。

推论:在定理 10 中,若 α_1 不是为纯策略 $\alpha_2,\cdots,\alpha_m$

中之一所优超,而是为 $\alpha_2,\cdots,\alpha_m$ 的某个凸线性组合所优超,则定理的结论仍然成立。

此处的定理 10 实际给出了一个化简收入矩阵 $\boldsymbol{D}$ 的原则,或者说淘汰落后攻防手段的原则,称之为优超原则,即,当攻方的某个攻击手段 a_i 被其他攻击手段或其凸线性组合所优超时,可在收入矩阵 $\boldsymbol{D}$ 中划去第 i 行,而得到一个与原对抗等价但收入矩阵阶数较小的攻防对抗,从而,使得求解其最佳对抗策略解时更容易些。类似地,对防守方来说,可以在收入矩阵 $\boldsymbol{D}$ 中划去被其他列或其他列的凸线性组合所优超的那些列。

到此,我们给出 3 个方面的有趣结果:(1)如何使攻防武器库中的已有武器,发挥最大的作用,即,给出了最佳攻防策略,见定理 5 的证明过程;(2)如何对已有的武器库进行精练,淘汰落后的武器,使得战时所用的武器能够更好地发挥作用,即,定理 6 和定理 10 等;(3)如何丰富武器库,定理 7 和定理 8 等。

2 最佳攻防对抗策略的计算

虽然在定理 5 的证明过程中,我们已经给出了如何计算最佳攻防策略,但是,本节想再做一些细节强调,以供有特殊兴趣的读者直接使用。

先看最简单的情况:攻守双方都各只有两种手段,即,攻方的收入矩阵为 2×2 阶的,即,$\boldsymbol{D}=[d_{ij}],i,j=1,2$。

如果 $\boldsymbol{D}$ 有鞍点,则很快可求出攻防双方的最优纯策略;如果 $\boldsymbol{D}$ 没有鞍点,则可证明攻防双方最优混合策略中的 x_i^*,y_j^* 均大于零。于是,由定理 6 可知,为求最优混合攻防策略,可求解下列方程组:

(Ⅰ) $d_{11}x_1+d_{21}x_2=v;\ d_{12}x_1+d_{22}x_2=v;\ x_1+x_2=1$

(Ⅱ) $d_{11}y_1+d_{12}y_2=v;\ d_{21}y_1+d_{22}y_2=v;\ y_1+y_2=1$

当矩阵 $\boldsymbol{D}$ 不存在鞍点时,可以证明上面方程组(Ⅰ)和(Ⅱ)一定有严格非负解 $x^*=(x_1^*,x_2^*)$(最佳攻击策略)、$y^*=(y_1^*,y_2^*)$(最佳防护策略)和最佳收入值 v,其中,

$x_1^*=(d_{22}-d_{21})/[(d_{11}+d_{22})-(d_{12}+d_{21})]$和

$x_2^*=(d_{11}-d_{12})/[(d_{11}+d_{22})-(d_{12}+d_{21})]$

$y_1^*=(d_{22}-d_{12})/[(d_{11}+d_{22})-(d_{12}+d_{21})]$和

$y_2^*=(d_{11}-d_{21})/[(d_{11}+d_{22})-(d_{12}+d_{21})]$

$v=(d_{11}d_{22}-d_{12}d_{21})/[(d_{11}+d_{22})-(d_{12}+d_{21})]$

对一般的攻防对抗情况,最佳策略解可用如下线性方程组方法:

根据定理 4,求解最佳攻防对策解 (x^*,y^*) 的问题等价于求解不等式方程组

$$\sum_i d_{ij}x_i\geqslant v,\ 1\leqslant j\leqslant n;\ \sum_i x_i=1;x_i\geqslant 0,\ 1\leqslant i\leqslant m$$

和 $\sum_j d_{ij}y_j\leqslant v,1\leqslant i\leqslant m;\ \sum_j y_j=1;y_j\geqslant 0,\ 1\leqslant j\leqslant n$。

又根据定理 5 和定理 6,如果假设最优攻防策略中的 x_i^* 和 y_j^* 均不为零,即可将上述两个不等式组的求解问题转化成求解下面两个方程组的问题:

(Ⅰ) $\sum_i d_{ij}x_i=v,j=1,\cdots,n;\ \sum_i x_i=1$ 和

(Ⅱ) $\sum_j d_{ij}y_j=v,i=1,\cdots,m;\ \sum_{jy_j=1}$

如果该方程组(Ⅰ)和(Ⅱ)存在非负解 x^* 和 y^*,便求得了一个最佳攻防对策解 (x^*,y^*)。如果由上述两个方程组求出的解 x^* 和 y^* 中有负的分量,则可视具体情况,将(Ⅰ)和(Ⅱ)式中的某些等式改成不等式,继续试算求解,直至求出最佳攻防对策解。这种方法由于事先假设 x_i^* 和 y_j^* 均不为零,故当 x^* 和 y^* 的实际分量中有些为零时,(Ⅰ)和(Ⅱ)式一般无非负解,而随后的试算过程则是无固定规程可循的。因此,这种最佳攻防策略的计算方法在实际应用中具有一定的局限性。

计算最佳攻防策略的更好的方法,是如下的线性规划方法。

由定理 5 已知,最佳攻防对策的求解等价于一对互为对偶的线性规划问题,而定理 4 表明,最佳攻防对策解 x^* 和 y^* 等价于下面两个不等式组的解。

$$(\text{Ⅰ})\ \sum_i d_{ij}x_i\geqslant v,\quad j=1,\cdots,n;\quad \sum_i x_i=1;\quad x_i\geqslant 0,i=1,\cdots,m$$

$$(\text{Ⅱ})\ \sum_j d_{ij}y_j\leqslant v,\quad i=1,\cdots,m;\quad \sum_j y_j=1;\quad y_j\geqslant 0,j=1,\cdots,n$$

其中,$v=\max\limits_{x\in S_1}[\min\limits_{y\in S_2}E(x,y)]=\min\limits_{y\in S_2}[\max\limits_{x\in S_1}E(x,y)]$ 就是最佳攻防对策的收入值。

定理 11:最佳攻防策略的收入值为

$v=\max\limits_{x\in S_1}[\min\limits_{1\leqslant j\leqslant n}E(x,j)]=\min\limits_{y\in S_2}[\max\limits_{1\leqslant i\leqslant m}E(i,y)]$。

证明:因 v 最佳攻防对策的收入值,

故,$v=\max\limits_{x\in S_1}[\min\limits_{y\in S_2}E(x,y)]=\min\limits_{y\in S_2}[\max\limits_{x\in S_1}E(x,y)]$。

一方面,任给 $x\in S_1$,有 $\min\limits_{1\leqslant j\leqslant n}E(x,j)\geqslant\min\limits_{y\in S_2}E(x,y)$,

故,$\max\limits_{x\in S_1}[\min\limits_{1\leqslant j\leqslant n}E(x,j)]\geqslant\max\limits_{x\in S_1}[\min\limits_{y\in S_2}E(x,y)]$

另一方面,任给 $x\in S_1,y\in S_2$,有,$E(x,y)=\sum\limits_{j=1}^{n}E(x,j)y_j\geqslant\min\limits_{1\leqslant j\leqslant n}E(x,j)$

故,$\min\limits_{y\in S_2}E(x,y)\geqslant\min\limits_{1\leqslant j\leqslant n}E(x,j)$ 和

$\max\limits_{x\in S_1}[\min\limits_{y\in S_2}E(x,y)]\geqslant\max\limits_{x\in S_1}[\min\limits_{1\leqslant j\leqslant n}E(x,j)]$

于是,$v=\max\limits_{x\in S_1}[\min\limits_{1\leqslant j\leqslant n}E(x,j)]$

同理可证 $v=\min\limits_{y\in S_2}[\max\limits_{1\leqslant i\leqslant m}E(i,y)]$。证毕。

下面给出求解攻防对抗最佳策略的线性规划方法。

作变换(根据定理 7,不妨设 $v>0$):$f_i=x_i/v, i=1,\cdots,m$,则不等式组(I)变为,

(Ⅰ) $\sum_i d_{ij}f_i\geqslant 1, j=1,\cdots,n; \sum_i f_i=1/v; f_i\geqslant 0, i=1,\cdots,m$

根据定理 11,有 $v=\max\limits_{x\in S_1}[\min\limits_{1\leqslant j\leqslant n}(\sum_i d_{ij}x_i)]$,这样,不等式组(Ⅰ)即等价于线性规划问题:

(P):$\min z=\sum_i f_i; \sum_i d_{ij}f_i\geqslant 1, j=1,\cdots,n; f_i\geqslant 0$

同理,作变换 $g_j=y_j/v, j=1,\cdots,n$

则不等式组(II)变为

(Ⅱ) $\sum_j d_{ij}g_j\leqslant 1, i=1,\cdots,m; \sum_j g_j=1/v; g_j\geqslant 0, j=1,\cdots,n$

其中,$v=\min\limits_{y\in S_2}[\max\limits_{1\leqslant i\leqslant m}\sum_j d_{ij}y_j]$,与之等价的线性规划问题是:

(D):$\max w=\sum_j g_j; \sum_j d_{ij}g_j\leqslant 1, i=1,\cdots,m; g_j\geqslant 0, j=1,\cdots,n$

显然,问题(P)和(D)是互为对偶的线性规划,故可利用单纯形或对偶单纯形方法求解。在求解时,一般先求问题(D)的解,因为这样容易在迭代的第一步就找到第一个基本可行解,而问题(P)的解从问题(D)的最后一个单纯形表上即可得到。当求得问题(P)和(D)的解后,再利用变换 $f_i=x_i/v$ 和 $g_j=y_j/v$ 即可求出原对策问题的解及最佳攻防对策值。

3　结束语

在实战中要想知道每个 d_{ij} 的精确值,确实不容易;但是,如果攻防双方只考虑每次对抗的输、赢结果,那么,情况一下子就很明朗了。即,若攻方用 α_i 去攻,守方用 β_j 来防时:若攻方胜,则令 $d_{ij}=1$;若守方胜,则令 $d_{ij}=-1$;若双方平局,则令 $d_{ij}=0$。本文的所有结果,对这种输赢矩阵也是有效的。只是,如果最佳收入值为正时,攻方赢;否则,守方赢。当然,若对这种输赢情况进行专门的、更深入的分析,也许还能够得出一些更好的结果。

当然,本文所演示的沙盘攻防,并不包含网络安全攻防的所有情况(比如,文献[7]中研究过的偷袭就是例外),但是,它确实是网络安全攻防的主流,因此,本文具体给出的最佳攻防策略的计算方案,对完善安全观念是很有帮助的。希望攻防双方理智行动,在实现自身利益最大化的同时,最终共赢。

参考文献:

[1] 杨义先,钮心忻. 安全通论(1)之“经络篇”[EB/OL]. http://blog. sciencenet. cn/blog-453322-944217. html,2015-12-18.

[2] 杨义先,钮心忻. 安全通论(2):攻防篇之“盲对抗”[EB/OL]. http://blog. sciencenet. cn/blog-453322-947304. html,2016-01-01.

[3] 杨义先,钮心忻. 安全通论(3):攻防篇之“非盲对抗”之“石头剪刀布游戏”[EB/OL]. http://blog. sciencenet. cn/blog-453322-948089. html,2016-01-04.

[4] 杨义先,钮心忻. 安全通论(4):攻防篇之“非盲对抗”之“童趣游戏”[EB/OL]. http://blog. sciencenet. cn/blog-453322-949155. html,2016-01-09.

[5] 杨义先,钮心忻. 安全通论(5):攻防篇之“非盲对抗”收官作及“劝酒令”[EB/OL]. http://blog. sciencenet. cn/blog-453322-950146. html,2016-01-13.

[6] 杨义先,钮心忻. 安全通论(6):攻防篇之“多人盲对抗”[EB/OL]. http://blog. sciencenet. cn/blog-453322-954445. html,2016-02-04.

[7] 杨义先,钮心忻. 安全通论(7):黑客篇之“战术研究”[EB/OL]. http://blog. sciencenet. cn/blog-453322-956051. html,2016-02-14.

[8] 杨义先,钮心忻. 安全通论(8):黑客篇之“战略研究”[EB/OL]. http://blog. sciencenet. cn/blog-453322-958609. html,2016-02-25.

[9] 杨义先,钮心忻. 安全通论(9):红客篇[EB/OL]. http://blog. sciencenet. cn/blog-453322-960372. html,2016-03-04.

[10] 杨义先,钮心忻. 安全通论(10):攻防一体的输赢次数极限[EB/OL]. http://blog. sciencenet. cn/blog-453322-984644. html,2016-06-14.

[11] 杨义先,钮心忻. 安全通论(11):信息论、博弈论与安全通论的融合[EB/OL]. http://blog. sciencenet. cn/blog-453322-989745. html,2016-07-11.

[12] 杨义先,钮心忻. 安全通论(12):对话的数学理论[EB/OL]. http://blog. sciencenet. cn/blog-453322-993540. html,2016-07-30.

[13] 杨义先. 刷新你的安全观念[EB/OL]. http://blog. sciencenet. cn/blog-453322-983276. html, 2016-06-08.

[14] 甘应爱,田丰. 运筹学[M]. 北京:清华大学出版社,2005.