文章编号: 2096-1618(2016)05-0447-06
稿件来源:科学网
网址:http://blog.sciencenet.cn/blog-453322-984644.html
发表时间:2016-06-14

安全通论(10)

——攻防一体的输赢次数极限

杨义先, 钮心忻
(北京邮电大学信息安全中心,北京 100876)

摘要:在实际的网络对抗中,攻与防其实是一体的,即每个当事人既是攻方(黑客)又是守方(红客),而且,除了最常见的"1对1"的对抗之外,还有"1对多",还有多人分为两个集团(比如,历史上的北约和华约集团)之间的对抗,当然,更一般地,还有所有当事人之间的混战。针对所有这些可能的对抗场景,在"任何人不会自己骗自己"的假定下,给出了全部"独裁评估事件"可达理论极限。

0 引言

由于在网络空间安全等许多真实对抗中,与"非盲对抗"相比,"盲对抗"才是常态,因此,有必要对"盲对抗"进行更深入的研究。本文是文献[2]和[6]的继续。

为清晰起见,在文献[2]和[6],我们将攻方(黑客)和守方(红客)进行了严格的区分。但是,在实际对抗中,往往各方都是攻守兼备:在攻击别人的同时,也要防守自己的阵地;他们既是黑客也是红客。因此,本文针对这种攻防一体的情况,研究相关各方的能力极限。

通过文献[2]和[6],我们知道:如果仅仅借助《信息论》,那么,面对诸如"1攻多"等攻防情况,我们就束手无策,最多建立起"某次攻击成功"与"某个广播信道无差错传输1比特信息"之间的等价关系,但是,由于至今"广播信道的信道容量"等都还是没有解决的世界难题,而且在短期内也不可能解决,所以,我们只好另辟蹊径:祭出《博弈论》这个法宝。

但是,要想驾驭《博弈论》绝非易事,如果按常规,根据每个回合中各方的"收益函数"值,套用纳什均衡定理等,那么,将面临一个致命的挑战,即:对政治黑客而言,压根就没有什么"收益函数",因为,他们是不计代价的;对经济黑客而言,确定"收益函数"值的难度,甚至可能超过"各方攻防对抗"的难度,显然这就本末倒置了! 就算是经济黑客愿意花大力气,把"收益函数"值都测试出来,那么,对《安全通论》的进步,也没有理论价值,只不过是做了一道小儿科习题而已。

所以,必须创新性地利用《博弈论》,为此,我们继续沿用文献[2]和[6]的研究对象,重点考虑各方在对抗中的输赢次数。当然,输赢次数的多少,只能在一定程度上说明对抗各方的损益情况,毕竟,一次大赢可能好过多次小输。

1 盲对抗的自评估输赢分类

既然"兵不厌诈",所以在盲对抗中,每个回合后,攻防双方都只知道"自己的损益"情况(即,盲自评估为"输"或"赢"),而对"对方的损益情况"一无所知。为了不影响其广泛适用性,文献[2]和[6]中,建立了以"攻防双方的盲自评估"为基础的,聚焦于"胜负次数"的对抗模型,而并不关心每次胜负到底意味着什么。下面,对这种模型及其"输赢分类"再进行更详细的说明。

在每个回合后,各方对自己本轮攻防的"业绩"进行"保密的自评估"(即,该评估结果不告诉任何人,因此,其客观公正性就有保障,因为,可以假定每个人不会"自己骗自己",阿Q除外):比如,一方(X)若认为本回合的攻防对抗中自己得胜,就自评估为$X=1$;若认为本回合自己失败,就自评估为$X=0$。同理,在每个回合后,另一方(Y)对自己的"业绩"也进行"保密的自评估":若认为本回合自己得胜,就自评估为$Y=1$;若认为本回合自己失败,就自评估为$Y=0$。

当然,每次对抗的胜负,绝不是由攻方或守方单方面说了算,但是,基于攻守双方的客观自评估结果,从旁观者角度来看,我们可以公正地确定如下一些输赢规则。为减少冗余,我们只给出每个回合后,从X方角度看到的自评估输赢情况(对Y方,也可以有类似的规则。为节省篇幅,不再重复了,因为,实际上每个人都是攻守一体的):

“对手服输的赢”(在文献[2]中,也称为“真正赢”),此时双方的自评估结果集是$\{X=1,Y=0\}\cup\{X=0,Y=0\}$,即,此时对手服输了($Y=0$),哪怕自己都误以为未赢($X=0$)。

“对手的阿 Q 式赢”,此时双方的自评估结果集是$\{X=0,Y=1\}\cup\{X=1,Y=1\}$,即,此时对手永远认为他赢了($Y=1$),那怕另一方并不认输($X=1$)。

“自己心服口服的输”(在文献[2]中,也称为“真正输”):此时双方的自评估结果集是$\{X=0,Y=1\}\cup\{X=0,Y=0\}$,即,此时自己服输了($X=0$),哪怕对手以为未赢($Y=0$)。

“自己的阿 Q 式赢”,此时双方的自评估结果集是$\{X=1,Y=0\}\cup\{X=1,Y=1\}$,即,此时永远都认为自己赢了($X=1$),哪怕另一方并不认赢($Y=1$)。

“对手服输的无异议赢”:此时双方的自评估结果集是$\{X=1,Y=0\}$,即,攻方自评为“成功”,守方也自评为“失败”。(从守方角度看,这等价于“无异议地守方认输”)

“对手不服的赢”:此时双方的自评估结果集是$\{X=1,Y=1\}$,即,攻守双方都咬定自己“成功”。

“意外之赢”:此时双方的自评估结果集是$\{X=0,Y=0\}$,即,攻守双方承认自己“失败”。

“无异议地自己认输”:此时双方的自评估结果集是$\{X=0,Y=1\}$,即,攻方承认自己“失败”,守方自评为“成功”。(从守方的角度看,这等价于“对手无异议的守方赢”)。

上面的 8 种自评估输赢情况,其实可以分为两大类:其一,叫“独裁评估”,即,损益情况完全由自己说了算(即,前面的 4 种情况,根本不考虑另一方的评估结果);其二,叫“合成评估”,即,损益情况由攻守双方的盲自评估合成(后面的 4 种情况)。

由于“合成评估”将攻守双方都锁定了,所以,其变数不大,完全可以根据攻防的自评估历史记录,客观地计算出来,而且,其概率极限范围也很平凡(介于 0 与 1 之间,而且还是遍历的),因此,它们没有理论研究的价值。故,本文只考虑“独裁评估”的极限问题。

2 星状网络对抗的输赢次数极限

所谓“星状网络对抗”,意指,对抗的一方只有一个人,比如,星状图的中心点(X);对抗的另一方有许多人,比如,星状图的非中心点($Y_1,Y_2,\cdots,Y_n$)。更形象地说,此时,一群人要围攻一位武林高手,当然,该武林高手也要回击那一群人。为研究方便,假设这一群人彼此之间是相互独立的,他们只与武林高手过招,互相之间不攻击。

由于在文献[6]中,还遗留了一个未解决的难题:1 攻多时的能力极限问题。当时虽然将此问题等价地转化为了“广播信道的信道容量计算问题”,但是,由于该容量问题至今还是一个世界难题,所以,本小节以“1 攻多”为例,一方面随便回答了“1 攻多的黑客能力极限”等问题;另一方面,为后面榕树网络和一般网络对抗的输赢次数极限研究做准备。

为了增强安全性,红客在建设网络系统时,常常建设一个甚至多个(异构)灾难备份恢复系统,一旦系统本身被黑客攻破后,红客可以马上启用备份系统,从而保障业务的连续性。因此,在这种情况下,黑客若想真正取胜,他就必须同时攻破主系统和所有备份系统,否则,黑客就会前功尽弃。这就是“一位黑客攻击多位红客”的实际背景,换句话说,只要有哪怕一个备份未被黑客攻破,那么,就不能算黑客真正赢。当然,也许红客们并不知道是同一个黑客在攻击他们,所以,可假定红客们互不协同,彼此独立。

先考虑 1 个高手对抗 2 个战士的情形,然后,再做推广。

设高手 $X=(X_1,X_2)$ 想同时对抗两个战士 Y_1 和 Y_2。由于这两个战士是互为备份系统的守卫者,因此,高手必须同时把这两个战士打败,才能算真赢。仍然假设:攻防各方采取“回合制”,并且,每个“回合”后,各方都对本次的攻防结果,给出一个“真心的盲自评”,由于这些自评结果是不告诉任何人的,所以,有理由假设“真心的盲自评”是真实可信的,没必要做假。

分别用随机变量 Y_1 和 Y_2 代表第一个和第二个战士,他们按如下方式对自己每个回合的战果,进行真心盲自评:

战士 Y_1 对本回合防御盲自评为成功,则 $Y_1=1$;战士 Y_1 对本回合防御盲自评为失败,则 $Y_1=0$;

战士 Y_2 对本回合防御盲自评为成功,则 $Y_2=1$;战士 Y_2 对本回合防御盲自评为失败,则 $Y_2=0$;

由于每个回合中,高手要同时攻击两个战士,所以,用 2 维随机变量 $X=(X_1,X_2)$ 代表高手。为形象计,假定高手有两只手 X_1 和 X_2,分别用来对付那两个战士。他按如下方式对自己每个回合攻击 Y_1 和 Y_2 的成果,进行真心盲自评:

本回合 X 自评攻击 Y_1 成功,自评攻击 Y_2 成功时,记为,$X_1=1,X_2=1$;

本回合 X 自评攻击 Y_1 成功,自评攻击 Y_2 失败时,记为,$X_1=1,X_2=0$;

本回合 X 自评攻击 Y_1 失败,自评攻击 Y_2 成功时,记为,$X_1=0,X_2=1$;

本回合 X 自评攻击 Y_1 失败,自评攻击 Y_2 失败时,

记为,$X_1=0, X_2=0$。

当然,每次对抗的胜负,绝不是由某个单方面说了算,但是,上述客观自评估结果,从旁观者角度来看,我们可以公正地确定如下一些输赢规则。由于这时从任何一个战士(Y_1或Y_2)的角度来看,他面临的情况与"1对1的情况"完全相同,没必要再重复讨论,所以,下面只从高手 X 的角度来对"独裁评估"输赢次数的极限问题。

首先看高手"真正赢"的情况,即,高手 X 同时使战士 Y_1和 Y_2服输,即,$\{Y_1=0, Y_2=0\}$。由于 Y_1和 Y_2相互独立,所以,$P(Y_1=0, Y_2=0)=P(Y_1=0)P(Y_2=0)=[P(X_1=1,Y_1=0)+P(X_1=0,Y_1=0)][P(X_2=1,Y_2=0)+P(X_2=0, Y_2=0)]=P(X_1=Z_1)P(X_2=Z_2)$,其中,随机变量 $Z_1=(X_1+Y_1)\bmod 2, Z_2=(X_2+Y_2)\bmod 2$。由于如下两个信道:(1)以 X_1为输入,Z_1为输出,其信道容量记为 C_1;(2)以 X_2为输入,Z_2为输出,其信道容量记为 C_2。根据仙农编码极限定理[11],知道$P(X_1=Z_1)\leqslant C_1$和 $P(X_2=Z_2)\leqslant C_2$,而且,这两个不等式还是可以达到的,于是,$P(Y_1=0, Y_2=0)\leqslant C_1C_2$。因此,我们有:

定理 1　(1 攻 2 的攻击能力极限定理):在 N 个攻防回合中,一个高手最多能够同时把两个战士打败 NC_1C_2次,而且,一定有某种技巧,可以使高手达到该极限。

其实,上面的定理 1 是下面定理 2 的特殊情况,之所以单独将其列出,是因为这个问题在文献[6]中未被解决。

在 1 对 2 情况下,所有可能的"独裁评估"有:$X_1=a$、$X_2=b$、$(X_1,X_2)=(a,b)$、$Y_1=a$、$Y_2=b$、$(Y_1,Y_2)=(a,b)$、$(X_1,Y_2)=(a,b)$、$(X_2,Y_1)=(a,b)$,这里 a 和 b 取值为 0 或 1。由于 X_1与 X_2相互独立,由于 Y_1与 Y_2相互独立,由于 X_1与 Y_2相互独立,由于 Y_1与 X_2相互独立,所以,仿照定理 1 的证明过程,可以得到:

定理 2　(独裁评估的极限):在一个高手 $X=(X_1,X_2)$同时攻击两个战士 Y_1和 Y_2的情况下,在 N 个攻防回合中,有如下极限,而且它们都是可以达到的极限:

(1)$\{X_1=a\}$最多出现 NC_1次,其中,C_1是以 Y_1为输入,以$(X_1+Y_1+a)\bmod 2$为输出的信道容量;

(2)$\{X_2=b\}$最多出现 NC_2次,其中,C_2是以 Y_2为输入,以$(X_2+Y_2+b)\bmod 2$为输出的信道容量;

(3)$\{(X_1,X_2)=(a,b)\}$最多出现 NC_1C_2次,其中 C_1和 C_2如(1)和(2)所述(此时,若 $a=b=1$,则意味着"X 既未被 Y_1打败,也未被 Y_2打败"或者说"X 成功地挡住了 Y_1和 Y_2的攻击"。由于,$P(X_1=0\cup X_2=0)=1-P(X_1=1,X_2=1)\geqslant 1-C_1C_2$,所以,在 N 回合的对抗中,X 被打败至少 $N(1-C_1C_2)$次。这也是文献[6]中研究过的多攻 1 的特例);

(4)$\{Y_1=a\}$最多出现 ND_1次,其中,D_1是以 X_1为输入,以$(X_1+Y_1+a)\bmod 2$为输出的信道容量;

(5)$\{Y_2=b\}$最多出现 ND_2次,其中,D_2是以 X_2为输入,以$(X_2+Y_2+b)\bmod 2$为输出的信道容量;

(6)$\{(Y_1,Y_2)=(a,b)\}$最多出现 ND_1D_2次,其中 D_1和 D_2如(4)和(5)所述(此时,若 $a=b=0$ 的特殊情况,就是定理 1 中的情况);

(7)$\{(X_1,Y_2)=(a,b)\}$最多出现 NC_1D_2次,其中 C_1和 D_2如(1)和(5)所述;

(8)$\{(X_2,Y_1)=(a,b)\}$最多出现 NE_1E_2次。其中,E_1是以 Y_2为输入,以$(X_2+Y_2+a)\bmod 2$为输出的信道容量;E_2是以 X_1为输入,以$(X_1+Y_1+b)\bmod 2$为输出的信道容量。

现在将 1 对 2 的情况推广到 1 对多的星状网络攻防情况。

星状网络的中心点是高手 $X=(X_1,X_2,\cdots,X_m)$,他要同时对抗 m 个战士 $Y_1,Y_2,\cdots,Y_m$(他们对应于星状网的非中心点)。

每个回合后,战士们对自己在本轮攻防中的表现,给出如下保密的不告知任何人的盲自评估:战士 Y_i若自评估自己打败了高手,则记 $Y_i=1$;否则,记 $Y_i=0$ 这里 $1\leqslant i\leqslant m$。

每个回合后,高手 $X=(X_1,X_2,\cdots,X_m)$对自己在本轮攻防中的表现,给出如下保密的不告知任何人的盲自评估:若他在对抗 Y_i时得分为 a_i(这里 $a_i=0$ 时,表示自认为输给了 Y_i;否则,$a_i=1$,即,表示自己战胜了 Y_i),那么,就记 $X_i=a_i, 1\leqslant i\leqslant m$。这时,也可以形象地将高手看成"长了 m 只手:$X_1、X_2,\cdots,X_m$"的大侠。

类似于定理 2,我们有:

定理 3　(星状网络对抗的独裁极限):在一个高手 $X=(X_1,X_2,\cdots,X_m)$同时对抗 m 个战士 $Y_1,Y_2,\cdots,Y_m$的星状网络环境中,所有的独裁评估都可以表示为事件:

$\{[\bigcap\limits_{i\in S}\{X_i=a_i\}]\cap[\bigcap\limits_{j\in R}\{Y_j=b_j\}]\}$,其中 S 和 R 是数集$\{1,2,\cdots,m\}$中的两个不相交子集,即,$S\cap R=\Phi$,$a_i、b_j$取值为 0 或 1$(1\leqslant i,j\leqslant m)$。

而且,独裁评估的概率为 $P(\{[\bigcap\limits_{i\in S}\{X_i=a_i\}]\cap[\bigcap\limits_{j\in R}\{Y_j=b_j\}]\})=\{[\prod\limits_{i\in S}P(\{X_i=a_i\})][\prod\limits_{j\in R}P(\{Y_j=b_j\})]\}\leqslant\prod\limits_{i\in S,j\in R}[C_iD_j]$,这里,$C_i$是以 Y_i为输入,以$(X_i+Y_i+a_i)\bmod 2$为输出的信道的信道容量;D_j是以 X_j为输入,以$(X_j+Y_j+b_j)\bmod 2$为输出的信道的信道容量。而且,该极限是可达的。

换句话说,在星状网络的 N 次攻防对抗中,每个

独裁事件$\{[\underset{i\in S}{\cap}\{X_i=a_i\}]\cap[\underset{j\in R}{\cap}\{Y_j=b_j\}]\}$最多只出现$N\underset{i\in S,j\in R}{\prod}[C_iD_j]$次,而且,这个极限还是可达的。

该定理的证明过程与定理 1 类似,只是注意到如下事实:从随机变量角度来看,当 $i\neq j$ 时,X_i 与 Y_j 相互独立;各 X_i 之间相互独立;各 Y_j 之间也相互独立。定理 3 其实也包含了文献[6]考虑的"1 攻多"和"多攻 1"的情况。

3 榕树网络(Banyan)对抗的输赢次数极限

除了 1 对 1 的单挑、1 对多的星状网络攻防之外,在真实的网络对抗中,还常常会出现集团之间的对抗情况,即,由一群人(比如,北约集团 $X_1,X_1,\cdots,X_n$)去对抗另一群人(比如,华约集团 $Y_1,Y_2,\cdots,Y_m$)。这里,北约集团的成员($X_1,X_1,\cdots,X_n$)之间不会相互攻击;同样,华约集团的成员($Y_1,Y_2,\cdots,Y_m$)之间也不会相互攻击;北约(华约)的每一个成员,都会攻击华约(北约)的每一个成员。因此,对抗的两个阵营,其实就形成了一个榕树网络(Banyan)。为研究简便,假定同一集团成员之间都是独立行事(即,各 X_i 之间相互独立;各 Y_i 之间也相互独立),因为,如果某两个集团成员之间是协同工作的,那么,就可以将它们视为同一个(融合)成员。

仍然采用回合制。仍然假定在每个回合后,各成员都对自己在本轮对抗中的表现,给出一个真心的盲评价。具体地说:

每个北约成员 $X_i(1\leqslant i\leqslant n)$ 都长了 m 只手,即,$X_i=(X_{i1},X_{i2},\cdots,X_{im})$,当他自认为在本轮对抗中打败了华约成员 $Y_j(1\leqslant j\leqslant m)$ 时,就记 $X_{ij}=1$;否则,当他自认为在本轮对抗中输给了华约成员 $Y_j(1\leqslant j\leqslant m)$ 时,就记 $X_{ij}=0$。

同样,每个华约成员 $Y_j(1\leqslant j\leqslant m)$ 也都长了 n 只手,即,$Y_j=(Y_{j1},Y_{j2},\cdots,Y_{jn})$,当他自认为在本轮对抗中打败了北约成员 $X_i(1\leqslant i\leqslant n)$ 时,就记 $Y_{ji}=1$;否则,当他自认为在本轮对抗中输给了北约成员 $X_i(1\leqslant i\leqslant n)$ 时,就记 $Y_{ji}=0$。

类似于定理 3,我们有:

定理 4 (榕树网络对抗的独裁极限):在该榕树网络(Banyan)攻防环境中,所有的独裁评估事件都可表示为:$[\underset{(i,j)\in S}{\cap}\{X_{ij}=a_{ij}\}]\cap[\underset{(j,i)\in R}{\cap}\{Y_{ji}=b_{ji}\}]$。这里 S 和 R 是集合$\{(i,j):1\leqslant i\leqslant n,1\leqslant j\leqslant m\}$中的这样两个子集:当$(i,j)\in S$ 时,一定有"(j,i) 不属于 R";同时,当$(i,j)\in R$ 时,一定有"(j,i) 不属于 S"。而且,独裁评估的概率为 $P([\underset{(i,j)\in S}{\cap}\{X_{ij}=a_{ij}\}]\cap[\underset{(j,i)\in R}{\cap}\{Y_{ji}=b_{ji}\}])=[\underset{(i,j)\in S}{\prod}P\{X_{ij}=a_{ij}\}].[\underset{(j,i)\in R}{\prod}P\{Y_{ji}=b_{ji}\}]\leqslant\underset{(i,j)\in S,(p,q)\in R}{\prod}[C_{ij}D_{pq}]$,这里,$C_{ij}((i,j)\in S)$ 是以 Y_{ji} 为输入,以$(X_{ij}+Y_{ji}+a_{ij})\bmod 2$ 为输出的信道的信道容量;$D_{pq}((p,q)\in R)$ 是以 X_{qp} 为输入,以$(X_{pq}+Y_{pq}+b_{pq})\bmod 2$ 为输出的信道的信道容量。而且,该极限是可达的。

换句话说,在榕树网络的 N 次攻防对抗中,每个独裁事件$\{[\underset{(i,j)\in S}{\cap}\{X_{ij}=a_{ij}\}]\cap[\underset{(j,i)\in R}{\cap}\{Y_{ji}=b_{ji}\}]\}$最多只出现$N\underset{(i,j)\in S,(p,q)\in R}{\prod}[C_{ij}D_{pq}]$次,而且,这个极限还是可达到的。

4 麻将网络对抗的输赢次数极限

一个有 n 个终端的网络中,如果所有这些终端之间都相互攻击,就像打麻将时每个人都"盯上家,卡对家,打下家"一样,那么,这样的攻防场景就称之为麻将网络攻防,或者,更学术一些,叫作"全连通网络攻防"。在实际情况中,这种攻防场景虽然不常见,但是,偶尔还是会出现的。为了学术研究的完整性,我们在此也来介绍一下。

在麻将网络中的 n 个战士,用 $X_1,X_2,\cdots,X_n$ 来表示。每个战士 $X_i(1\leqslant i\leqslant n)$ 都有 n 只手 $X_i=(X_{i1},X_{i2},\cdots,X_{in})$,其中,他的第 $j(1\leqslant j\leqslant n)$ 只手(X_{ij})是用来对付第 j 个战士 X_j 的,而 X_{ii} 这只手是用来保护自己的。

仍然假设他们的攻防是采用回合制,仍然假设他们在每个回合后,都对本轮攻防的效果进行一次只有自己知道的评估,即,

如果战士 X_i 自认为在本回合中打败了战士 $X_j(1\leqslant i\neq j\leqslant n)$,那么,他就记 $X_{ij}=1$;否则,如果他认为输给了战士 X_j,那么,他就记 $X_{ij}=0$。说明:对 X_{ii} 不做任何赋值,因为它对整个攻防不起任何作用,放在这里仅仅是使得相关公式整洁而已。

类似于定理 4,我们有:

定理 5 (麻将网络对抗的独裁极限):在麻将网络攻防环境中,所有的独裁评估事件都可表示为:$\underset{(i,j)\in S}{\cap}\{X_{ij}=a_{ij}\}$,这里,$S$ 是集合$\{(i,j):1\leqslant i\neq j\leqslant n\}$中的一个特殊子集,它满足条件:如果$(i,j)\in S$,那么,一定有"$(j,i)$不属于 S"。而且,独裁评估事件的概率为 $P(\underset{(i,j)\in S}{\cap}\{X_{ij}=a_{ij}\})=\underset{(i,j)\in S}{\prod}P\{X_{ij}=a_{ij}\}\leqslant\underset{(i,j)\in S}{\prod}C_{ij}$,这里,$C_{ij}((i,j)\in S)$ 是以 X_{ji} 为输入,以$(X_{ij}+X_{ji}+a_{ij})\bmod 2$为输出的信道的信道容量。而且,该极限是可达的。换句话说,在麻将网络的 N 次攻防对抗中,每个独裁事件 $\underset{(i,j)\in S}{\cap}\{X_{ij}=a_{ij}\}$ 最多出现$N\underset{(i,j)\in S}{\prod}C_{ij}$次,而且,这个极限还是可达的。

5　结束语

《安全通论》以“建立网络空间安全的统一基础理论”为最高目标,并希望它能够适用于网络空间安全这个一级学科的所有分支。可见,其难度相当大!

仙农是全世界几百年才出一个的神人,他仅凭一己之力,仅凭一篇论文就成功地建立了“信息通信工程学科的统一基础理论”:信息论。恐怕其他人很难再如此神奇,至少老夫我肯定不行!

在整个 IT 界,几乎没有哪门学科的基础理论是由中国人建立的,国人最多只参与了一些局部工作,或者说只啃了一些吃力不讨好的硬骨头。难道中国人真的就没能力创立核心的新学科?我不相信!但是,如果国人连创立新学科的欲望都没有的话,那肯定就没戏了!

横扫当今和可见将来的 IT 界,除了网络空间安全之外,好像还真没有什么别的机会了,因为,诸如信息论、冯.诺伊曼理论、电磁场理论等基础理论,都已经把相关的学科分支统一起来了。唯独网络空间安全的各个分支,到目前为止,还仍然只是一盘散沙,还急需统一的基础理论!

没有仙农那样的天才,那么,我们能否“三个臭皮匠顶个诸葛亮”?!很难像仙农那样,用一篇论文“The Mathematical Theory of Communications”搞定《信息论》,那么,我们能否用一堆论文来搭建《安全通论》?!这就是我到处宣传《安全通论》,并甘当伯乐的原因。我将在不断探索研究《安全通论》的同时,也乐意为所有学者,特别是青年才俊,敞开大门,愿意毫无保留地为大家服务,争取早日完善《安全通论》。

经过前段时间的宣讲,我收集到一些学者的相关疑问,现简要回答如下:

(1)问:《安全通论》存在吗?答:安全的核心是对抗,它也是一种特殊的博弈。既然前人已经能够把广泛的博弈,用很紧凑的《博弈论》给统一起来,那么,从理论上说,《安全通论》的“上界”是存在的,甚至它就是博弈论的某种精练。当然,这种精练绝非易事!另一方面,从本文和已经发表的其他 9 篇文章[1-9],我们至少可以说,《安全通论》的“下界”也是存在的。因此,只要大家一起努力,把“上界”不断压小,把“下界”不断增大,那么,紧凑的《安全通论》就一定能够建成。

(2)问:实际的网络攻防不是回合制呀?答:表面上,现实世界的网络攻防确实不是回合制!但是,设想一下,如果把时间进行必要的局部拉伸和压缩(这样做,对攻防各方来说,并无实质性的改变),那么,所有攻防也都可转化成回合制了。况且,既然《博弈论》都是采用的回合制,那么,作为一种特殊的博弈,为什么安全对抗就不能是回合制呢?理论研究一定要建立相应的模型,一定要抛弃一些不必要的差异和非核心细节,否则,就只能做“能工巧匠”了。采用什么制,并不重要。重要的是,是否能够把所有安全分支给紧凑地统一起来。

(3)问:为什么你只考虑了对抗的输赢次数?答:我承认,对抗中的“输赢次数”只包含了部分输赢信息(比如,一次大赢可能胜过多次小输),但是,在没有能力揭示更多输赢信息的情况下,能“向前迈一步”总好过无所作为。做科研,特别是创立一门新学科,只能步步逼近,至少,我没本事一步登天。

(4)问:《安全通论》完成后,对网络空间安全到底有什么具体的指导价值?答:关键看今后《安全通论》完成后,到底是什么样子。也许它会是安全界的“信息论”,也许一钱不值。但是,如果是后者,就说明网络空间安全根本就是“一堆扶不上墙的烂泥”,我不相信会出现这种情况。当然,你若问我,今后到底如何用《安全通论》去指导安全的各个细枝末叶,那么,我可以告诉你:仙农也不知道如何用《信息论》去指导电视机的生产。

(5)问:实际安全对抗中还有许多诸如模糊性、随机性等因素,你的《安全通论》中为什么没有考虑?答:首先,《安全通论》不是我的,我只是抛了块“砖”,来引各位的“玉”而已;其次,做研究,一定要有所为,有所不为。只要不影响普适性,那么,能够简化的东西都要尽量简化,否则,搞得太复杂,就会无处下手,就很难建立一门紧凑的科学。

(6)问:至今,为什么你竟然没有用到《博弈论》?答:从研究《安全通论》的第一天开始,我就想把《博弈论》当成核心工具,可是,总是事与愿违!这也许有两方面原因:其一,《博弈论》真的不能简单地平移到网络安全对抗中来,虽然我花费了大量的精力和时间来专攻《博弈论》,研读了,包括冯.诺伊曼原著等在内的,近两千页博弈论专著;其二,我的《博弈论》功底还不够深,没能从中找到打开《安全通论》的博弈论金钥匙。因此,我真诚地欢迎博弈论专家,介入《安全通论》。

特别说明:这本该是一篇高影响因子的 SCI 论文,但是,如今国人已被 SCI 绑架了,所以,老夫想带头摆脱 SCI 的束缚,故将此文在这里发表。本文欢迎所有媒体转载。

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] DrewFudenberg, Jean Tirole. 博弈论[M]. 黄涛,郭凯,龚鹏,等译. 北京:中国人民大学出版社,2016.

[11] Thomas M Cover, Joy A Thomas. 信息论基础[M]. 阮吉寿,张华,译. 北京:机械工业出版社,2007.