文章编号：2096-1618(2016)04-0342-06
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-958609.html
发表时间：2016-02-25

安全通论(8)

——黑客篇之“战略研究”

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：对技术水平有限的(经济)黑客来说，他如何通过“田忌赛马”式的组合攻击策略，来实现“黑产收入”最大化呢？是否存在这种最优的攻击组合呢？借助股票投资领域中的相关思路和方法，得到了一些有趣的结果。比如，给出了黑客同时攻击 m 个系统的对数最优攻击组合策略(见定理2)，它不但能使黑客的整体收益最大化，而且还能够使每轮攻击的收益最大化(见定理3)；发现了如果采用对数最优的攻击组合策略，那么，黑客攻击每个系统的“投入产出比”不会在本轮攻击结束后发生变化(见定理3)；如果黑客还能够通过其他渠道获得一些“内部消息”，那么，他因此多获得的“黑产收入”的增长率不超过“被攻击系统的“投入产出比”与“内部消息”之间的互信息”(见定理6)；如果随时间变化的被攻击系统是平稳随机过程，那么，黑客的最优攻击增长率是存在的(见定理7)。总之，熵越小的黑客攻击策略，所获得的“黑产收入”越大！

0　引言

由于政治黑客后台很硬，不计成本，不择手段，耐得住寂寞，因此，从纯技术角度看，政治黑客是最牛的黑客，他们的攻击力远远超过经济黑客等普通黑客。

为了量化分析(因为政治问题无法量化)，文献[7]不得不用“宰牛刀”来“杀鸡”(即，用政治黑客的技术来为经济黑客的利益服务)，给出了最牛黑客的完整静态描述，并且还给出了他们的最佳组合攻击战术。但是，并不是所有黑客都能够达到如此高的技术极限，甚至这样的黑客也许可望而不可即。

幸好，经济黑客的主要目标是获取最大的“黑产收入”，而不是要伤害被攻击系统(政治黑客刚好相反，他的目标是伤害对方，而非获得经济利益)，当然，经济黑客也不会有意去保护对手。所以，经济黑客的技术水平虽然有限，但是，他们可以依据已有的技术水平，像“田忌赛马”那样，通过巧妙地“组合攻击”来尽可能实现收益最大化。

黑客攻击和炒股其实很相像。实际上，政治黑客的攻击就像“庄家炒股”，虽然他对被攻击系统(待炒的股票)的内部情况了如指掌，但是，他的期望值也很高，不出手则已，一旦出手就要摧毁目标(赚大钱)，因此，一旦行动起来，其战术就非常重要，不能有任何细节上的失误，否则前功尽弃。事实证明，“庄家炒股”也有赔钱的时候，同样，政治黑客的攻击也有失手的时候，其主要失败原因，基本上都是“输在战术细节上”。

经济黑客的攻击就像“散户炒股”，虽然整体上处于被动地位，资金实力也很差，但是，自身的期望值并不很高，只要有钱赚，哪怕刚够喝稀饭。经济黑客的攻击(散户的炒股)当然不能靠硬拼，必须讲究战略，比如，1)正确选择被攻击系统(待炒的股票)。目标选错了，当然要赔本；2)合理分配精力去攻击所选系统(炒作所选股票)，既不要“在一棵树上吊死”也不能“小猫钓鱼”(既不能把资金全部投到某一只股票，也不要到处“撒胡椒粉”)。事实证明，散户炒股也有赢钱的时候，只要他很好地运用了相关战略(即，选股选对了，在每只股票上的投资额度分配对了)；同样，经济黑客也有可能获利，如果他正确地把握了相关战略。本文将给出一些确保黑客获利的“对数最优”战略，当然，本文的结果也可帮助散户股民炒股，前提是他们能够读懂此文(我相信普通的经济黑客是可以读懂此文的)。

过去若干年以来，人们已经在投资策略(包括炒股)方面进行了大量研究，并由此丰富了博弈论的内容。本文的许多思想、方法和结果也是来源于这些理论。

1　数最优攻击组合

设黑客想通过攻击某 m 个系统来获取其经济利益，并且根据过去的经验，他攻击第 i 个系统的“投入

产出比”是随机变量 $X_i(\geqslant 0,\ i=1,2,\cdots,m)$,即,攻击第 i 个系统时,若投入 1 元钱,则其收益是 X_i 元钱。记收益列向量 $X=(X_1,X_2,\cdots,X_m)^t$ 服从联合分布 $F(x)$,即,$X\sim F(x)$。

从经济角度看,所谓黑客的一个攻击组合,就是这样一个列向量 $b=(b_1,b_2,\cdots,b_m)^t$,$b_i\geqslant 0$,$\sum b_i=1$,它意指该黑客将其“用于攻击的资金总额”的 b_i 部分,花费在攻击第 i 个系统上($i=1,2,\cdots,m$)。于是,在此组合攻击下,黑客的收益便等于 $S=b^tX=\sum_{i=1}^{m}b_iX_i$。这个 S 显然也是一个随机变量。

当本轮组合攻击完成后,黑客还可以发动第 2 轮、第 3 轮等组合攻击,即,黑客将其上一轮结束时所得到的全部收益,按相同比例 b 分配,形成新一轮的攻击组合 b。下面,我们将努力寻找最佳的攻击组合 b,使得经过 n 轮组合攻击后,黑客的收益 S,在某种意义上达到最大值。

定义 1　攻击组合 b 关于收益分布 $F(x)$ 的增长率,定义为

$$W(b,F)=\int \log(b^tx)\,\mathrm{d}F(x)=E[\log(b^tX)]$$

如果该对数的基底是 2,那么,该增长率 $W(b,F)$ 就称为双倍率(见文献[7])。攻击组合 b 的最优增长率 $W^*(F)$ 定义为

$$W^*(F)=\max_b W(b,F)$$

这里的最大值遍取所有可能的攻击组合 $b=(b_1,b_2,\cdots,b_m)^t$,$b_i\geqslant 0$,$\sum b_i=1$。如果某个攻击组合 b^* 使得增长率 $W(b,F)$ 达到最大值,那么,这个攻击组合就称为“对数最优攻击组合”。

为了简化上角标,本文对 b^* 和 $b(*)$ 交替使用,不加区别。

定理 1　设 $X_1,X_2,\cdots,X_n$ 是服从同一分布 $F(x)$ 的独立同分布随机序列。令 $S_n^*=\prod_{i=1}^{n}b^{*t}X_i$ 是在同一攻击组合 b^* 之下,n 轮攻击之后,黑客的收益,那么,

$$(\log S_n^*)/n\to W^*,\ \text{依概率 1。}$$

证明　由强大数定律可知,

$$(\log S_n^*)/n=[\sum_{i=1}^{m}\log(b^{*t}X_i)]/n\to W^*,\ \text{依概率 1}$$

所以,$S_n^*=2^{nW(*)}$。证毕。

引理 1　$W(b,F)$ 关于 b 是凹函数,关于 F 是线性的,而 $W^*(F)$ 关于 F 是凸函数。

证明　增长率公式为 $W(b,F)=\int\log(b^tx)\,\mathrm{d}F(x)$,由于积分关于 F 是线性的,所以,$W(b,F)$ 关于 F 是线性的。又由于对数函数的凸性,可知,

$$\mathrm{Log}[\lambda b_1+(1-\lambda)b_2]^tX\geqslant\lambda\log(b_1^tX)+(1-\lambda)\ \log(b_2^tX)$$

对该公式两边同取数学期望,便推出 $W(b,F)$ 关于 b 是凹函数。最后,为证明 $W^*(F)$ 关于 F 是凸函数,我们假设 F_1 和 F_2 是收益列向量的两个分布,并令 $b^*(F_1)$ 和 $b^*(F_2)$ 分别是对应于两个分布的最优攻击组合。令 $b^*(\lambda F_1+(1-\lambda)F_2)$ 为对应于 $\lambda F_1+(1-\lambda)F_2$ 的对数最优攻击组合,那么,利用 $W(b,F)$ 关于 F 的线性性,有:

$$\begin{aligned}&W^*(\lambda F_1+(1-\lambda)F_2)\\&=W^*[b^*(\lambda F_1+(1-\lambda)F_2),\ \lambda F_1+(1-\lambda)F_2]\\&=\lambda W^*[b^*(\lambda F_1+(1-\lambda)F_2),F_1]+(1-\lambda)W^*[b^*(\lambda F_1+(1-\lambda)F_2),F_2]\\&\leqslant\lambda W^*[b^*(F_1),F_1]+(1-\lambda)W^*[b^*(F_2),F_2]\end{aligned}$$

因为 $b^*(F_1)$ 和 $b^*(F_2)$ 分别使得 $W(b,F_1)$ 和 $W(b,F_2)$ 达到最大值。证毕。

引理 2　关于某个分布的全体对数最优攻击组合构成的集合是凸集。

证明　令 b_1^* 和 b_2^* 是两个对数最优攻击组合,即 $W(b_1,F)=W(b_2,F)=W^*(F)$。由 $W(b,F)$ 的凹性,可以推出

$$W[\lambda b_1+(1-\lambda)b_2,F]\geqslant\lambda W(b_1,F)+(1-\lambda)W(b_2,F)=W^*(F)$$

也就是说,$\lambda b_1+(1-\lambda)b_2$ 还是一个对数最优的攻击组合。证毕。

令 $B=\{b\in R^m:\ b_i\geqslant 0,\ \sum_{i=1}^{m}b_i=1\}$ 表示所有允许的攻击组合。

定理 2　设黑客欲攻击的 m 个系统的收益列向量 $X=(X_1,X_2,\cdots,X_m)^t$ 服从联合分布 $F(x)$,即 $X\sim F(x)$。那么,该黑客的攻击组合 b^* 是对数最优(即,使得增长率 $W(b,F)$ 达到最大值的攻击组合)的充分必要条件是

当 $b_i^*>0$ 时,$E[X_i/(b^{*t}X)]=1$;

当 $b_i^*=0$ 时,$E[X_i/(b^{*t}X)]\leqslant 1$。

证明　由于增长率 $W(b)=E[\log(b^tX)]$ 是 b 的凹函数,其中 b 的取舍范围为所有攻击组合形成的单纯形。于是,b^* 是对数最优的当且仅当 $W(.)$ 沿着从 b^* 到任意其他攻击组合 b 方向上的方向导数是非正的。于是,对于 $0\leqslant\lambda\leqslant 1$,令 $b_\lambda=(1-\lambda)b^*+\lambda b$,我们可得

$$[\mathrm{d}W(b_\lambda)/\mathrm{d}\lambda]\mid_{\lambda=0+}\leqslant 0,\ b\in B$$

由于 $W(b_\lambda)$ 在 $\lambda=0+$ 处的单边导数为

$$\begin{aligned}&[\mathrm{d}E(\log(b_\lambda^tX))/\mathrm{d}\lambda]\mid_{\lambda=0+}\\&=\lim_{\lambda\to 0}\{E[\log[[(1-\lambda)b^{*t}X+\lambda b^tX][b^{*t}X]]]\}/\lambda\\&=E\{\lim_{\lambda\to 0}\{[\log[1+\lambda[(b^tX)/(b^{*t}X)-1]]]/\lambda\}\}\\&=E[(b^tX)/(b^{*t}X)]-1\end{aligned}$$

这里 $\lambda\to 0$ 表示从正数方向,越来越小地趋于 0。于是,对所有 $b\in B$ 都有:$E[(b'X)/(b^{*t}X)]-1\leqslant 0$。如果从 b 到 b^* 的线段可以朝着 b^* 在单纯形 B 中延伸,那么 $W(b_\lambda)$ 在 $\lambda=0$ 点,具有双边导数且导数为 0,于是,$E[(b'X)/(b^{*t}X)]=1$;否则,$E[(b'X)/(b^{*t}X)]<1$。(注:此定理的更详细证明可参考[8]的定理 16.2.1的证明过程)证毕。

由上面的定理 2,可以得出如下推论:

定理 3 设 $S^*=b^{*t}X$ 是对应于对数最优攻击组合 b^* 的黑客收益,令 $S=b'X$ 是对应于任意攻击组合 b 的随机收益,那么,对所有的 S 有 $E[\log(S/S^*)]\leqslant 0$,当且仅当对所有 S 有 $E(S/S^*)\leqslant 1$

证明 对于对数最优的攻击组合 b^*,由定理 2 可知,对任意 i 有 $E[X_i/(b^{*t}X)]\leqslant 1$。对此式两边同乘 b_i,并且关于 i 求和,可得到

$$\sum_{i=1}^{m}\{b_iE[X_i/(b^{*t}X)]\}\leqslant\sum_{i=1}^{m}b_i=1$$

这等价于 $E[(b'X)/(b^{*t}X)]=E(S/S^*)\leqslant 1$,其逆可由 Jensen 不等式得出,因为,$E[\log(S/S^*)]\leqslant\log[E(S/S^*)]\leqslant\log 1=0$。证毕。

此定理表明,对数最优攻击组合不但能够使得增长率最大化,而且,也能使得每轮攻击的收益比值 $E(S/S^*)$ 最大化。

另外,定理 3 还揭示了一个实事:如果采用对数最优的攻击组合策略,那么,对于每个系统的攻击投入,所获得的收益比例的期望值,不会在此轮攻击结束后而变化。具体地说,假如初始的攻击资金分配比例为 b^*,那么,第一轮攻击后,第 i 个系统的收益与整合攻击组合的收益的比例为 $(b_i^*X_i)/(b^{*t}X)$,其期望为:

$$E[(b_i^*X_i)/(b^{*t}X)]=b_i^*\,E[X_i/(b^{*t}X)]=b_i^*$$

因此,第 i 个系统在本轮攻击结束后的收益,占整个攻击组合收益的比例的数学期望值,与本轮攻击开始时第 i 个系统的攻击投入比例相同。因此,一旦选定按比例进行攻击组合,那么,在随后的各轮攻击中,在期望值的意义下,该攻击组合比例将保持不变。

现在深入分析定理 1 中,n 轮攻击后,黑客的收益情况。令 $W^*=\max_b W(b,F)=\max_b E(\log(b'X))$ 为最大增长率,并用 b^* 表示达到最大增长率的攻击组合。

定义 2 一个因果的攻击组合策略,定义为一列映射 $b_i:R^{m(i-1)}\to B$,其中 $b_i(x_1,x_2,\cdots,x_{i-1})$ 解释为第 i 轮攻击的攻击组合策略。

由 W^* 的定义可以直接得出:对数最优攻击组合使得最终收益的数学期望值达到最大。

引理 3 设 S_n^* 为定理 1 所示的,在对数最优攻击组合 b^* 之下,n 轮攻击后,黑客的收益。又设 S_n 为采用定义 2 中的因果攻击组合策略 b_i,n 轮攻击后黑客的收益。那么,$E(\log S_n^*)=n\,W^*\geqslant E(\log S_n)$。

证明
$$\max E(\log S_n)=\max[E\sum_{i=1}^{n}\log(b_i'X_i)]$$
$$=\sum_{i=1}^{n}\{\max E[\log(b_i'(X_1,X_2,\cdots,X_{i-1})X_i]\}$$
$$=\sum_{i=1}^{n}[E(\log(b^{*t}X_i))]=nW^*$$

此处,第一项和第二项中的最大值(max)是对 b_1,$b_2,\cdots,b_n$ 而取的;第 3 项中的最大值(max)是对 $b_i(X_1,X_2,\cdots,X_{i-1})$ 而取的。可见,最大值恰好是在恒定的攻击组合 b^* 之下达到的。证毕。

到此,我们就知道:由定理 2 中的 b^* 给出的攻击组合,能够使得黑客收益的期望值达到最大值,而且,所得的收益 S_n^* 以高概率在一阶指数下等于 $2^{nW(*)}$。其实,我们还可以得到如下更强的结论。

定理 4 设 S_n^* 和 S_n 如引理 3 所述,那么,依概率 1 有,

$$\limsup_{n\to\infty}\{[\log(S_n/S_n^*)]/n\}\leqslant 0$$

证明 由定理 2 可推出 $E(S_n/S_n^*)\leqslant 1$,从而,由马尔可夫不等式,得到

$Pr(S_n>t_nS_n^*)=Pr[(S_n/S_n^*)>t_n]<1/t_n$,因此,$Pr\{[\log(S_n/S_n^*)]/n>[\log t_n]/n\}\leqslant 1/t_n$

取 $t_n=n^2$,并对所有 n 求和,我们得到

$$\sum_{n=1}^{\infty}Pr\{[\log(S_n/S_n^*)]/n>(2\log n)/n\}\leqslant\sum_{n=1}^{\infty}1/n^2=\pi^2/6$$

利用 Borel-Cantelli 引理,我们有

$Pr\{[\log(S_n/S_n^*)]/n>(2\log n)/n$,无穷多个成立$\}=0$

这意味着,对于被攻击的每个系统向量序列,都存在 N,使得,当 $n>N$ 时,均有 $\log(S_n/S_n^*)]/n<(2\log n)/n$ 成立。于是,依概率 1,成立:$\limsup_{n\to\infty}\{[\log(S_n/S_n^*)]/n\}\leqslant 0$。证毕。

该定理表明,在一阶指数意义下,对数最优攻击组合的表现相当好。

散户炒股都有这样的经验:如果能够搞到某些“内部消息”(学术上称之为“边信息”),那么,炒股赚钱的可能性就会大增;但是,到底能够增加多少呢?下面就来回答这个问题。当然,我们将其叙述为:边信息对黑客收益的可能影响。

定理 5 设 X 服从分布 $f(x)$,而 b_f 为对应于 $f(x)$ 的对数最优攻击组合。设 b_g 为对应于另一个密度函数 $g(x)$ 的对数最优攻击组合。那么,采用 b_f 替代 b_g 所带来的增长率的增量满足如下不等式,$\Delta W=W(b_f,F)-W(b_g,F)\leqslant D(f\mid g)$。这里,$D(f\mid g)$ 表示相对熵(见

文献[8])。

证明　$\Delta W=\int f(x)\log({b_f}^t x)-\int f(x)\log({b_g}^t x)$

$=\int f(x)\{\log[({b_f}^t x)/({b_g}^t x)]\}$

$=\int f(x)\{\log[({b_f}^t x)/({b_g}^t x)][g(x)/f(x)][f(x)/g(x)]\}$

$=\int f(x)\{\log[({b_f}^t x)/({b_g}^t x)][g(x)/f(x)]\}+D(f\mid g)$

$\leqslant\log\{\int f(x)[({b_f}^t x)g(x)][({b_g}^t x)f(x)]\}+D(f\mid g)$

$=\log[\int g(x)({b_f}^t x)/({b_g}^t x)]+D(f\mid g)$

$\leqslant\log 1+D(f\mid g)=D(f\mid g)$。证毕。

定理 6　由边信息 Y 所带来的增长率的增量 ΔW 满足如下不等式,$\Delta W\leqslant I(X;Y)$。这里 $I(X;Y)$ 表示随机变量 X 与 Y 之间的互信息。

证明　设 (X,Y) 服从分布 $f(x,y)$,其中 X 是被攻击系统的"投入产出比"向量,而 Y 是相应的边信息。当已知边信息 $Y=y$ 时,黑客采用关于条件分布 $f(x\mid Y=y)$ 的对数最优攻击组合,从而,在给定条件 $Y=y$ 下,利用定理 5,可得,

$$\Delta W_{Y=y}\leqslant D[f(x\mid Y=y)\mid f(x)]=\int_x f(x\mid Y=y)\log[(f(x\mid Y=y))/f(x)]\mathrm{d}x$$

对 Y 的所有可能取值进行平均,得到

$$\Delta W\leqslant\int_y f(y)\{\int_x f(x\mid Y=y)\log[(f(x\mid Y=y))/f(x)]\mathrm{d}x\}\mathrm{d}y$$

$$=\int_y\int_x f(y)f(x\mid Y=y)\log[(f(x\mid Y=y))/f(x)][f(y)/f(y)]\mathrm{d}x\mathrm{d}y$$

$$=\int_y\int_x f(x,y)\log\{f(x,y)[f(x)f(y)]\}\mathrm{d}x\mathrm{d}y$$

$=I(X;Y)$。从而,边信息 Y 与被攻击的系统向量序列 X 之间的互信息 $I(X;Y)$ 是增长率的增量的上界。证毕。

该定理 6 形象地告诉我们,"内部消息"能够使黑客的"黑产收益"增长率的精确上限,不会超过 $I(X;Y)$。

下面再考虑被攻击系统,依时间而变化的情况。

设 $X_1,X_2,\cdots,X_n,\cdots$ 为向量值随机过程,即,X_i 为第 i 时刻被攻击系统向量,或者说 $X_i=(X_{1i},X_{2i},\cdots,X_{mi})$,$i=1,2,3,\cdots$,其中 $X_{ji}\geqslant 0$ 是第 i 时刻攻击第 j 个系统时的"投入产出比"。下面的攻击策略是以因果方式,依赖于过去的历史数据,即,b_i 可以依赖于 $X_1,X_2,\cdots,X_{i-1}$。令 $S_n=\prod_{i=1}^{n}{b_i}^t(X_1,X_2,\cdots,X_{i-1})X_i$,黑客的目标显然就是要使整体"投入产出比"达到最大化,即,让 $E\log S_n$ 在所有因果组合攻击策略集 $\{b_i(.)\}$ 上达到最大值。而此时,

$$\mathrm{Max}[E\log S_n]=\sum_{i=1}^{n}\mathrm{Max}\{E({\log b_i}^t X_i)\}=\sum_{i=1}^{n}E[\log({b^*}_i^t X_i)]$$

其中,b_i^* 是在已知过去"黑产收入"的历史数据下,X_i 的条件分布的对数最优攻击组合,换言之,如果记条件最大值为

$$\mathrm{Max}_b\{E[\log b^t X_i\mid(X_1,X_2,\cdots,X_{i-1})=(x_1,x_2,\cdots,x_{i-1})]\}=W^*(X_i\mid x_1,x_2,\cdots,x_{i-1})$$

则 $b_i^*(x_1,x_2,\cdots,x_{i-1})$ 就是达到上述条件最大值的攻击组合。关于过去期望值,我们记 $W^*(X_i\mid X_1,X_2,\cdots,X_{i-1})=E_{\max_b}E[\log b^t X_i\mid X_1,X_2,\cdots,X_{i-1}]$,并称之为条件增长率,这里的最大值函数是取遍所有定义在 $X_1,X_2,\cdots,X_{i-1}$ 上的攻击组合 b 的"攻击组合价值函数"。于是,如果在每一阶段中,均采取条件对数最优的攻击组合策略,那么,黑客的最高期望对数回报率(投入产出率)是可以实现的。令,

$$W^*(X_1,X_2,\cdots,X_n)=\max_b E\log S_n$$

其中最大值取自所有因果攻击组合策略。此时,由,$\log S_n^*=\sum_{i=1}^{n}{\log b_i}^{*t}X_i$,可以得到如下关于 W^* 的链式法则:

$$W^*(X_1,X_2,\cdots,X_n)=\sum_{i=1}^{n}W^*(X_i\mid X_1,X_2,\cdots,X_{i-1})$$

该链式法则,在形式上与熵函数 H 的链式法则完全一样(见文献[8])。确实,在某些方面 W 与 H 互为对偶,特别地,条件作用使 H 减小,而使 W 增长,换句话说:熵 H 越小的黑客攻击策略,所获得的"黑产收入"越大!

定义 3　(随机过程的熵率):如果存在如下极限,

$$W_\infty^*=\lim_{\to\infty}[W^*(X_1,X_2,\cdots,X_n)]/n$$

那么,就称该极限 W_∞^* 为增长率。

定理 7　如果黑客"投入产出比"形成的随机过程 $X_1,X_2,\cdots,X_n,\cdots$ 为平稳随机过程,那么,黑客的最优攻击增长率存在,并且等于

$$W_\infty^*=\lim_{\to\infty}W^*(X_n\mid X_1,X_2,\cdots,X_{n-1})$$

证明　由随机过程的平稳性可知,$W^*(X_n\mid X_1,X_2,\cdots,X_{n-1})$ 关于 n 是非减函数,从而,其极限是必然存在的,但是,有可能是无穷大。但是,由于,

$$[W^*(X_1,X_2,\cdots,X_n)]/n=[\sum_{i=1}^{n}W^*(X_i\mid X_1,X_2,\cdots,X_{i-1})]/n$$

故,根据 Cesaro 均值定理(见文献[8]的定理 4.2.3),可以推出上式左边的极限值等右边通项的极限值。因此,W_∞^* 存在,并且,

$$W_\infty^*=\lim_{\to\infty}[W^*(X_1,X_2,\cdots,X_n)]/n=\lim_{\to\infty}W^*(X_n\mid X_1,X_2,\cdots,X_{n-1})$$

证毕。

在平稳随机过程的情况下,还有如下的渐近最优特性,即,

定理 8 对任意随机过程$\{X_i\}$,$X_i \in R_+^m$,$b_i^*(X^{i-1})$为条件对数最优的攻击组合,而S_n^*为对应的相对"黑产收益"。令S_n为对应某个因果攻击组合策略$b_i(X^{i-1})$的相对收益。那么,关于由过去的$X_1, X_2, \cdots, X_n$生成的σ代数序列,比值S_n/S_n^*是一个正上鞅。从而,存在一个随机变量V使得

$S_n/S_n^* \to V$,依概率 1

$EV \leqslant 1$,且 $Pr\{\sup_n[S_n/S_n^*] \geqslant t\} \leqslant 1/t$

证明 S_n/S_n^*为正上鞅是因为使用关于条件对数最优攻击组合(定理 2),可得

$$
\begin{aligned}
&E\{[(S_{n+1}(X^{n+1}))/(S_{n+1}^*(X^{n+1}))] \mid X^n\}\\
&=E\{[[(b_{n+1}^t X_{n+1})S_n(X^n)][(b_{n+1}^{*t}X_{n+1})\\
&\quad S_n^*(X^n)]] \mid X^n\}\\
&=\{S_n(X^n)/S_n^*(X^n)\}E\{[(b_{n+1}^t X_{n+1})/(b_{n+1}^{*t}X_{n+1})]\\
&\quad \mid X^n\}\\
&\leqslant S_n(X^n)/S_n^*(X^n)
\end{aligned}
$$

于是,利用鞅收敛定理(见文献[8]),得知S_n/S_n^*的极限存在,记为 V,那么,$EV \leqslant E(S_0/S_0^*)=1$。最后,利用关于正鞅的科尔莫戈罗夫不等式,便得到了关于$\sup_n[S_n/S_n^*]$的结果。证毕。

2 结束语

至此,《安全通论》的三块基石(安全经络、安全攻防、黑客本质)就基本奠定。

接下来将努力探索《安全通论》的另一个重要篇章,即,第四块基石:红客篇。虽然,红客是被黑客逼出来的,但是,毕竟红客是"女一号"(如果把黑客看成"男一号"的话),因此,也需要对他进行深入研究。

到现在为止,《安全通论》的基本架构已经显现出来了。当然,还有许多更细致的工作要做,特别是,如何用《安全通论》去指导网络空间安全的技术与实践,即要使《安全通论》"落地",这当然需要安全界全体同仁的共同努力。

回过头来看考查《安全通论》(1)至(7)时,我们发现了一个很奇怪的现象,即,在《安全通论》的全部成果中(文献[1]-[7]),总有一个"幽灵"始终挥之不去。这个"幽灵"便是"熵"! 其实,在《安全通论》的研究过程中,我们并未刻意依赖(或回避)"熵",但是,这个"熵"却总是要主动跳出来,这到底是为什么呢?是必然还是偶然?

下面,我们试图来回答这个问题,特别是把"熵"和老子的"道"[9]放在一起进行比较。

"熵"是什么? 在化学及热力学中,"熵"是"在动力学方面不能做功的能量";最形象的"熵"定义为"热能除以温度",它标志热量转化为功的程度。在自然科学中,"熵"表示系统的不确定(或失序)程度。在社会科学中,"熵"用来借喻人类社会某些混乱状态的程度。在传播学,"熵"表示情境的不确定性和无组织性。根据文献[1],"安全"也是一种"负熵",或"不安全"是一种"熵"。在信息论中,"熵"表示不确定性的量度,即,"信息"是一种"负熵",是用来消除不确定性的东西。总之,"熵"存在于一切系统之中,而且,在不同的系统中,其表现形式也各不相同。其实,老子的"道"(见文献[9])也是这样的,即,

天地初之"道",称为"无";万物母之"道",称为"有";"有"与"无"相生。"道"体虚空,功用无穷;"道"深如渊,万物之源;"道"先于一切有形。"道"体如幽悠无形之神,是最根本的母体,也是天地之本源。"道"隐隐约约,绵延不绝,用之不竭。"道"具无形之形,无象之象,恍恍惚惚;迎面不见其首,随之不见其后。幽幽冥冥,"道"中有核,其核真切,核中充实。对"道"而言,尝之无味,视之无影,听之无声,但是,却用之无穷。天得道,则清静;地得道,则安宁;神得道,则显灵;虚谷得道,则流水充盈;万物得道,则生长;侯王得道,则天下正。"道"很大,大得无外;"道"很小,小得无内。

"熵"都有哪些特点? 在热力学中,"熵"的特征由热量表现,即,热量不可能自发地从低温物体传到高温物体;在绝热过程中,系统的"熵"总是越来越大,直到"熵"值达到最大值,此时系统达到平衡状态。从概率论的角度来看,系统的"熵"值,直接反映了它所处状态的均匀程度,即,系统的熵值越小,它所处的状态就越有序,越不均匀;系统的熵值越大,它所处的状态就越无序,越均匀。系统总是力图自发地从熵值较小的状态向熵值较大(即从有序走向无序)的状态转变,这就是封闭系统"熵值增大原理"。从社会学角度来看,"熵"就是社会生存状态及社会价值观,它的混乱程度将不断增加;现代社会中恐怖主义肆虐,疾病疫病流行,社会革命,经济危机爆发周期缩短,人性物化等都是社会"熵"增加的表征。从宇宙论角度看,"熵"值增大的表现形式是:在整个宇宙当中,当一种物质转化成另外一种物质之后,不仅不可逆转物质形态,而且会有越来越多的能量变得不可利用,宇宙本身在物质的增殖中走向"热寂",走向一种缓慢的"熵"值不断增加的死亡。总之,"熵"的有效性始终在不断地减少,这是一种"反动",与"道者反之动"完全吻合,即,

“道”被荒废后,才出现仁义。智慧出来后,才滋生伪诈。六亲不和,才倡导孝慈。国家昏乱,才需要忠臣。失“道”后,才用德;失德后,才用仁;失仁后,才用义;失义后,才用礼;失礼后,才用法。

若将物质看成“道体”,将能量看成“道用”,将熵看成“道动”,那么,老子在2500多年撰写的《道德经》就已活灵活现地,描绘了宇宙大爆炸学说。因此,我们再结合宇宙爆炸学说,对比一下老子的“道”:“道”是一种混沌物,它先天地而生,无声无形,却独立而不改变;周而复始不停息。它可做天地之母,“道”在飞速膨胀,膨胀至无际遥远;远至无限后,又再折返。“道”生宇宙之混沌元气,元气生天地,天地生阳气、阴气、阴阳合气,合气生万物。

综上所述,“熵”在哲学中,就变为“道”;“道”在科学中,就变成“熵”。由于“道生一,一生二,二生三,三生万物”,即“道”能生万物,那么,“道”生《安全通论》也就名正言顺了。这也许就是“熵”的身影在《安全通论》中始终挥之不去的本质原因吧。

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,2015-12-08.

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

[9] 杨义先. 最形似的《道德经》[EB/OL]. http://blog. sciencenet. cn/blog-453322-845400. html.