文章编号：2096-1618(2016)02-0126-04
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-949155.html
发表时间：2016-01-09

《安全通论》(4)

——攻防篇之“非盲对抗”之“童趣游戏”

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：本文继续利用《安全通论》这个“高大上”工具，来玩两个家喻户晓的童趣游戏：“猜正反面游戏”和“手心手背游戏”。当然，这些成果理所当然地，也成为了《安全通论》攻防篇之“非盲对抗”的重要内容。之所以用游戏方式来表述，只不过是为了增加趣味性，寓庄于谐，让大家体会一下“如何用大炮打蚊子”而已。其实，能打中蚊子的大炮，才是好大炮！

0　引言

以“网络空间安全”、“经济安全”、“领土安全”为代表的所有安全问题的核心，就是“对抗”！所以，多花一些篇幅，从不同角度，甚至利用古老游戏，来全面深入地研究安全对抗问题，是值得的。

“安全经络”(文献[1])是《安全通论》的第一块基石。“安全对抗”是《安全通论》的第二块基石。为了打好这第二块基石，我们在文献[2]中，研究了两大安全对抗之一(盲对抗)，并给出了黑客(红客)攻击(防守)能力的精确极限；并在文献[3]中，以著名的“石头剪刀布游戏”为对象，研究了另一种安全对抗(非盲对抗)，给出了输赢极限和获胜技巧。

与“盲对抗”相比，虽然一般来说，“非盲对抗”不那么血腥，但是，这绝不意味着“非盲对抗”就容易研究，相反，“非盲对抗”的胜败规则等更加千变万化。由于“非盲对抗”的外在表现形式千差万别，所以此文中，我们再利用信道容量法，来研究两个家喻户晓的“非盲对抗”童趣游戏：“猜正反面游戏”和“手心手背游戏”。

1　“猜正反面游戏”的信道容量法

猜正反面游戏：“庄家”用手把一枚硬币掩在桌上，“玩家”来猜是“正面”还是“反面”。若猜中，则“玩家”赢；若猜错，则“庄家”赢。

这个游戏显然是一种“非盲对抗”。他们到底会谁输，谁赢呢？他们怎样才能赢呢？下面就用看似毫不相关的“信道容量法”，来回答这些问题。

由概率论中的大数定律，频率趋于概率，所以，根据“庄家”和“玩家”的习惯，即，过去的统计规律，就可以分别给出他们的概率分布：

用随机变量 X 代表“庄家”，当他把“正面”向上时，记为 $X=0$；否则，记为 $X=1$。所以，“庄家”的习惯就可以用 X 的概率分布来描述，比如，$P_r(X=0)=p$，$P_r(X=1)=1-p$。$1<p<1$。

用随机变量 Y 代表“玩家”，当他猜“正面”时，记为 $Y=0$；否则，记为 $Y=1$。所以，“玩家”的习惯就可以用 Y 的概率分布来描述，比如，$P_r(Y=0)=q$，$P_r(Y=1)=1-q$。$1<q<1$。

同样，根据过去“庄家”和“玩家”的记录，可以知道随机变量 (X,Y) 的联合概率分布，比如：

$$P_r(X=0,Y=0)=a;$$
$$P_r(X=0,Y=1)=b;$$
$$P_r(X=1,Y=0)=c;$$
$$P_r(X=1,Y=1)=d。$$

这里各个参数 $0<p,q,a,b,c,d<1$ 并且还满足如下三个关系式：

$$a+b+c+d=1;$$
$$p=P_r(X=0)=P_r(X=0,Y=0)+P_r(X=0,Y=1)=a+b;$$
$$q=P_r(Y=0)=P_r(X=0,Y=0)+P_r(X=1,Y=0)=a+c。$$

考虑信道 $(X;Y)$，即，以 X 为输入，以 Y 为输出的信道，称之为“庄家信道”。

由于有事件等式：$\{\text{玩家猜中}\}=\{X=0,Y=0\}\cup\{X=1,Y=1\}=\{1$ 比特信息被从“庄家信道”的发送端 X 成功地传输到了收信端 $Y\}$，所以，“玩家”每赢一次，就相当于“庄家信道”成功地传输了 1 比特信息。由此，再结合仙农信息论的著名“信道编码定理”[4][5]：如果“庄家信道”的容量为 C，那么，对于任意传输率 $k/n\leqslant C$，都可以在译码错误概率任意小的情况下，通过某个 n 比特长的码字，成功地把 k 个比特传输

到收信端。反过来,如果“庄家信道”能够用 n 长码字,把 S 个比特无误差地传输到收端,那么,一定有 $S \leqslant nC$。把这段话翻译一下,便有如下定理:

定理 1(庄家定理) 设由随机变量$(X;Y)$组成的“庄家信道”的信道容量为 C。那么,(1)如果玩家想胜 k 次,那么,一定有某种技巧(对应于仙农编码),使得他能够在 k/C 次游戏中,以任意接近 1 的概率达到目的。反过来,(2)如果玩家在 n 次游戏中,赢了 S 次,那么,一定有 $S \leqslant nC$。

由定理 1 可知,只要求出“庄家信道”的信道容量 C,那么,玩家获胜的极限就确定了。下面来求“庄家信道”的转移概率矩阵 $\mathbf{A}=[A(i,j)]$, $i,j=0,1$:

$A(0,0)= P_r(Y=0 \mid X=0)= P_r(Y=0,X=0)/ P_r(X=0)=a/p$;

$A(0,1)= P_r(Y=1 \mid X=0)= P_r(Y=1,X=0)/ P_r(X=0)=b/p=1-a/p$;

$A(1,0)= P_r(Y=0 \mid X=1)= P_r(Y=0,X=1)/ P_r(X=1)=c/(1-p)=(q-a)/(1-p)$;

$A(1,1)= P_r(Y=1 \mid X=1)= P_r(Y=1,X=1)/ P_r(X=1)=d/(1-p)=1-(q-a)/(1-p)$

于是,X 与 Y 之间的互信息 $I(X,Y)$ 等于

$$
\begin{aligned}
&I(X,Y)\\
&=\sum_x\sum_Y p(X,Y)\log(p(X,Y)/[p(X)p(Y)])\\
&=a\log[a/(pq)]+b\log[b/[p(1-q)]]\\
&+c\log[c/[(1-p)q]]+d\log[d/[(1-p)(1-q)]]\\
&=a\log[a/(pq)]+(p-a)\log[(p-a)/[p(1-q)]]\\
&+(q-a)\log[(q-a)/[(1-p)q]]+(1+a-p-q)\log[(1+a-p-q)/[(1-p)(1-q)]]
\end{aligned}
$$

所以,“庄家信道”的信道容量 C 就等于 $\mathrm{Max}[I(X,Y)]$(这里的最大值是对所有可能的二元随机变量 X 来取的),或者,更简单地说,$C=\mathrm{Max}[I(X,Y)]_{0<a,p<1}$(这里的 $I(X,Y)$ 就是上面的互信息公式,而最大值是对满足条件 $0<a,p<1$ 的自然数而取的。注意:这时 q 是当作一个常量来对待的)。可见,“庄家信道”的信道容量 C 是 q 的函数,记为 $C(q)$。

设随机变量 $Z=(X+1)\bmod 2$。下面再考虑另一个信道,$(Y;Z)$,它以 Y 为输入,以 Z 为输出。称该信道为“玩家信道”。

由于有事件等式:$\{$庄家赢$\}=\{Y=0,X=1\}\cup\{Y=1,X=0\}=\{Y=0,Z=0\}\cup\{Y=1,Z=1\}=\{1$ 比特信息被从“玩家信道”的发送端 Y 成功地传输到了收信端 $Z\}$,所以,“庄家”每赢一次,就相当于“玩家信道”成功地传输了 1 比特信息。由此,再结合仙农信息论的著名“信道编码定理”[4][5]:如果“玩家信道”的容量为 D,那么,对于任意传输率 $k/n \leqslant D$,都可以在译码错误概率任意小的情况下,通过某个 n 比特长的码字,成功地把 k 个比特传输到收信端。反过来,如果“玩家信道”能够用 n 长码字,把 S 个比特无误差地传输到收端,那么,一定有 $S \leqslant nD$。把这段话翻译一下,便有如下定理:

定理 2(玩家定理) 设由随机变量$(Y;Z)$组成的“玩家信道”的信道容量为 D。那么,(1)如果庄家想胜 k 次,那么,一定有某种技巧(对应于仙农编码),使得他能够在 k/D 次游戏中,以任意接近 1 的概率达到目的。反过来,(2)如果庄家在 n 次游戏中,赢了 S 次,那么,一定有 $S \leqslant nD$。

由定理 2 可知,只要求出“玩家信道”的信道容量 D,那么,庄家获胜的极限就确定了。

与上面求“庄家信道”的步骤类似,我们可以求出“玩家信道”的信道容量 $D=\mathrm{Max}[I(Y,Z)]_{0<a,q<1}$(这里最大值是对满足条件 $0<a,q<1$ 的自然数而取的,而 $I(Y,Z)$ 如下面公式所示。注意:这时 p 是当作一个常量来对待的)。可见,“玩家信道”的信道容量 D 是 p 的函数,记为 $D(p)$。

$$
\begin{aligned}
&I(Y,Z)\\
&=\sum_Y\sum_Z p(Y,Z)\log(p(Y,Z)/[p(Y)p(Z)])\\
&=a\log[a/(pq)]+(p-a)\log[(p-a)/[p(1-q)]]\\
&+(q-a)\log[(q-a)/[(1-p)q]]+(1+a-p-q)\log[(1+a-p-q)/[(1-p)(1-q)]]
\end{aligned}
$$

结合定理 1 和定理 2,我们便可以对“庄家和玩家的最终输赢情况”以及“玩家和庄家的游戏技巧”,给出一个量化的结果,即,

定理 3(实力定理) 在“猜正反面游戏”中,如果“庄家信道”和“玩家信道”的信道容量分别是 $C(q)$ 和 $D(p)$,那么,

情况 1:如果庄家和玩家都是老实人,即,他们在游戏过程中不试图去调整自己的习惯,即,p 和 q 都恒定不变。那么,如果 $C(q)$ 大于 $D(p)$,则,总体上玩家会赢;如果 $C(q)$ 小于 $D(p)$,则,总体上庄家赢;如果 $C(q)=D(p)$,则,总体上玩家和庄家持平。

情况 2:如果庄家和玩家中的某一方(比如,玩家)是老实人,但是,另一方(比如,庄家)却不老实,他会悄悄调整自己的习惯,即,改变随机变量 X 的概率分布 p,使得“玩家信道”的 $D(p)$ 变大,并最终大于“庄家信道”的 $C(q)$,那么,庄家将整体上赢得该游戏。反之亦然,即,若只有庄家是老实人,那么,玩家也可以通过调整自己的习惯,即,调整 Y 的概率分布 q,使得“庄家信道”的 $C(q)$ 变大,并最终大于“玩家信道”的 $D(p)$,那么,玩家将整体上赢得该游戏。

情况 3:如果玩家和庄家都不是老实人,他们都在不断地调整自己的习惯,使 $C(q)$ 和 $D(p)$ 不断变大,出现“水涨船高”的态势,那么,最终他们将在 $p=q=0.5$ 的地方,达到动态平衡,此时他们都没有输赢。“猜正反面游戏”出现“握手言和”的局面。

2 “手心手背游戏”的信道容量法

手心手背游戏:三个小朋友,同时亮出自己的“手心”或“手背”,如果其中某个小朋友的手势与别人的相反(比如,别人都出“手心”,他却出“手背”),那么,他在本次游戏中就赢了。

这个家喻户晓的游戏,显然也是一种“非盲对抗”,只不过相互对抗的是三人而非常见的二人。他们到底会谁输,谁赢呢? 他们怎样才能赢呢? 下面仍然用“信道容量法”,来回答这些问题。

由概率论中的大数定律,频率趋于概率,所以,根据甲、乙、丙过去习惯的统计规律,就可以分别给出他们的概率分布:

用随机变量 X 代表甲,当他出“手心”时,记为 $X=0$;出“手背”时,记为 $X=1$。所以,甲的习惯就可以用 X 的概率分布来描述,比如,$P_r(X=0)=p$,$P_r(X=1)=1-p$。$1<p<1$。

用随机变量 Y 代表乙,当他出“手心”时,记为 $Y=0$;出“手背”时,记为 $Y=1$。所以,乙的习惯就可以用 Y 的概率分布来描述,比如,$P_r(Y=0)=q$,$P_r(Y=1)=1-q$。$1<q<1$。

用随机变量 Z 代表丙,当他出“手心”时,记为 $Z=0$;出“手背”时,记为 $Z=1$。所以,丙的习惯就可以用 Z 的概率分布来描述,比如,$P_r(Z=0)=r$,$P_r(Z=1)=1-r$。$1<r<1$。

同样,由大数定律的“频率趋于概率”可知,先让甲乙丙三个小朋友玩一段时间后,根据他们的游戏结果情况,就可以知道随机变量(X,Y,Z)的联合概率分布,比如,

P_r(甲手心,乙手心,丙手心)$=P_r(X=0,Y=0,Z=0)=a$;

P_r(甲手心,乙手心,丙手背)$=P_r(X=0,Y=0,Z=1)=b$;

P_r(甲手心,乙手背,丙手心)$=P_r(X=0,Y=1,Z=0)=c$;

P_r(甲手心,乙手背,丙手背)$=P_r(X=0,Y=1,Z=1)=d$;

P_r(甲手背,乙手心,丙手心)$=P_r(X=1,Y=0,Z=0)=e$;

P_r(甲手背,乙手心,丙手背)$=P_r(X=1,Y=0,Z=1)=f$;

P_r(甲手背,乙手背,丙手心)$=P_r(X=1,Y=1,Z=0)=g$;

P_r(甲手背,乙手背,丙手背)$=P_r(X=1,Y=1,Z=1)=h$。

这里各个参数 $0<p,q,r,a,b,c,d,e,f,g,h<1$ 并且还满足如下四个关系式(所以,其实只有 7 个独立变量):

$$a+b+c+d+e+f+g+h=1;$$

$$p=P_r(\text{甲手心})=P_r(X=0)=a+b+c+d;$$

$$q=P_r(\text{乙手心})=P_r(Y=0)=a+b+e+f;$$

$$r=P_r(\text{丙手心})=P_r(Z=0)=a+c+e+g.$$

设随机变量 $M=(X+Y+Z)\bmod 2$,于是,M 的概率分布为:

$$P_r(M=0)$$

$$=P_r(X=0,Y=0,Z=0)+P_r(X=0,Y=1,Z=1)+P_r(X=1,Y=1,Z=0)+P_r(X=1,Y=0,Z=1)$$

$$=a+d+g+f$$

$$P_r(M=1)$$

$$=P_r(X=0,Y=0,Z=1)+P_r(X=0,Y=1,Z=0)+P_r(X=1,Y=0,Z=0)+P_r(X=1,Y=1,Z=1)$$

$$=b+c+e+h$$

再考虑信道(X,M),即,以 X 为输入,以 M 为输出的信道,称之为“甲信道”。

若剔除三个小朋友的手势相同的情况,那么,由于有事件等式:

$$\{\text{甲赢}\}=\{\text{甲手心,乙手背,丙手背}\}\cup\{\text{甲手背,乙手心,丙手心}\}=\{X=0,Y=1,Z=1\}\cup\{X=1,Y=0,Z=0\}=\{X=0,M=0\}\cup\{X=1,M=1\}=\{1\text{ 比特的信息被成功地在“甲信道”中,从发端}(X)\text{传输到收端}(M)\}。$$

反过来,在剔除三个小朋友的手势相同的情况后,若$\{1$ 比特的信息被成功地在“甲信道”中,从发端(X)传输到收端$(M)\}$,那么,就有$\{X=0,M=0\}\cup\{X=1,M=1\}=\{X=0,Y=1,Z=1\}\cup\{X=1,Y=0,Z=0\}=\{\text{甲手心,乙手背,丙手背}\}\cup\{\text{甲手背,乙手心,丙手心}\}=\{\text{甲赢}\}$。所以,甲每赢一次,就相当于“甲信道”成功地把 1 比特信息,从发端 X 传输到了收端 M。由此,再结合仙农信息论的著名“信道编码定理”[4][5]:如果“甲信道”的容量为 E,那么,对于任意传输率 $k/n\leqslant E$,都可以在译码错误概率任意小的情况下,通过某个 n 比特长的码字,成功地把 k 个比特传输到收信端。反过来,如果“甲信道”能够用 n 长码字,把 S 个比特无误差地传输到收端,那么,一定有 $S\leqslant nE$。把这段话翻译一下,便有如下定理:

定理 4 设由随机变量$(X;M)$组成的“甲信道”的信道容量为 E。那么,在剔除平局(即三人的手势相同)的情况下,(1)如果甲想赢 k 次,那么,一定有某种技巧(对应于仙农编码),使得他能够在 k/E 次游戏中,以任意接近 1 的概率达到目的。反过来,(2)如果甲在 n 次游戏中,赢了 S 次,那么,一定有 $S\leqslant nE$。

为了计算信道$(X;M)$的信道容量,首先来计算随机变量(X,M)的联合概率分布:

$P_r(X=0,M=0)=P_r(X=0,Y=0,Z=0)+P_r(X=0,Y=1,Z=1)=a+d$;

$P_r(X=0,M=1)=P_r(X=0,Y=1,Z=0)+P_r(X=0,Y=0,Z=1)=c+b$;

$P_r(X=1,M=0)=P_r(X=1,Y=1,Z=0)+P_r(X=1,Y=0,Z=1)=g+f$;

$P_r(X=1,M=1)=P_r(X=1,Y=0,Z=0)+P_r(X=1,Y=1,Z=1)=e+h$.

所以,随机变量 X 和 M 之间的互信息就等于:

$$\begin{aligned}&I(X,M)\\&=(a+d)\log[(a+d)/[p(a+d+g+f)]]+(g+f)\log[(g+f)/[(1-p)(a+d+g+f)]]\\&+(c+b)\log[(c+b)/[p(b+c+e+h)]]+(e+h)\log[(e+h)/[(1-p)(b+c+e+h)]]\\&=(a+d)\log[(a+d)/[p(a+d+g+f)]]+(g+f)\log[(g+f)/[(1-p)(a+d+g+f)]]\\&+(p-a-d)\log[(p-a-d)/[p(1-(a+d+f+g))]]\\&+(1-(p+f+g))\log[(1-(p+f+g))/[(1-p)(1-(a+d+f+g))]]\end{aligned}$$

于是,“甲信道”的信道容量就等于 $E=Max[I(X,M)]$,这里的最大值是针对自然数 $0<a,d,f,g,p<1$ 来取的。这时,q 和 r 已经当作定量,而非变量来处理了,所以,“甲信道”的信道容量其实是 q 和 r 的函数,记为 $E(q,r)$。

再考虑信道 (Y,M),即以 Y 为输入,以 M 为输出的信道,称之为“乙信道”。由于在“手心手背”游戏中,甲乙丙的地位是相同的,所以,仿照定理 4,就有:

定理 5　设由随机变量 $(Y;M)$ 组成的“乙信道”的信道容量为 F。那么,在剔除平局(即三人的手势相同)的情况下,(1)如果乙想赢 k 次,那么,一定有某种技巧(对应于仙农编码),使得他能够在 k/F 次游戏中,以任意接近 1 的概率达到目的。反过来,(2)如果乙在 n 次游戏中,赢了 S 次,那么,一定有 $S\leqslant nF$。

关于信道容量 F 的值,可以完全仿照 E 值来计算,不过,“乙信道”的容量其实是 p 和 r 的函数,可以记为 $F(p,r)$。

同样,再考虑信道 (Z,M),即以 Z 为输入,以 M 为输出的信道,称之为“丙信道”。由于在“手心手背”游戏中,甲乙丙的地位是相同的,所以,仿照定理 4,就有:

定理 6　设由随机变量 $(Z;M)$ 组成的“乙信道”的信道容量为 G。那么,在剔除平局(即三人的手势相同)的情况下,(1)如果丙想赢 k 次,那么,一定有某种技巧(对应于仙农编码),使得他能够在 k/G 次游戏中,以任意接近 1 的概率达到目的。反过来,(2)如果乙在 n 次游戏中,赢了 S 次,那么,一定有 $S\leqslant nG$。

关于信道容量 G 的值,可以完全仿照 E 值来计算,不过,“丙信道”的容量其实是 p 和 q 的函数,可以记为 $G(p,q)$。

结合定理 4,5,6,我们便可以对甲乙丙三方,在“手心手背”游戏中的宏观输赢情况进行描述了:

定理 7　在“手心手背游戏”中,如果“甲信道”、“乙信道”和“丙信道”的信道容量分别是 E、F 和 G,那么,三方在该游戏中,甲乙丙的最终输赢情况,整体上依赖于 E、F 和 G 的大小,谁的信道容量越大,谁就占优势。注意到这三个信道容量不能由任何一方单独调整,除非有某两方合谋,否则,很难通过改变自己的习惯(即,单独改变 p,q 或 r)来改变最终的输赢情况。

3　结束语

本文的游戏和文献[3]中的“石头剪刀布游戏”,看似千差万别,但是,我们却巧妙地应用了一个几乎相同的方法,给出了出人意料的答案,即,建立某个信道,把攻防某方的“一次胜利”,转化为“1 比特信息在该信道中被成功传输”,于是,利用仙农编码定理,攻防双方的对抗问题,就转化为了信道容量的计算问题了。

当然,《安全通论》“信道容量法”的威力,还远不止于此!

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”[EB/OL]. http://blog. sciencenet. cn/blog-453322-948089. html ,2016-01-04.

[4]　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.

[5]　Shu Lin,Daniel J. Costello Jr. 差错控制码[M]. 晏坚,何元智,潘亚汉,等译. 北京:机械工程出版社.