第31卷第3期 成都信息工程大学学报 Vol. 31 No. 3
2016年6月 JOURNAL OF CHENGDU UNIVERSITY OF INFORMATION TECHNOLOGY Jun. 2016

文章编号：2096-1618(2016)03-0242-05
稿件来源：科学网
网　　址：http://blog.sciencenet.cn/blog-453322-954445.html
发表时间：2016-02-04

安全通论(6)

——攻防篇之“多人盲对抗”

杨义先，　钮心忻
(北京邮电大学信息安全中心，北京 100876)

摘要：给出常见于网络空间安全攻防战中，如下两种情形下，攻守双方极限能力的精确值：(1)多位黑客攻击一位红客；(2)一个黑客攻击多位红客。

0　引言

“攻防”是安全的核心，而“攻防”的实质就是“对抗”。

为了全面深入地研究“对抗”，我们已经花费了四篇文章[2-5]来进行地毯式探索：

文献[2]，统一研究了“盲对抗”，并给出了黑客(红客)攻击(防守)能力的精确极限。

文献[3]、[4]和[5]，以国际著名的“石头剪刀布游戏”、国内家喻户晓的“猜正反面游戏”和“手心手背游戏”、酒桌上著名的“划拳”和“猜拳”为对象，研究了“非盲对抗”的五个有趣实例，给出了输赢极限和获胜技巧。

特别是文献[5]，针对“非盲对抗”的很大一个子类(输赢规则线性可分的情况)，给出了统一的解决方案。

但是，文献[2]~[5]都只限于“攻”与“守”单挑的情形，即，一个黑客攻击一个红客。虽然在一般系统中，黑客与红客几乎都是“一对一”的，但是，在网络空间安全对抗中，还会经常出现“群殴”事件，特别是多位黑客攻击一位红客；一个黑客攻击多位红客；黑客借助跳板来攻击红客；在有人协助时，黑客攻击红客等。而另一方面，在网络空间安全对抗中，几乎只涉及“盲对抗”，所以，下面我们就重点研究这类“盲群殴”。当然，本文的结果，绝不仅仅限于网络空间安全，仍然对各类安全都有效。

本文的攻防场景描述，主要是引入“上帝”的做法，与文献[2]相同，为了节省篇幅，此处不再重复。

1　多位黑客攻击一位红客

为了直观计，我们先考虑2个黑客攻击一个红客的情形，然后，再做推广。

设黑客 X_1 和 X_2 都想攻击红客 Y，并且两个黑客互不认识，甚至可能不知道对方的存在，因此，作为随机变量，可以假设 X_1 和 X_2 是相互独立的。

与文献[2]类似，我们仍然假设：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 X_1 和 X_2 代表第一个和第二个黑客，他们按如下方式对自己每个回合的战果，进行真心盲自评：

X_1 对本回合盲自评为成功，则 $X_1=1$；X_1 对本回合盲自评为失败，则 $X_1=0$；

X_2 对本回合盲自评为成功，则 $X_2=1$；X_2 对本回合盲自评为失败，则 $X_2=0$；

由于每个回合中，红客要同时对付两个黑客的攻击，所以，用2维随机变量 $Y=(Y_1, Y_2)$ 代表红客，他按如下方式对自己每个回合的防御 X_1 和 X_2 成果，进行真心盲自评：

本回合 Y 自评防御 X_1 成功，自评防御 X_2 也成功时，记为，$Y_1=1, Y_2=1$；

本回合 Y 自评防御 X_1 成功，自评防御 X_2 也失败时，记为，$Y_1=1, Y_2=0$；

本回合 Y 自评防御 X_1 失败，自评防御 X_2 也成功时，记为，$Y_1=0, Y_2=1$；

本回合 Y 自评防御 X_1 失败，自评防御 X_2 也失败时，记为，$Y_1=0, Y_2=0$；

让黑客们和红客不断地进行攻防对抗，并各自记下他们的盲自评结果。虽然他们的盲自评结果是保密的，没有任何人知道，但是，上帝知道这些结果，而且，

根据“频率趋于概率”这个大数定律,上帝就可以计算出如下概率:

$0<P_r(X_1=1)=p<1$; $0<P_r(X_1=0)=1-p<1$;

$0<P_r(X_2=1)=q<1$; $0<P_r(X_2=0)=1-q<1$;

$0<P_r(Y_1=1,Y_2=1)=a_{11}<1$;$0<P_r(Y_1=1, Y_2=0)=a_{10}<1$;

$0<P_r(Y_1=0,Y_2=1)=a_{01}<1$;$0<P_r(Y_1=0, Y_2=0)=a_{00}<1$;

这里,$a_{00}+a_{01}+a_{10}+a_{11}=1$

上帝再造一个 2 维随机变量 $Z=(Z_1,Z_2)=((1+X_1+Y_1)\bmod 2,(1+X_2+Y_2)\bmod 2)$,即,$Z_1=(1+X_1+Y_1)\bmod 2$,$Z_2=(1+X_2+Y_2)\bmod 2$。并利用随机变量 X_1、X_2 和 Z 构造一个 2-接入信道$(X_1,X_2,p(z\mid x_1,x_2),Z)$,并称该信道为红客的防御信道 F。(注:关于多接入信道的细节,请见文献[6]的 15.3 节。)

好了,下面来考虑几个事件恒等式:

{某个回合红客防御成功}={红客防御 X_1 成功}∩{红客防御 X_2 成功}

而

{红客防御 X_1 成功}={黑客 X_1 自评本回合攻击成功,红客自评防御 X_1 成功}∪{黑客 X_1 自评本回合攻击失败,红客自评防御 X_1 成功}$=\{X_1=1,Y_1=1\}\cup\{X_1=0,Y_1=1\}=\{X_1=1,Z_1=1\}\cup\{X_1=0,Z_1=0\}$

同理,

{红客防御 X_2 成功}={黑客 X_2 自评本回合攻击成功,红客自评防御 X_2 成功}∪{黑客 X_2 自评本回合攻击失败,红客自评防御 X_2 成功}$=\{X_2=1,Y_2=1\}\cup\{X_2=0,Y_2=1\}=\{X_2=1,Z_2=1\}\cup\{X_2=0,Z_2=0\}$

所以,{某个回合红客防御成功}$=[\{X_1=1,Z_1=1\}\cup\{X_1=0,Z_1=0\}]\cap[\{X_2=1,Z_2=1\}\cup\{X_2=0,Z_2=0\}]$=[防御信道 F 的第一个子信道传信成功]∩[防御信道 F 的第二个子信道传信成功]= {2 输入信道 F 的传输信息成功}

于是,便有如下引理:

引理 1　如果红客在某个回合防御成功,那么,1 比特信息就在 2-输入信道 F(防御信道)中,被成功传输。

反过来,如果“2-输入信道 F 的传输信息成功”,那么,“防御信道 F 的第一个子信道传输成功”同时“防御信道 F 的第二个子信道传输成功”,即,$[\{X_1=1,Z_1=1\}\cup\{X_1=0,Z_1=0\}]\cap[\{X_2=1,Z_2=1\}\cup\{X_2=0,Z_2=0\}]$,这等价于$[\{X_1=1,Y_1=1\}\cup\{X_1=0,Y_1=1\}]\cap[\{X_2=1,Y_2=1\}\cup\{X_2=0,Y_2=1\}]$

而

$\{X_1=1,Y_1=1\}\cup\{X_1=0,Y_1=1\}$意味着{黑客 X_1 自评本回合攻击成功,红客自评防御 X_1 成功}∪{黑客 X_1 自评本回合攻击失败,红客自评防御 X_1 成功},即,{红客防御 X_1 成功}

同理,

$\{X_2=1,Y_2=1\}\cup\{X_2=0,Y_2=1\}$意味着{黑客 X_2 自评本回合攻击成功,红客自评防御 X_2 成功}∪{黑客 X_2 自评本回合攻击失败,红客自评防御 X_2 成功},即,{红客防御 X_2 成功}

所以,$[\{X_1=1,Y_1=1\}\cup\{X_1=0,Y_1=1\}]\cap[\{X_2=1,Y_2=1\}\cup\{X_2=0,Y_2=1\}]$就等同于{某个回合红客防御成功},从而,我们就得到了如下引理(它是引理 1 的逆)。

引理 2　如果 1 比特信息在 2-输入信道 F(防御信道)中被成功传输,那么,红客就在该回合中防御成功。

结合引理 1 和引理 2,我们就得到了如下定理:

定理 1　设随机变量 X_1、X_2 和 Z 如上所述,防御信道 F 是如下 2-接入信道$(X_1,X_2,p(z\mid x_1,x_2),Z)$,那么,“红客在某回合中防御成功”就等价于“1 比特信息在防御信道 F 中被成功传输”。

根据文献[6]的定理 15.3.1 及其逆定理,我们知道信道 F 的可达容量区域为满足下列条件的全体(R_1,R_2)所组成集合的凸闭包,

$$0\leqslant R_1\leqslant \max_X I(X_1;Z\mid X_2),$$
$$0\leqslant R_2\leqslant \max_X I(X_2;Z\mid X_1),$$
$$0\leqslant R_1+R_2\leqslant \max_X I(X_1, X_2;Z).$$

这里最大值是针对所有独立随机变量 X_1 和 X_2 的概率分布而取的;$I(A,B;C)$表示互信息,而 $I(A;B\mid C)$表示条件互信息;$Z=(Z_1,Z_2)=((1+X_1+Y_1)\bmod 2,(1+X_2+Y_2)\bmod 2)$。

利用定理 1,并将上述可达容量区域的结果翻译成攻防术语后,便得到:

定理 2　两个黑客 X_1 和 X_2 独立地攻击一个红客 Y。如果,在 n 个攻防回合中,红客成功防御第一个黑客 r_1 次,成功防御第二个黑客 r_2 次,那么,一定有:

$$0\leqslant r_1\leqslant n[\max_X I(X_1;Z\mid X_2)],$$
$$0\leqslant r_2\leqslant n[\max_X I(X_2;Z\mid X_1)],$$
$$0\leqslant r_1+r_2\leqslant n[\max_X I(X_1, X_2;Z)].$$

而且,上述的上限是可达的,即,红客一定有某种最有效的防御方法,使得在 n 次攻防回合中,红客成功防御第一个黑客 r_1 次,成功防御第二个黑客 r_2 次,的成功次数 r_1 和 r_2 达到上限:$r_1=n[\max_X I(X_1;Z\mid X_2)]$,同时 $r_2=n[\max_X I(X_2;Z\mid X_1)]$以及 $r_1+r_2=n[\max_X I(X_1, X_2;Z)]$。再换一个角度,还有:

如果红客要想成功防御第一个黑客 r_1 次,成功防

御第二个黑客 r_2 次,那么,他至少得进行 $\max\{r_1[\max_X I(X_1;Z\mid X_2)], r_2[\max_X I(X_2;Z\mid X_1)], [\max_X I(X_1,X_2;Z)]\}$ 次防御。

下面来将定理 2 推广到任意 m 个黑客 $X_1,X_2,\cdots,X_m$,独立地攻击一个红客 $Y=(Y_1,Y_2,\cdots,Y_m)$ 的情况。

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。

对任意 $1\leqslant i\leqslant m$,黑客 X_i 按如下方式对自己每个回合的战果,进行真心盲自评:

黑客 X_i 对本回合盲自评为成功,则 $X_i=1$;黑客 X_i 对本回合盲自评为失败,则 $X_i=0$;

每个回合中,红客按如下方式对自己防御黑客 $X_1,X_2,\cdots,X_m$ 的成果,进行真心盲自评:任取整数集合 $\{1,2,\cdots,m\}$ 的一个子集 S,记 S^c 为 S 的补集,即,$S^c=\{1,2,\cdots,m\}-S$,再记 $X(S)$ 为 $\{X_i:i\in S\}$,$X(S^c)$ 为 $\{X_i:i\in S^c\}$,如果红客成功地防御了 $X(S)$ 中的黑客,但却自评被 $X(S^c)$ 中的黑客打败,那么,红客的盲自评估就为:$\{Y_i=1:i\in S\}$,$\{Y_i=0:i\in S^c\}$。

上帝再造一个 m 维随机变量 $Z=(Z_1,Z_2,\cdots,Z_m)=((1+X_1+Y_1)\bmod 2,\ (1+X_2+Y_2)\bmod 2,\cdots,\ (1+X_m+Y_m)\bmod 2)$,即,$Z_i=(1+X_i+Y_i)\bmod 2$,$1\leqslant i\leqslant m$。并利用随机变量 $X_1,X_2,\cdots,X_m$ 和 Z 构造一个 m-接入信道,并称该信道为红客的防御信道 G。

仿照上面 $m=2$ 的证明方法,利用文献[6]的定理 15.3.6 及其逆定理,我们知道信道 G 的可达容量区域为满足下列条件的所有码率向量所成集合的凸闭包,

$R(S)\leqslant I(X(S);Z\mid X(S^c))$,对 $\{1,2,\cdots,m\}$ 的所有子集 S。

这里 $R(S)$ 定义为 $R(S)=\sum_{i\in S}R_i=\sum_{i\in S}[r_i/n]$,$r_i/n$ 是第 i 个输入的码率。

仿照前面,将该可达容量区域的结果翻译成攻防术语后,便得到:

定理 3 m 个黑客 $X_1,X_2,\cdots,X_m$ 独立地攻击一个红客 Y。如果,在 n 个攻防回合中,红客成功防御第 i 个黑客 r_i 次,$1\leqslant i\leqslant m$,那么,一定有 $r(S)\leqslant n[I(X(S);Z\mid X(S^c))]$,对 $\{1,2,\cdots,m\}$ 的所有子集 S。这里 $r(S)=\sum_{i\in S}r_i$。而且,该上限是可达的,即,

红客一定有某种最有效的防御方法,使得在 n 次攻防回合中,红客成功防御黑客集 S 的次数集合 $r(S)$,达到上限:$r(S)=n[I(X(S);Z\mid X(S^c))]$,对 $\{1,2,\cdots,m\}$ 的所有子集 S。再换一个角度,还有:

如果红客要想实现成功防御黑客集 S 的次数集合为 $r(S)$,那么,他至少得进行 $\max\{r(S)/[I(X(S);Z\mid X(S^c))]\}$ 次防御。

2 一位黑客攻击多位红客

为了增强安全性,红客在建设系统时,常常建设一个甚至多个(异构)备份系统,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。这就是“一位黑客攻击多位红客”的实际背景,换句话说,只要有那怕一个备份未被黑客攻破,那么,就不能算黑客赢。当然,也许红客们并不知道是同一个黑客在攻击他们,至于红客们是否协同,都不影响下面的研究。

先考虑 1 个黑客攻击 2 个红客的情形,然后,再做推广。

设黑客 $X=(X_1,X_2)$ 想同时攻击两个红客 Y_1 和 Y_2。由于这两个红客是两个互为备份系统的守卫者,因此,黑客必须同时把这两个红客打败,才能算真赢。

与上节类似,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红客,他们按如下方式对自己每个回合的战果,进行真心盲自评:

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

红客 Y_2 对本回合防御盲自评为成功,则 $Y_2=1$;红客 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,黑客要同时攻击两个红客,所以,用 2 维随机变量 $X=(X_1,X_2)$ 代表黑客,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,$X_1=0$,$X_2=0$;

让黑客和红客们不断地进行攻防对抗,并各自记下他们的盲自评结果。虽然他们的盲自评结果是保密

的，没有任何人知道，但是，上帝知道这些结果，而且，根据“频率趋于概率”这个大数定律，上帝就可以计算出如下概率：

$0<P_r(Y_1=1)=f<1$；$0<P_r(Y_1=0)=1-f<1$；

$0<P_r(Y_2=1)=g<1$；$0<P_r(Y_2=0)=1-g<1$；

$0<P_r(X_1=1,X_2=1)=b_{11}<1$；$0<P_r(X_1=1,\ X_2=0)=b_{10}<1$；

$0<P_r(X_1=0,X_2=1)=b_{01}<1$；$0<P_r(X_1=0,\ X_2=0)=b_{00}<1$；

这里，$b_{00}+b_{01}+b_{10}+b_{11}=1$

上帝再造两个随机变量 Z_1 和 Z_2，这里 $Z_1=(X_1+Y_1)\bmod 2$，$Z_2=(X_2+Y_2)\bmod 2$。并利用随机变量 X(输入)和 Z_1、Z_2(输出)构造一个 2-输出广播信道 $p(z_1,z_2|x)$，并称该信道为黑客的攻击信道 G。(注：关于广播信道的细节，请见文献[6]的 15.6 节。)

好了，下面来考虑几个事件恒等式：

{黑客 X 攻击成功}＝{黑客 X 攻击 Y_1 成功}∩{黑客 X 攻击 Y_2 成功}＝[{黑客 X 自评攻击 Y_1 成功，红客 Y_1 自评防御失败}∪{黑客 X 自评攻击 Y_1 失败，红客 Y_1 自评防御失败}]∩[{黑客 X 自评攻击 Y_2 成功，红客 Y_2 自评防御失败}∪{黑客 X 自评攻击 Y_2 失败，红客 Y_2 自评防御失败}]＝[$\{X_1=1,Y_1=0\}\cup\{X_1=0,\ Y_1=0\}$]∩[$\{X_2=1,Y_2=0\}\cup\{X_2=0,\ Y_2=0\}$]＝[$\{X_1=1,Z_1=1\}\cup\{X_1=0,\ Z_1=0\}$]∩[$\{X_2=1,Z_2=0\}\cup\{X_2=0,\ Z_2=0\}$]＝[1 比特信息被成功地从广播信道 G 的第 1 个分支传输到目的地]∩[1 比特信息被成功地从广播信道 G 的第 2 个分支传输到目的地]＝[1 比特信息在广播信道 G 中被成功传输]。

以上推理过程，完全可以逆向进行，所以，我们有：

定理 4　一个黑客 $X=(X_1,X_2)$ 同时攻击两个红客 Y_1 和 Y_2，如果在某个回合中黑客攻击成功，那么，1 比特信息就在上述 2-输出广播信道(攻击信道)G 中被成功传输，反之亦然。

下面再将定理 4 推广到 1 个黑客 $X=(X_1,X_2,\cdots,X_m)$，同时攻击任意 m 个红客 Y_1、Y_2、…、Y_m 的情况。由于这 m 个红客是互为备份系统的守卫者，因此，黑客必须同时把这 m 个红客打败，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。

对任意 $1\leqslant i\leqslant m$，红客 Y_i 按如下方式对自己每个回合的战果，进行真心盲自评：

红客 Y_i 对本回合防御盲自评为成功，则 $Y_i=1$；红客 Y_i 对本回合盲自评防御为失败，则 $Y_i=0$；

每个回合中，黑客按如下方式对自己攻击红客 $Y_1,Y_2,\cdots,Y_m$ 的成果，进行真心盲自评：任取整数集合 $\{1,2,\cdots,m\}$ 的一个子集 S，记 S^c 为 S 的补集，即，$S^c=\{1,2,\cdots,m\}-S$，再记 $Y(S)$ 为 $\{Y_i:i\in S\}$，$Y(S^c)$ 为 $\{Y_i:i\in S^c\}$，如果黑客自评成功地攻击了 $Y(S)$ 中的红客，但却自评被 $Y(S^c)$ 中的红客成功防御，那么，黑客 X 的盲自评就为：$\{X_i=1:i\in S\}$，$\{X_i=0:i\in S^c\}$。

上帝再造 m 个随机变量 Z_i，这里 $Z_i=(X_i+Y_i)\bmod 2$，$1\leqslant i\leqslant m$。并利用随机变量 X(输入)和 $Z_1,Z_2,\cdots,Z_m$(输出)构造一个 m-输出广播信道 $p(z_1,z_2,\cdots,z_m|x)$，并称该信道为黑客的攻击信道 H。(注：关于广播信道的细节，请见文献[6]的 15.6 节。)

好了，下面来考虑几个事件恒等式：

{黑客 X 攻击成功}＝$\cap_{1\leqslant i\leqslant m}${黑客 X 攻击 Y_i 成功}＝$\cap_{1\leqslant i\leqslant m}$[{黑客 X 自评攻击 Y_i 成功，红客 Y_i 自评防御失败}∪{黑客 X 自评攻击 Y_i 失败，红客 Y_i 自评防御失败}]＝$\cap_{1\leqslant i\leqslant m}$[$\{X_i=1,Y_i=0\}\cup\{X_i=0,\ Y_i=0\}$]＝$\cap_{1\leqslant i\leqslant m}$[$\{X_i=1,Z_i=1\}\cup\{X_i=0,\ Z_i=0\}$]＝$\cap_{1\leqslant i\leqslant m}$[1 比特信息被成功地从广播信道 G 的第 i 个分支传输到目的地]＝[1 比特信息在 m-广播信道 G 中被成功传输]。

以上推理过程，完全可以逆向进行，所以，我们有：

定理 5　一个黑客 $X=(X_1,X_2,\cdots,X_m)$ 同时攻击 m 个红客 $Y_1,Y_2,\cdots,Y_m$，如果在某个回合中黑客攻击成功，那么，1 比特信息就在上述 m-输出广播信道(攻击信道)H 中被成功传输，反之亦然。

根据上述定理 4 和定理 5，一个黑客同时攻击多个红客的问题，就完全等价于广播信道的信息容量区域问题。可惜，到目前为止，广播信道的信息容量区域问题还未被解决。

3　结束语

在实际的网络空间安全对抗中，还有两种常见的攻击情况：(1)黑客借助跳板来攻击红客；(2)在有人协助(比如，在红方有一个内奸)时，黑客攻击红客等。可是，如何来研究这两种攻防极限呢？目前还没有答案。

另一方面，在多用户信息论中，也有两种常见的信道：(1)中继信道(见文献[6]的 15.7 节)；(2)边信息信道(见文献[6]的 15.8 节)。

我严重怀疑“中继信道可用于研究黑客的跳板攻击”，同时，“边信息信道可用于研究有内奸攻击”，但是，很可惜，我始终没能找到突破口。欢迎有兴趣的读

者来“接棒”。

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 ,2016-01-01.

[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] 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.