服务跳变抗 DoS 机制的博弈理论分析

石乐义[①②]　贾春福[②]　吕述望[②]
[①](中国石油大学计算机与通信工程学院　东营　257061)
[②](南开大学信息技术科学学院　天津　300071)

摘　要：该文对 DoS 攻防进行不完全信息博弈分析，讨论了 DoS 防范的困境，指出信息的不对称性和未能形成服务方-用户联盟是防范困境的根本原因。通过引入服务跳变策略，增加服务类型并建立服务方-用户联盟，即可构造新的 DoS 攻防博弈均衡，理论上证明了服务跳变策略具有主动的抗 DoS 特性，对于服务跳变与 DoS 主动防范策略研究具有理论意义。

关键词：拒绝服务；博弈论；纳什均衡；服务跳变；联盟
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)01-0228-05

A Game Theoretic Analysis of Service Hopping Mechanism for DoS Defense

Shi Le-yi[①②]　Jia Chun-fu[②]　Lü Shu-wang[②]
[①](*College of Computer and Communication Engineering*, *China University of Petroleum*, *Dongying* 257061, *China*)
[②](*College of Information Technical Science*, *Nankai University*, *Tianjin* 300071, *China*)

Abstract: A game-theoretic analysis of security interactive behavior is performed between the DoS attacker and the defender under incomplete information. The dilemma of defense is discussed and the underlying fact is revealed that asymmetric nature of information and absence of server-user coalition lead to the dilemma. An improved DoS game is performed which can acquire new equilibrium through service hopping tactic, increasing service type and establishing the server-user coalition. Theoretical analysis shows that service hopping tactic is active and efficient for DoS defense. It is fundamental and important for service hopping mechanism and DoS defense.

Key words: Denial of Service (DoS); Game theory; Nash equilibrium; Service hopping; Coalition

1　引言

DoS(Denial of Service)攻击是一种以消耗网络带宽和系统资源为目的，通过对服务器发送大量“合理”请求，造成系统无法提供正常服务的攻击方式。DDoS(Distributed Denial of Service)则是一种分布式、协同工作的大规模拒绝服务攻击方式。DoS/DDos攻击是互联网中最常见并且难以防范的攻击手段，其防范策略经历了阻截、检测、跟踪和容忍等阶段，出现了防火墙、入侵检测、IP/ICMP跟踪[1,2]、入口/出口过滤[3,4] 、覆盖网络[5]等防范方法。近来，基于服务信息伪随机变化的DoS躲避策略受到关注，出现了端口跳变[6,7]、端址跳变[8,9]、地址跳变[10]、虚假端址跳变[11]等服务跳变技术。

从DoS攻防交互行为上看，攻击者总是希望破坏或阻止正常的网络服务，服务方则希望减弱、阻断DoS攻击以提供良好的服务。显然，DoS攻防构成了非合作博弈。本文通过不完全信息的动态博弈分析，讨论了当前DoS防范的困境，指出了信息不对称性和未能形成服务方-用户联盟是DoS防范困境的根本原因，并在改进的DoS攻防博弈中引入服务跳变策略，增加服务类型并构造服务方-用户联盟，实现了主动的DoS防御，从而在博弈理论上证明了服务跳变策略抗DoS机制的主动性和有效性。

2007-07-16 收到，2008-05-19 改回
国家自然科学基金(60577039)和天津市科技发展计划项目基金(05YFGZGX24200)资助项目

2　博弈数学模型

博弈理论是一门研究相互影响着的局中人进行策略选择时的行为规律的科学。博弈问题有5个要素：局中人，局中人策略集，局中人决策先后顺序，局中人收益函数和局中人信息(类型、收益偏好等)。博弈分析设定所有局中人都是理性的，力求收益的最大化。博弈有不同的分类准则：按局中人决策先后顺序可分为静态博弈和动态博弈；按局中人是否协作分为合作博弈和非合作博弈；按局中人对信息的掌握情况分为完全信息博弈和非完全信息博弈，前者局中人知道其他所有局中人类型及偏好，后者则只知道分布范围，需主观上进行后验概率判断。

定义1　标准博弈定义为三元组 $\Gamma \triangleq < N, (A_i)_{i\in N}, (u_i)_{i\in N} >$，其中 $N \triangleq \{1,2,\cdots,n\}$ 为局中人集合，共 n 个局中人；$(A_i)_{i\in N}$ 为局中人 i 的策略集；$(u_i)_{i\in N}$ 则是局中人 i 的收益函数。

在标准博弈中，局中人策略集和收益函数是确定的，局中人 i 在博弈中理性化的表现是使 u_i 极大化。标准博弈是一种完全信息静态博弈，而实际博弈并非如此理想化。在增加了局中人的类型以及不确定性因素后，标准博弈就变成了不完全信息的博弈形式[12]。

定义2　不完全信息动态博弈定义为六元组 $\Gamma \triangleq < N, (\Theta_i)_{i\in N}, (A_i)_{i\in N}, (H_i)_{i\in N}, (u_i)_{i\in N}, P >$，其中 $N \triangleq \{1,2,\cdots,n\}$ 为局中人集合；$(\Theta_i)_{i\in N}$ 表示局中人 i 的类型，$(A_i)_{i\in N}$ 表示局中人 i 的策略集；$(H_i)_{i\in N}$ 表示局中人 i 的历史行动序列；$(u_i)_{i\in N}$ 表示局中人 i 的支付函数；P 是定义在类型空间 Θ 上的概率分布。

博弈过程正是参与者选择策略进行博弈，并且不断获取并修正信息，甚至改变或调整效用的决策过程。

3　DoS 攻防博弈分析

网络攻防具有理性、非合作等特点，攻防双方无法完全掌握敌手的类型和信息价值，构成了非合作不完全信息的攻防博弈[13]。DoS攻防博弈具有以下特点：局中人包括了服务方、合法用户和攻击者，但服务者视角中的博弈对手是一个具有两种不同类型(合法用户和攻击者)的来访者；服务方无法掌握但可以推测来访者的具体类型，旨在为合法用户提供良好服务并阻止攻击者；攻击者视角中的博弈对手则是服务方和合法用户，并可通过踩点、侦察等手段获取固定网络服务的类型(协议、端口、地址等)，假冒合法用户发起恶意访问，达到破坏或阻止合法用户访问信息服务的目的。下面从不同局中人的视角，对DoS攻防进行不完全信息的动态博弈分析：

局中人集合：$N=\{1,2,0\}$，1为服务方，2为访问者，0为虚拟局中人“自然”。

局中人类型：固定服务类型 $\Theta_1=\{\theta_{11}\}=\{(\text{Protocal}_1, \text{IP}_1, \text{Port}_1)\}$，访问类型 $\Theta_2=\{\theta_{21},\theta_{20}\}=\{\text{Attacker}, \text{User}\}$。

局中人策略集：服务方策略集 $A_1=\{\pi_{11},\pi_{10}\}$，$\pi_{11}$ 表示提供服务，π_{10} 表示不提供服务；访问者策略集 $A_2(\theta_{21})=A_2(\theta_{20})=\{\pi_{21},\pi_{20}\}$，$\pi_{21}$ 表示访问 θ_{11} 类型的服务，π_{20} 则表示不访问。

局中人收益：服务方若为合法用户提供服务，双方收益均为 a $(a>0)$，否则收益为 $-a$；服务方若为攻击者提供服务，服务性能将恶化，收益为 $-ka$，攻击者收益 $ka-b$ (k 为攻击破坏因子，反映不同攻击的破坏程度且 $k>1$，b 为攻击代价且 $a>b>0$)；若攻击访问遭拒绝，攻击者收益为 $-b$。表1给出了DoS攻防博弈不同局中人的收益情况。

具有海萨尼转换的DoS攻防博弈树如图1所示，博弈过程如下：

(1)虚拟局中人“自然”首先选择访问者的类型 θ_{2t}，服务方不知道访问者类型，但对访问类型有一个先验概率判断 $\{P(\theta_{21})=p, P(\theta_{20})=1-p\}$。

表1 DoS攻防博弈收益表

		访　问　者			
		θ_{21} 攻击者		θ_{20} 合法用户	
		π_{21}	π_{20}	π_{21}	π_{20}
服务方	π_{11}	$-ka\ ,ka-b$	0,0	a,a	0,0
	π_{10}	$0,-b$	0,0	$-a,-a$	0,0

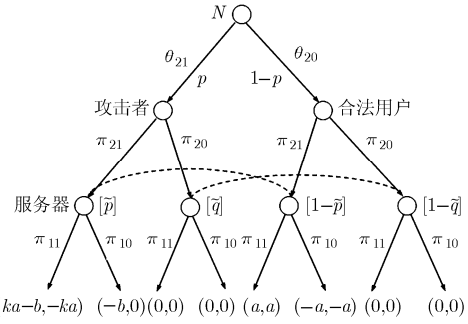

图1 服务方视角下的DoS攻防博弈树

(2)访问者观测到访问类型 θ_{2t} 之后，从策略空间 $A_2(\theta_{21})=A_2(\theta_{20})=\{\pi_{21},\pi_{20}\}$ 中选择一个策略 π_{2i}。

(3)服务方观测到访问者行动 π_{2i} 后，运用贝叶斯法则得到访问类型后验概率 $\tilde{p}_{it}=p(\theta_{2t}\mid\pi_{2i})$，然后从策略空间 $A_1=\{\pi_{11},\pi_{10}\}$ 中选择一个行动 π_{1j}。将服务方和访问者的收益表示为 $f_1(\theta_{2t},\pi_{2i},\pi_{1j})$ 和 $f_2(\theta_{2t},\pi_{2i},\pi_{1j})$，那么服务方选择的策略 π_{1j} 应使得服务方期望收益极大化，即 $\max\limits_{\pi_{1j}\in A_1}\sum\limits_{\theta_{2t}\in\Theta_2}\tilde{p}_{it}\cdot f_1(\theta_{2t},\pi_{2i},\pi_{1j})$ 的解。

从服务方的视角分析该DoS攻防博弈，按照“自然”所选择的访问者类型 θ_{2t}，访问者行动存在4种纯组合策略，分别是 $\{(\pi_{21},\pi_{21}),(\pi_{21},\pi_{20}),(\pi_{20},\pi_{21}),(\pi_{20},\pi_{20})\}$，其中 (π_{2m},π_{2n}) 表示访问类型分别为 $(\theta_{21}=\text{Attacker},\theta_{20}=\text{User})$ 时访问者的策略组合。下面讨论服务方视角下是否存在纯策略均衡，以 (π_{21},π_{21}) 策略为例进行分析：

来访者策略为 $\pi(\theta_{21})=\pi(\theta_{20})=\pi_{21}$，即不论“自然”选择访问类型为 θ_{21} 或是 θ_{20}，访问者均选择访问策略 π_{21}。服务方观测到来访者策略 π_{21} 后，推测来访者访问类型的后验概率 $\tilde{p}_{11}=p(\theta_{21}\mid\pi_{21})=p$，$\tilde{p}_{10}=p(\theta_{20}\mid\pi_{21})=1-p$，并以此为依据，计算出选择 π_{11} 服务策略和选择 π_{10} 不服务策略情况下服务方的期望收益：

$$u(\pi_{11})=\sum_{\theta_{2t}\in\Theta_2}\tilde{p}_{1t}f_1(\theta_{2t},\pi_{21},\pi_{11})=p(\theta_{21}\mid\pi_{21})\times(-ka)+p(\theta_{20}\mid\pi_{21})\times(a)=(1-(1+k)p)a \quad (1)$$

$$u(\pi_{10})=\sum_{\theta_{2t}\in\Theta_2}\tilde{p}_{1t}f_1(\theta_{2t},\pi_{21},\pi_{10})=p(\theta_{21}\mid\pi_{21})\times 0+p(\theta_{20}\mid\pi_{21})\times(-a)=(p-1)a \quad (2)$$

令 $u(\pi_{11})=u(\pi_{10})$，得 $p=2/(2+k)$。对于访问者策略

组合(π_{21},π_{21})，当$p<2/(2+k)$的来访为攻击者时，服务方的占优策略是π_{11}提供服务，反之占优策略为π_{10}不服务。本文分两种情况继续讨论是否存在博弈均衡：

(1) $p<2/(2+k)$　$p<2/(2+k)$时，服务方对于(π_{21},π_{21})的占优策略为π_{11}提供服务，收益期望$u(\pi_{11})=(1-(1+k)p)a$。下面反向考察(π_{21},π_{21})是否构成对服务策略π_{11}的占优策略。服务方策略π_{11}下，来访者组合策略的期望收益是：

$$u((\pi_{2i},\pi_{2j}))=p\times f_2(\theta_{21},\pi_{2i},\pi_{11})+(1-p)\times f_2(\theta_{20},\pi_{2j},\pi_{11}) \quad (3)$$

由式(3)计算得到$u((\pi_{21},\pi_{21}))=(ka-b)p+a(1-p)$；$u((\pi_{21},\pi_{20}))=(ka-b)p$；$u((\pi_{20},\pi_{21}))=(1-p)a$；$u((\pi_{20},\pi_{20}))=0$。显然，$u((\pi_{21},\pi_{21}))>u((\pi_{21},\pi_{20}))>u((\pi_{20},\pi_{20}))$且$u((\pi_{21},\pi_{21}))>u((\pi_{20},\pi_{21}))$，访问策略$(\pi_{21},\pi_{21})$也是服务策略$\pi_{11}$的占优策略，因此$((\pi_{21},\pi_{21}),\pi_{11})$构成了贝叶斯均衡策略。

(2)　$p>2/(2+k)$　$p>2/(2+k)$时，服务方对于(π_{21},π_{21})的占优策略为π_{10}不提供服务，收益期望$u(\pi_{11})=(p-1)a$。同样考察知：(π_{21},π_{21})不构成对服务方策略π_{10}的占优策略，$((\pi_{21},\pi_{21}),\pi_{10})$在$p>2/(2+k)$下不构成均衡。

同理，依次分析各组合策略得到结论：服务方视角下$((\pi_{20},\pi_{20}),\pi_{10})$和$p<2/(2+k)$条件下$((\pi_{21},\pi_{21}),\pi_{11})$策略构成了均衡；而$p>2/(2+k)$时服务方对$(\pi_{21},\pi_{21})$的占优策略为$\pi_{10}$不服务，但不构成均衡。

以上从服务方视角分析了DoS攻防博弈的策略均衡，然而还需要进一步从攻击者视角，分析服务方视角的均衡策略是否符合攻击者预期目标并构成占优策略。从攻击者视角看，博弈目标是阻止或破坏服务方和合法用户的信息传输；博弈对手是非联盟的服务方和合法用户；服务方视角的均衡策略$((\pi_{20},\pi_{20}),\pi_{10})$，$((\pi_{21},\pi_{21}),\pi_{11})$可以分别描述为$(\pi_{20},(\pi_{20},\pi_{10}))$和$(\pi_{21},(\pi_{21},\pi_{11}))$。对于非联盟策略$(\pi_{20},\pi_{10})$，攻击者收益$u(\pi_{20})=0>-b=u(\pi_{21})$，因此$\pi_{20}$是攻击者对$(\pi_{20},\pi_{10})$的占优策略；同理，当攻击概率$p<2/(2+k)$时对于非联盟策略$(\pi_{21},\pi_{11})$，攻击者收益$u(\pi_{21})=ka-b>0=u(\pi_{20})$，因此$\pi_{21}$也构成攻击者对$(\pi_{21},\pi_{11})$的占优策略。可见，服务方视角的均衡策略构成了攻击视角的策略占优。当$p>2/(2+k)$时，服务方对来访策略(π_{21},π_{21})的占优决策为π_{10}不服务，尽管攻击者策略π_{21}并不是对非联盟策略(π_{21},π_{11})的占优策略，但服务方拒绝合法用户的服务请求同样符合攻击者预期。

以上分析可知，服务方视角的均衡策略$((\pi_{20},\pi_{20}),\pi_{10})$和$((\pi_{21},\pi_{21}),\pi_{11})_{p<2/(2+k)}$符合攻击视角下攻击者策略占优的要求，构成了DoS攻防博弈均衡。$((\pi_{20},\pi_{20}),\pi_{10})$均衡意味着无请求无服务，尽管没有实际意义，但符合攻击者预期；策略$((\pi_{21},\pi_{21}),\pi_{11})$在$p<2/(2+k)$前提下达到均衡，但攻击概率$p$，攻击破坏因子$k$均由攻击者动态选择，服务方难以准确预期，易受到攻击者的元策略(Meta-Strategies)欺骗而影响博弈决策。反观DoS攻击者，当观测到无合法用户访问时选择策略π_{20}，反之选择策略π_{21}，总可以实现阻止或破坏对手信息传递的目标。更进一步，攻击者可以主动改变攻击概率p和破坏因子k，致使DoS防范十分被动。

4 服务跳变策略抗 DoS 机制分析

以上讨论了DoS防范困境，从攻防博弈角度分析，其根本原因在于：(1)信息不对称，攻击者可以获得固定服务类型的完全信息；(2)服务方与合法用户未能形成联盟。本文考虑在DoS攻防博弈中增加服务类型并构造服务方-用户联盟：扩展固定服务类型$\Theta_1=\{\theta_{11}\}$为$\Theta_1=\{\theta_{11},\theta_{12},\theta_{13},\cdots,\theta_{1N}\}$，$\theta_{1i}=(\text{Protocal}_i,\text{IP}_i,\text{Port}_i)$，服务类型由虚拟局中人“自然”选择，简单起见假定“自然”等概率选择服务类型，即$P(\theta_{1i})=1/N,i=1\cdots N$；建立服务方-用户联盟，合法用户通过联盟的同步机制可获知当前服务类型θ_{1t}，即概率$\tilde{p}_{1k}|_{k=t}=1$，$\tilde{p}_{1k}|_{k\neq t}=0$；攻击者无法获知具体服务类型，但可以在观测到服务方策略进行后验推断$\tilde{p}_{1t}=p(\theta_{1t}\,|\,\pi_{11})=p_t$，$\tilde{p}_{0t}=p(\theta_{1t}\,|\,\pi_{10})=p_t$；由于增加了服务类型，访问者策略空间相应修正为$A_2(\theta_{21})=A_2(\theta_{20})=\{\pi_{21},\pi_{22},\cdots,\pi_{2N},\pi_{20}\}$，$\pi_{2k}$ $(k=1,\cdots,N)$表示访问θ_{1k}类型服务，π_{20}表示不访问。改进后的攻防博弈扩展了服务类型，增加了来访者策略，其收益情况如表2所示。

同理，按前一节方法即可分析不同策略组合$((\pi_{2m},\pi_{2n}),\pi_{1i})$的收益与贝叶斯均衡情况。为了直观比较改进前后攻防博弈结果，我们归一化访问者策略空间为$A_2(\theta_{21})=A_2(\theta_{20})=\{\pi_{21},\pi_{20}\}$，其中$\pi_{20}$表示不访问，$\pi_{21}$则表示所有服务访问策略，即原策略空间中的$\{\pi_{21},\pi_{22},\cdots,\pi_{2N}\}$。这样，分别计算出$\pi_{21}$，$\pi_{20}$策略收益的数学期望，得到简化的攻防博弈收益表3。直观地对比表1和表3可见，改进的博弈仅改变了(π_{11},π_{21})的策略收益，然而这种变化是重要和积极的。下面我们仍然从服务方和攻击者视角进行博弈分析，证明这种收益改变影响攻防双方行为决策的有效性。

依然首先从服务方视角分析：对于访问策略(π_{21},π_{21})，服务方期望收益分别是$u(\pi_{11})=-kap/N+(1-p)a$，$u(\pi_{10})=(p-1)a$；显然，攻击概率$p<2N/(2N+k)$时，服务方占优决策为$\pi_{11}$提供服务，反之$\pi_{10}$不服务。该结果与原博弈结论十分相似，但攻击概率阈值已经由原来的$p=2/(2+k)$变为$p=2N/(2N+k)$。N为服务类型数，考虑到服务类型$\theta_{1i}=(\text{Protocal}_i,\text{IP}_i,\text{Port}_i)$，理论上可用TCP/UDP端口数$2^{16}$个，加之一定数量的可用服务IP地址数，因此$N>>k$，攻击概率阈值$p=2N(2N+k)\to 1$。得到结论：增加服务类型和联盟后，当攻击概率$p<1$时服务方对$(\pi_{21},\pi_{21})$的占优决策为$\pi_{11}$提供服务；极端情况$p=1$时，策略$(\pi_{21},\pi_{21})$蜕化为$(\pi_{21},\pi_{20})$，服务方占优决策为$\pi_{10}$不提供服务。反向考察服务方视角下$(\pi_{21},\pi_{21})$策略，由式(3)计算并比较知：$N<ka/b$时，访问策略$(\pi_{21},\pi_{21})$是对服务策略$\pi_{11}$的占优策略。但由于$N>>k$且$N>>a>b$，$N<ka/b$均衡条件几乎无法满足，因此$((\pi_{21},\pi_{21}),\pi_{11})$并不能构成实际的均衡策略。同

表2 增加服务类型与建立联盟后的博弈收益表

			访 问 者									
			θ_{21} 攻击者					θ_{20} 合法用户				
			π_{21}	π_{22}	…	π_{2N}	π_{20}	π_{21}	π_{22}	…	π_{2N}	π_{20}
服务方	θ_{11}	π_{11}	$-ka,ka-b$	$0,-b$	…	$0,-b$	0,0	a,a	$-a,-a$	…	$-a,-a$	0,0
		π_{10}	$0,-b$	$0,-b$	…	$0,-b$	0,0	$-a,-a$	$-a,-a$	…	$-a,-a$	0,0
	θ_{12}	π_{11}	$0,-b$	$-ka,ka-b$	…	$0,-b$	0,0	$-a,-a$	a,a	…	$-a,-a$	0,0
		π_{10}	$0,-b$	$0,-b$	…	$0,-b$	0,0	$-a,-a$	$-a,-a$	…	$-a,-a$	0,0
	…	π_{11}	…	…	…	…	0,0	$-a,-a$	$-a,-a$	…	$-a,-a$	0,0
		π_{10}	…	…	…	…	0,0	$-a,-a$	$-a,-a$	…	$-a,-a$	0,0
	θ_{1N}	π_{11}	$0,-b$	$0,-b$	…	$-ka,ka-b$	0,0	$-a,-a$	$-a,-a$	…	a,a	0,0
		π_{10}	$0,-b$	$0,-b$	…	$0,-b$	0,0	$-a,-a$	$-a,-a$	…	$-a,-a$	0,0

表3 简化的改进博弈收益表

		访　问　者			
		θ_{21} 攻击者		θ_{20} 合法用户	
		π_{21}	π_{20}	π_{21}	π_{20}
服务方	π_{11}	$\dfrac{-ka}{N},\dfrac{ka}{N}-b$	0,0	a,a	0,0
	π_{10}	$0,-b$	0,0	$-a,-a$	0,0

理分析得知 $((\pi_{20},\pi_{21}),\pi_{11})_{N>ka/b}$，$((\pi_{20},\pi_{20}),\pi_{10})$ 构成服务方视角的策略均衡，且符合攻击视角的策略占优，因而构成了改进的DoS攻防博弈均衡。

$((\pi_{20},\pi_{21}),\pi_{11})$ 策略在 $N>ka/b$ 条件下达到贝叶斯均衡，并且 $N>ka/b$ 条件几乎总是成立，这对于DoS防范具有重要意义：原DoS攻防博弈中 $((\pi_{21},\pi_{21}),\pi_{11})$ 构成均衡的条件是 $p<2/(2+k)$，服务方决策受到攻击概率 p 和破坏因子 k 的影响而十分被动。而在增加了服务类型和联盟后的DoS博弈中，当 $N>ka/b$ 时，攻击者攻击收益总是小于不攻击收益，因而 π_{20} 不攻击策略是攻击者的占优策略，而服务策略 π_{11} 对 (π_{20},π_{21}) 严格占优，均衡条件几乎总成立并与服务类型数 N 及破坏因子 k 有关，与攻击概率 p 无关，因此服务方可以通过改变 N 进行元策略欺骗以影响攻击者决策，构成了主动DoS防范。这正是服务跳变策略对抗DoS跳变的机理所在。

5　结束语

本文对DoS攻防进行了不完全信息的动态博弈分析，推理了在DoS攻防博弈中服务方均衡决策受到攻击概率 p 和破坏因子 k 的影响而十分被动，而攻击者则通过简单的跟从策略即总能达到阻止或破坏服务信息传递的目的，从而在理论上推证了当前DoS被动防范的困境，并指出了信息的不对称性和未能形成服务方-用户联盟博弈是DoS防范困境的根本原因。

通过引入服务信息伪随机跳变的服务跳变策略，增加服务类型并建立服务方-用户联盟，可以构成新的贝叶斯均衡策略。理论分析表明：引入服务跳变策略后，服务方均衡决策条件几乎总是成立，与服务类型数 N 、破坏因子 k 有关，而与攻击概率 p 无关，服务方可以通过改变 N 进行元策略欺骗以影响攻击者决策，获得积极主动的DoS防范效果。总体上讲，本文对于DoS主动防范和服务跳变策略的研究具有较好的理论意义。

参 考 文 献

[1] Savage S, Wetherall D, and Karlin A, *et al*.. Practical network support for ip traceback. Proc. ACM SIGCOMM 2000. New York, 2000: 295–306.

[2] Bellovin S. The ICMP traceback message. http://www.research.att.com, 2000.

[3] Ferguson P and Senie D. Network ingress filtering: Defeating denial of service attacks which employs ip source address spoofing. http://www.ietf.org/rfc/rfc2267.txt, 1998.

[4] SANS Institute. Egress filtering. http://www.sans.org/y2k/egress.htm, 2000.

[5] Wang J and Lu L. Tolerating denial of service attacks using overlay networks: Impact of overlay network topology. Proc. 1st ACM Workshop on Survivable and Self-Regenerative Systems, Fairfax VA, 2003: 43–52.

[6] Lee H C J and Thing V L L. Port hopping for resilient networks. Proc. 60th IEEE Vehicular Technology Conference, Washington, 2004: 3291–3295.

[7] Atighetchi M, Pal P, and Webber F, *et al*.. Adaptive use of network-centric mechanisms in cyber-defense. Proc. 6th IEEE Int"l Symp. Object-Oriented Real-Time Distributed Computing, Hokkaido, 2003: 183–192.

[8] Shi L, Jia C, and Lu S, *et al*.. Port and address hopping for

active cyber-defense. Pacific Asia Workshop on Intelligence and Security Informatics, Chengdu, 2007, LNCS 4430: 295–300.

[9] Shi L, Jia C, and Lu S, *et al.*. DoS evading mechanism upon service hopping. IFIP International Conference on Network and Parallel Computing, Dalian, 2007: 119–122.

[10] Sifalakis M, *et al.*. Network address hopping: a mechanism to enhance data protection for packet communications. IEEE International Conference on Communications, Seoul, 2005: 1518–1523.

[11] Badishiy G, Herzberg A, and Keidar I. Keeping denial-of-service attackers in the dark. International Symposium on Distributed Computing, Cracow, 2005: 18–31.

[12] 侯定丕. 博弈论导论. 合肥: 中国科学技术大学出版社, 2004, 第 5 章.

[13] 贾春福, 钟安鸣, 张炜等. 网络安全不完全信息动态博弈模型. 计算机研究与发展, 2006, 43(8)增刊: 530–533.

石乐义： 男，1975 年生，博士，研究方向为网络与信息安全.

贾春福： 男，1967 年生，教授，研究方向为信息安全、运筹优化.

吕述望： 男，1941 年生，教授，研究方向为密码学、信息安全.

勘误 本刊 2008 年第 11 期第 2685 页和第 2687 页的书眉出现错误，现更正如下：

冯新岗等：基于质心的数字图像置乱度衡量准则