# 基于动态博弈的网络诱骗信息获取策略研究

胡光俊 闫怀志
(北京理工大学信息安全与对抗技术研究中心 北京 100081)

〔摘要〕 基于网络诱骗系统信息获取特点的分析,视入侵者与诱骗系统构成网络环境中的博弈主体,结合随机博弈和不完全信息动态博弈理论,探讨了网络对抗环境下诱骗系统信息获取各阶段的获取策略特点。
〔关键词〕 网络诱骗 信息获取 动态博弈 网络对抗 〔中图分类号〕 TP393.08 O225
〔文献标识码〕 A 〔文章编号〕 1000-7857(2005)01-0032-03

# A STUDY OF ACQUIRING INFORMATION STRATEGIES BASED ON DYNAMIC GAME

*HU Guang-jun YAN Huai-zhi*
(Information Security and Countermeasure Technology Research Center, Beijing Institute of Technology, Beijing 100081, China)

**Abstract:** Based on the characteristics of network decoy system, the acquiring Information strategies of dynamic game theory were suggested. Looked upon the attacker and network decoy system as the game players, and in accordance with the dynamic game of incomplete information theory and stochastic games theory, the characteristics of the acquiring information strategies in different phase of acquiring information under network warfare environments were discussed.
**Key Words:** network decoy, acquiring Information, dynamic game, network warfare
**CLC Numbers:** TP393.08 O225 **Document Code:** A **Article ID:** 1000-7857(2005)01-0032-03

## 1 引言

近年来，随着网络规模的不断扩大、复杂性的不断提高,不安全因素随之增多,网络攻击方法层出不穷,传统的防火墙、加密等网络安全技术已经不能满足网络信息的安全需求。网络诱骗技术的出现改变了网络安全被动防御的思路,它通过欺骗入侵者,将其引入事先设计的虚假资源环境,并在该环境中对入侵者的行为进行记录和跟踪,减少真实系统受攻击的风险且可达到提前预警的目的。但传统的诱骗系统自身防护脆弱，容易被有经验的入侵者发觉,而且,获取信息资源有限,无法进行进一步综合分析。为使诱骗系统能够实时监测网络状态,必须对计算机网络入侵、破坏等行为进行识别、记录和分析。要重建入侵事件并解释入侵,必须全面获取诱骗系统的访问信息。诱骗系统工作在严格的对抗环境当中，诱骗信息获取与入侵者的访问行为可视为网络空间的对抗博弈，而诱骗方一般不能完全掌握入侵者的信息，故利用传统方法制定信息获取方法是非常困难的。为此,本文提出了一种基于不完全信息博弈理论的诱骗信息获取策略,为解决上述问题提供了新的思路。

## 2 网络诱骗系统构成

网络诱骗系统要能够监控入侵者对诱骗主机的行为，并对获得的原始入侵行为记录进行统计分析，提供用户配置系统、查询记录等操作的友好图形接口。

网络诱骗系统分为 3 个子系统:诱骗主机子系统、证据数据库子系统和控制台子系统。系统整体的功能结构框架如图 1 所示。

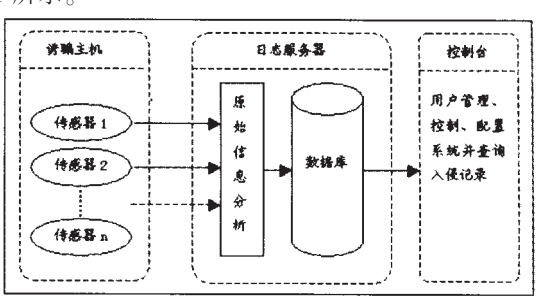


**图 1 系统结构框架图**

诱骗主机子系统监测入侵者的入侵行为,并发送获取的数据到证据数据库子系统;证据数据库子系统接收到的原始入侵记录，一方面作为原始记录存储到原始证据数据库中,一方面通过告警分析模块进行统计分析,并把分析的结果存储到证据数据库中；控制台子系统作为人机交互的接口,为用户管理、控制、配置系统并查询入侵记录提供了接口。

从图 1 可以看出，诱骗主机子系统是整个网络诱骗系

收稿日期:2004-12-20。
基金项目:国防科技基础研究项目。
作者简介:胡光俊,男,1980~ ,北京理工大学信息安全与对抗技术研究中心硕士研究生,主要从事计算机网络安全方面研究,E-mail: city_93@126.com; 闫怀志，男，1975~ ,北京理工大学机电工程学院讲师,主要从事信息安全及智能系统方面的研究工作,E-mail: yhzhi@bit.edu.cn。

统的关键组成部分，其中信息获取策略的制定是决定系统能否实现其功能的首要问题。

## 3 诱骗信息获取博弈行为分析

### 3.1 网络攻击的一般步骤及分析

入侵者攻击的目标可能各不相同，但都有一些基本的步骤。攻击一般包括如下 7 个步骤：被动的侦察、主动的侦察、入侵系统、上传程序、下载数据、利用后门或特洛伊木马保持访问、隐藏踪迹。

### 3.2 信息获取的博弈行为

网络攻防过程始终存在着对抗双方攻击与保护的博弈，在网络诱骗系统环境下，这种对抗关系存在于系统工作的始终，并且有微妙的变化。为完成信息获取，系统首先必须为引导攻击者做相应的伪装；当伪装被发现，为防止入侵者进一步破坏，系统要具有检测和响应的能力；如果攻击者识别出了伪装并实施了破坏，系统还应具有灾难恢复的能力。

通常，入侵者的意图和行动我方是无法完全掌握的，同样我方的目的和策略对敌方来说也是不透明的，但随着对抗博弈的进行，双方可能根据当前对方给出的信号，来对敌方的性质做出判断，从而采取相应的策略，以最大化自己的效用。也就是说，在网络诱骗环境下，信息获取是诱骗系统与入侵者之间的不完全信息多阶段动态博弈的过程，诱骗系统必须动态实时地寻求最优策略，以取得博弈的优势。

在网络诱骗系统环境下，根据对抗目的的不同，把信息获取分为两个阶段：吸引入侵阶段和全面对抗阶段。对系统而言，在吸引入侵阶段，对抗结果的理想状态是入侵者取得博弈优势，其收益为正，主机被入侵，从而达到保护真实主机的目的；在全面对抗阶段，博弈的理想结果是系统较好地完成信息获取任务，而入侵者没有察觉。从一般的攻击步骤来看，吸引入侵阶段包括被动的侦察、主动的侦察和入侵系统 3 个步骤；全面对抗阶段则包括上传程序、下载数据、保持访问、隐藏踪迹 4 个环节。

### 3.3 不完全信息动态博弈

根据随机博弈的思想，诱骗主机的每一时期的历史都可以被概括为一种“状态”。一方当期的收益取决于这种状态和当期双方行为（黑客攻击行为，己方伪装保护措施）。通常，一个两人随机博弈用如下七元组描述：$(S,A_1,A_2,Q,R_1R_2,\beta)$，其中：—$S=\{\xi_1\cdots\xi_N\}$是状态集，博弈不断地由一个状态转换到下一个状态；—$AK=\{\alpha_{K_1}\cdots\alpha_{K_M}\}$ $R_2=\sum_{k=1}^{n}R_{2k}p_k$，$K=1,2.M_K=|A_K|$是参与人 $K$ 的策略集，参与人每一步的策略都是策略集的子集；—$Q:S\times A_1\times A_2\times S\rightarrow[0,1]$ 是状态转换方程，它决定了状态转换的方向；—$R_K:S\times A_1\times A_2\rightarrow R,K=1,2$ 是参与人 $K$ 的收益方程，它由当前状态、己方策略及对方策略确定；$0<\beta\leq 1$ 是折现率，用于参与人将未来收益折算到当前状态，一个高的折现率意味着参与人非常关心未来的收益。

一般的网络对抗博弈过程如下：在一个时刻 $t$，博弈处于状态 $S_t\in S$，攻击者从自己的策略集 $A_1$ 中选择策略 $\alpha_{1t}$，系统从自己的策略集中选择策略 $\alpha_{2t}$，然后攻击者得到一个收益 $r_{1t}=R_1(S_t,\alpha_{1t},\alpha_{2t})$，系统得到收益 $r_{2t}=R_2(S_t,\alpha_{1t},\alpha_{2t})$，然后博弈进入第二个状态 $S_{t+1}\in S$。

根据不完全信息动态博弈理论，在网络诱骗系统环境下，当期收益不仅取决于当前状态和这种状态下攻击者与系统的行为，还取决于双方针对对方类型所做的概率分布判断。例如在主动侦察状态，攻击者获取到诱骗主机的操作系统、所开的服务端口、系统漏洞等信息，根据随机博弈理论，攻击者的收益应该为 $r_{1t}=R_1(S_t,\alpha_{1t},\alpha_{2t})$，假设此时攻击者对主机是否是陷阱的概率判断为$(\mu,1-\mu)$，根据不完全信息博弈理论，其收益为 $r_{1t}=R_1(S_t,\alpha_{1t},\alpha_{2t},\mu)$，同理，假设此时系统对攻击者是否判断出身处陷阱的概率判断为$(\lambda,1-\lambda)$，此状态下其收益为 $r_{2t}=R_2(S_t,\alpha_{1t},\alpha_{2t},\lambda)$。

## 4 基于不完全信息动态博弈的信息获取策略选择

网络诱骗系统环境下，针对一个特定的状态，策略选择过程分以下 6 步。

（1）首先确定系统和攻击者双方的策略集。

（2）根据当前状态，确定针对系统不同的策略，攻击者对系统类型评估的概率 $\mu$ 分布。

（3）根据攻击者历史的攻击策略，系统首先确定攻击者类型的概率分布 ，然后在此基础上根据攻击者在当前状态下采取不同的策略，确定攻击者判断出自己身处监控的概率分布 $\lambda$。

（4）确定攻击者的收益函数。为了取得尽可能多的信息量（$I$），攻击者需要付出时间代价（$T$），由此确定攻击者的线性收益函数为：

$$R_1=(\alpha_1 I-\beta_1 T)(1-\mu) \quad (1)$$

其中，参数 $\alpha_1,\beta_1$ 由当前状态决定，变量 $I$、$T$ 由系统采取的策略决定，$\mu$ 为攻击者对系统是陷阱的判断概率。

（5）确定系统的收益函数。网络诱骗系统的目的在于保证自身安全的前提下，延长攻击者驻留时间，保护提供真实服务的主机；获取攻击者攻击信息，进行分析综合。所以系统的收益函数与攻击者需要付出时间代价（$T$），系统获取的信息（$I_1$），该攻击者获取的系统信息（$I_2$）相关。但对诱骗系统而言，对抗所处阶段不同，系统收益函数不同。在吸引入侵阶段，针对特定类型的攻击者，系统的线性收益函数为：

$$R_{2k}=-(\beta_2 T+\gamma I_1-\alpha_2 I_2)(1-\lambda) \quad (2)$$

其中：$\beta_2$、$\gamma$、$\alpha_2$ 由当前状态决定，$T$、$I_1$、$I_2$ 由攻击者采取的策略决定，$\lambda$ 为系统对攻击者判断出自己身处陷阱的判断概率。

在全面对抗阶段，针对特定类型的攻击者，系统的线性收益函数为：

$$R_{2k}=(\beta_2 T+\gamma I_1-\alpha_2 I_2)(1-\lambda) \quad (3)$$

假设系统对攻击者是类型 $K$ 的判断概率是 $p_k$，则对 $n$ 类攻击者，系统在该状态下的收益为：

$$R_2=\sum_{k=1}^{n}R_{2k}p_k \quad (4)$$

（6）计算纳什均衡解，确定信息获取策略。要达到纳什均衡解必须满足 3 个条件：系统采取行动实现自己的收益最大化；攻击者的收益尽可能高；攻击者没有发现自己被监控。

对攻击者而言，使得条件：

$$R_{1k}'=\mu_k' R_1(\alpha_{1k}',\alpha_{2k})\geq\mu_k R_1(\alpha_{1k},\alpha_{2k}),\alpha_{1k}'\in\alpha_{1k} \quad (5)$$

成立的策略 $\alpha_{1k}'$ 为其最优策略，其中 $R_{1k}'$ 表示攻击者在系统所有策略下的最大收益，$\mu_k'$ 为选择该策略下的攻击者的判断概率。

对诱骗系统而言，使得条件：

$$R_{2k}'=\lambda_k' R_2(\alpha_{1k}',\alpha_{2k})\geq\lambda_k R_2(\alpha_{1k},\alpha_{2k}),\alpha_{2k}'\in\alpha_{2k} \quad (6)$$

成立的策略 $\alpha_{2k}'$ 为其最优策略，其中 $R_{2k}'$ 表示系统在攻

击者所有策略下的最大收益，$\lambda_k'$为选择该策略下的系统的判断概率。

## 5 示例与仿真

按照攻击者实施攻击的基本步骤，把网络诱骗系统的工作过程简化为 7 个状态，为了对上述模型与方法进行初步验证，本文选取被动的侦察状态，对简化策略集进行仿真分析。

### 5.1 确定双方策略集

在被动的侦察状态下，系统的策略集 (*S*–*A*, system action)为：

$A^{system}$={提供服务漏洞，操作系统漏洞，提供服务漏洞和操作系统漏洞}。

攻击者的策略集为：

$A^{system}$={攻击主机，放弃攻击}。

### 5.2 确定攻击者对系统类型评估的概率$\mu$ 分布

把攻击者分为 3 类：高级攻击者，中级攻击者和初级攻击者。根据经验，概率 分布如表 1。

表 1　攻击者判断概率表

| 攻击者类型 \ 系统策略 / 概率 $\mu$ | 提供服务漏洞 | 操作系统漏洞 | 提供服务漏洞和操作系统漏洞 |
|---|---|---|---|
| 高级攻击者 | 50% | 60% | 70% |
| 中级攻击者 | 30% | 40% | 50% |
| 初级攻击者 | 10% | 20% | 30% |

由经验可知，经验丰富的攻击者往往比较谨慎，对获取的信息比较敏感。如操作系统漏洞，如果系统提供的漏洞很陈旧，就可能增加对系统是陷阱类型的判断概率。

### 5.3 确定系统对攻击者判断出自己身处陷阱的概率 $\lambda$ 分布

由于此时系统获取的攻击者历史攻击策略有限，所以系统初始化攻击者类型的概率 分布如表 2。

表 2　系统对攻击者类型的概率判断

| 攻击者类型 | 高级攻击者 | 中级攻击者 | 初级攻击者 |
|---|---|---|---|
| 概率 $\nu$ | 20% | 50% | 30% |

根据经验，系统对攻击者判断出自己身处陷阱的概率分布如表 3。

表 3　系统判断概率分布表

| 攻击者类型 \ 攻击者策略 / 概率 $\lambda$ | 攻击主机 | 放弃攻击 |
|---|---|---|
| 高级攻击者 | 60% | 80% |
| 中级攻击者 | 40% | 70% |
| 初级攻击者 | 20% | 50% |

### 5.4 确定攻击者在当前状态下的收益

攻击者在付出时间成本和获取被攻击主机信息两者之间，一般情况下，更看重获取的信息。令当前状态下，攻击者获取的信息 *I*，花费时间 *T* 如表 4。

表 4　(I, T)值表

| 攻击者类型 \ 系统策略 / (IT)值 | 提供服务漏洞 | 操作系统漏洞 | 提供服务漏洞和操作系统漏洞 |
|---|---|---|---|
| 高级攻击者 | (50,60) | (60,40) | (90,30) |
| 中级攻击者 | (45,80) | (50,60) | (80,50) |
| 初级攻击者 | (40,120) | (45,80) | (70,60) |

根据式 (1)，计算攻击者收益。因为攻击者类型不同其收益也不同。高级攻击者在系统不同的策略下的收益如表 5。

表 5　攻击者收益表

| 攻击者类型 \ 系统策略 / 收益 $R_1$ | 提供服务漏洞 | 操作系统漏洞 | 提供服务漏洞和操作系统漏洞 |
|---|---|---|---|
| 高级攻击者 | 235 | 232 | 265.5 |
| 中级攻击者 | 287 | 282 | 387.5 |
| 初级攻击者 | 306 | 328 | 469 |

### 5.5 确定系统在当前状态下的收益

根据系统延长攻击者驻留时间，获取攻击者攻击信息，保护自身安全的目的，令当前状态下，$\beta_2$=10, $\gamma$=10, $\alpha_2$=10，系统获消耗攻击者的时间 *T*，获取的信息 $I_1$，被攻击者获取的信息 $I_2$ 如表 6。

表 6　(T、$I_1$、$I_2$)值表

| 攻击者类型 \ 系统策略 / (T, $I_1$,$I_2$)值 | 攻击主机 | 放弃攻击 |
|---|---|---|
| 高级攻击者 | (30,10,90) | (1,1,3) |
| 中级攻击者 | (50,15,80) | (2,2,2) |
| 初级攻击者 | (60,20,70) | (3,3,1) |

根据式 (2) 、(4)，计算的系统的收益如表 7。

表 7　系统收益表

| 攻击者策略 | 攻击系统 | 放弃攻击 |
|---|---|---|
| 收益 $R_2$ | 6.1 | –1.01 |

### 5.6 计算纳什均衡解

根据式 (5)及表 7，攻击者的最优策略是攻击系统；根据式(6) 及表 5，系统的最优策略是向攻击者提供服务漏洞和操作系统漏洞。

## 6 结论

网络诱骗技术是网络信息对抗的核心技术之一，而信息获取又是系统实现其功能的关键。本文提出了一种基于不完全信息动态博弈的信息获取策略选择的方法，该方法基于对抗的动态性及对抗双方信息不完全的特点，把信息获取和不完全信息动态博弈有机结合，示例与仿真初步证明了模型的正确性和有效性。本文在类型概率确定、函数参数和变量的确定方面没有给出明确的算法，这也将是下一步研究的重点。

### 参考文献(References)

[1] 闫怀志, 胡昌振, 谭惠民. 网络攻防对抗策略选择模糊矩阵博弈方法[J]. 武汉大学学报(理学版), 2004, 50(S1): 103~106

[2]弗登博格等著,姚洋等译.博弈论[M]. 北京: 中国人民大学出版社, 2002. 95~112, 283~295

[3] Eric Cole 著, 苏雷等译. 黑客–攻击透析与防范[M]. 北京: 电子工业出版社, 2002. 18~45

[4] Lye Kong–wei, Wing Jeannette M. Game Strategies In Network Security [J]. http://www –2.cs.cmu.edu/~wing/publications/CMU – CS–02–136. pdf

[5] David Burke. Towards a game theory model of information warfare [J]. Master´s thesis, Graduate School of Engineering and Management, Airforce Institute of Technology, Air University, 1999.

[6] Jha S, Sheyner O, Wing J. Minimization and reliability analyses of attack graphs [J]. Carnegie Mellon University Technical Report CS–02–109, 2002

[7] 胡昌振. 信息安全的概念及方法论探讨 [J]. 科技导报,2004 (3):18~45

(责任编辑　胡春华)