

基于贝叶斯博弈的 MP2P 高性能安全资源节点选择策略

刘岩¹, 张国印¹, 何金洲², 徐锋¹

(1. 哈尔滨工程大学计算机科学与技术学院, 黑龙江 哈尔滨 150001; 2. 中国电信集团公司哈尔滨分公司, 黑龙江 哈尔滨 150001)

摘要: 针对 MP2P 网络节点运算能力有限、移动性强、可靠性弱导致网络拓扑结构频繁变化, 提出一种基于贝叶斯博弈的 MP2P 高性能安全资源节点选择策略。该策略首先综合考虑节点的性能、信誉, 设定了一种计算安全资源节点的方案, 然后采用静态贝叶斯博弈理论进行信任资源节点连接通信, 确保请求资源节点连接高性能安全资源节点, 该方案有效降低了资源节点的失效率, 提高了网络效率。

关键词: MP2P; 博弈; 安全; 资源节点选择

中图分类号: TP302.1

文献标识码: A

MP2P high capacity and security resource node selection strategy based on Bayesian game

LIU Yan¹, ZHANG Guo-yin¹, HE Jin-zhou², XU Feng¹

(1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China;

2. Harbin Branch, Company of China Telecom., Harbin 150001, China)

Abstract: Considering the changes of MP2P topology due to the limitation of the capability, the unreliable and the churn of the node, the efficiency and safety resource node selection strategy based on Bayesian game were proposed in MP2P network. Firstly, the safety resource calculation method was designed that takes the node capability and the node reputation into consideration. Secondly, adopting the Bayesian game theory to connect the resource nodes, ensuring the requesting node can intercommunicate with the high efficiency and safety resource node, the strategy can efficiently reduce failure rate of the resource nodes, greatly improving the network efficiency.

Key words: MP2P network, game, security, node selection

1 引言

MP2P(mobile peer-to-peer)是伴随着 P2P (peer-to-peer) 网络和移动计算领域的不断发展而形成的新型网络, 是一种动态分布式自组织覆盖网络。MP2P 网络中各自治对等移动节点间采用直接交互的方式进行数据资源的传输、共享以及各类服务的协同处理^[1]。

MP2P 网络大量节点频繁加入、离开以及节点不断移动所导致的一系列不稳定问题, 导致 MP2P 网络的管理维护较传统 P2P 网络更难。简单地将传统 P2P 网络中资源节点的选择方法移植到 MP2P 网

络会造成较长的查询延迟、资源节点较高的失效率、安全性无法保证等问题。

本文提出了基于贝叶斯博弈的高性能安全资源节点选择策略, 首先, 在网络资源节点选择上, 侧重那些信誉高、性能好的节点作为资源节点, 有效降低节点的失效率和缩短查询延迟。其次, 利用贝叶斯博弈理论进行资源节点连接通信, 请求资源节点可以较好地连接高性能安全资源节点, 进而提高资源下载率。

2 相关工作

目前, 有关 MP2P 网络资源节点选择方面的文

收稿日期: 2014-10-15; 修回日期: 2015-02-03

基金项目: 国家自然科学基金资助项目(No.61073042, No.61202455); 中央高校基本科研业务费专项基金资助项目(No.HEUCF100612)

Foundation Items: The National Natural Science Foundation of China (No.61073042, No.61202455), The Fundamental Research Funds for the Central Universities of China (No.HEUCF100612)

献较少。资源节点选择实质上要考虑 2 个关键因素，即节点性能（包括信息处理能力和在线时长）和节点的可靠性。文献[2]提出了 2 个方案：1) 采用贪婪算法选择出超级节点，节点度最大的节点作为资源节点，和其相连的邻居节点作为叶子节点；2) 采用 MIS(maximum independent set)算法选择资源节点。文献[3,4]分别采用模糊认知图和多属性决策理论对 MP2P 系统中节点服务能力进行综合评估。

针对 MP2P 网络节点可靠性的探讨工作如下。文献[5]首次提出使用信任来解决“当请求节点对陌生节点的历史行为不可知的情况下，是否与其进行交互的问题”，采用双层架构的拓扑模型，采用随机策略选择陌生节点，信任方案应具有分布式、轻量级的特征。文献[6]提出一种以信任理论为理念层、信任模型为可操作层、移动应用系统为应用层的可信框架。文献[7]提出了一种基于直接、间接信誉值评估的全局信誉值评估信任机制以保障 MP2P 安全。

3 MP2P 网络下资源节点的选择

3.1 资源节点性能计算

如前所述，选择资源节点一个很重要的指标是资源节点的性能。定义 3 个变量描述节点综合性能：Capacity、Time、Reputation，其中，Capacity 表示节点的信息处理能力；Time 表示节点的在线时间；Reputation 表示节点和传播资源文件的信誉。

1) 节点 i 的 Capacity 值计算如下

$$Capacity[i] = aBandwidth[i] + bCPUSpeed[i] + cStorage[i], a + b + c = 1 \quad (1)$$

其中，Bandwidth 为带宽，CPUSpeed 为 CPU 速度，Storage 为存储空间。Capacity 值的大小表明节点的性能高低。

2) 节点 i 的 Time 值计算如下

$$Time[i] = \left(\frac{1}{PeerSpeed[i] \left(\frac{Tage[i]}{t[i]} \right)} \right) \quad (2)$$

其中，PeerSpeed 为节点的移动速度；Tage 为节点总在线时间； t 为节点上线次数。MP2P 网络节点通信范围有限并随时在移动，节点的移动速度越慢，则越不容易超出此通信范围，不会造成节点频繁失效。此外，节点会在网络中存在多久无法预知，但从节点在网络中的历史在线时间估测其在该网络中存在的时间。

3) 节点 i 的 Reputation 计算如下

$$Reputation[i] = mR_i + nR_f, m + n = 1 \quad (3)$$

其中， R_i 为节点 i 的信誉， R_f 为传播文件的信誉。综合信誉由节点信誉和传播文件信誉组成，代表资源节点的可信度。

$$R_i = [l, w] \begin{bmatrix} T_{upload} \\ Y \end{bmatrix}, l + w = 1 \quad (4)$$

其中， T_{upload} 为节点 i 上载流量； Y 为曾与节点 i 交互过的节点对其的评价； R_f 为 Peer 节点间对所传播文件的整体评价。

综合以上因素，算法周期性地对节点 i 进行评分

$$score[i] = aCapacity[i] + \beta Time[i] + g Reputation[i], a + \beta + g = 1 \quad (5)$$

采用熵权法确定节点 i 的性能指标权重。第 i 个指标的信息熵计算式为

$$E_i = -(\ln n)^{-1} \sum_{j=1}^n p_{ij} \ln p_{ij}, i = 1, 2, \dots, m$$

其中， n 为可获资源节点数目， m 为性能指标数目，且 $p_{ij} = r_{ij} \sum_{j=1}^n r_{ij}$ ， r_{ij} 表示第 j 个资源节点的第 i 个指标的状态值。第 i 个指标的熵权为

$$w_i = \frac{1 - E_i}{m - \sum_{i=1}^m E_i}, i = 1, 2, \dots, m \quad (6)$$

指标的信息熵 E_i 越小，其权重越大。反之，某指标的信息熵 E_i 越大，则其权重也应越小。

score 值存于各节点中，当请求资源节点发出资源请求时，资源节点根据性能排序形成请求节点可获得的资源列表，如图 1 所示。当新节点加入或资源节点的离开将触发更新请求资源列表。

节点ID	IP地址	端口	信誉值
1			
2			
...			
...			
$n-1$			
n			

图 1 资源列表

MP2P 网络节点处于对等地位，节点的异质性、能力的差异、匿名性、在线时间长短等都成为影响实

时性的关键^[8]。节点选择策略应充分考虑这些因素，选择合适的节点，避免恶意节点攻击以及节点失效导致的任务重调度等，从而提高系统的实时性。

3.2 贝叶斯博弈节点选择策略

MP2P 网络中节点资源有限，大量节点失效会引起整个 MP2P 网络被分割，造成系统瘫痪。因此，如何从请求资源列表中选取出安全高性能资源节点为请求节点提供服务成为一个关键问题。

MP2P 网络中的节点本身是中性的，但操作者的善恶以及理性使节点具有了善恶、理性的属性。这样一来，节点变为具有理性的智能体，问题可以理解为“理性智能体间的竞争与协作问题”，相应地可以建立博弈模型给出解决问题的方案。

1) 设 RP_i 为请求资源节点， $i \in Z^+$ ， L_{NID} 为 RP_i 可获资源列表中的资源节点集合， $NID \in Z^+$ 。

2) RP_i 从 $L_{NID} = \{NID | L_{NID}, NID \in Z^+\}$ 中选择安全高性能节点集合 U_{score} 。

假设 RP_i 与 $L_{NID} = \{NID | L_{NID}, NID \in Z^+\}$ 的每一元素博弈后得到安全高性能节点集合 U_{score} ， RP_i 与 $L_{NID} = \{NID | L_{NID}, NID \in Z^+\}$ 中任意元素的博弈是完全独立的。进而可以将问题转换为 l 组独立的 2 人非合作不完全信息静态博弈问题。采用并行同步处理可以同时获得一组安全高性能的节点组合。

定义 1 贝叶斯静态博弈 (2 人非合作的不完全信息静态博弈) 表示为 $G = [N, \{T_i\}, P, \{S_i(t_i)\}, \{u_i\}]$ 。

1) 参与者集合 $N = \{1, 2\}$ 。

2) 每个参与者具有各自类型集合，类型集合 $T = \prod_{i=1}^n T_i$ 上的概率分布为 $P(t_1, t_2, \dots, t_n)$ 。

3) 每个参与者与其类型 t_i 相关的策略集 $S_i = \{s_i\}, i \in N$ ，且 S_i 和其他参与者的类型无关。

4) 每个参与者均有各自的效益函数 $u_i(s_1, s_2, \dots, s_n, t_i)$ 。

以上 4 个要素同时具有，参与者同时选择各自策略以追求各自利益最大化。节点 RP_i 与节点 L_{NID} 的博弈过程描述如下。该博弈范式如表 1 所示。

1) 节点 RP_i 从获取到的资源列表中选择高性能安全的节点。

2) 资源列表中的节点 L_{NID} 可能为高性能的善意节点和高性能恶意节点的一种。

3) 节点 RP_i 知道 L_{NID} 的类型空间，但不知道 L_{NID} 是哪一类型，仅 L_{NID} 自己知道。

表 1 RP_i 与 L_{NID} 的博弈范式

节点	资源节点 L_{NID}	请求资源节点 RP_i	
		互连	不互连
高性能善意节点	为 RP_i 提供无污染资源	(1, 1)	(0, -2)
	不为 RP_i 提供资源	(0, -1)	(0, 0)
高性能恶意节点	为 RP_i 提供污染资源	(1, -2)	(-1, 1)
	为 RP_i 提供病毒资源	(2, -4)	(-2, 2)

经海萨尼转换可知，自然确定 L_{NID} 有 2 种类型， $T_1 = \{t_{11}, t_{12}\}$ ，其中， t_{11} 代表高性能善意节点， t_{12} 代表高性能恶意节点。而 RP_i 类型确定为 $T_2 = \{t_2\}$ 。

当 L_{NID} 为高性能善意节点时，其策略集 $S_1(t_{11}) = \{s_1^{(1)}(t_{11}), s_2^{(1)}(t_{11})\}$ ， $s_1^{(1)}(t_{11})$ 表示 RP_i 提供安全无污染的资源， $s_2^{(1)}(t_{11})$ 表示不为 RP_i 提供资源。 L_{NID} 选用 $s_1^{(1)}(t_{11})$ 策略的概率为 x_1 ，选用 $s_2^{(1)}(t_{11})$ 策略的概率为 $(1 - x_1)$ ， $x_1 \in [0, 1]$ 。

当 L_{NID} 为高性能恶意节点时，其策略集 $S_1(t_{12}) = \{s_1^{(1)}(t_{12}), s_2^{(1)}(t_{12})\}$ ， $s_1^{(1)}(t_{12})$ 表示为 RP_i 提供污染的资源， $s_2^{(1)}(t_{12})$ 表示为 RP_i 提供携带病毒的资源。 L_{NID} 选用 $s_1^{(1)}(t_{12})$ 策略的概率为 x_2 ，选用 $s_2^{(1)}(t_{12})$ 策略的概率为 $(1 - x_2)$ ， $x_2 \in [0, 1]$ 。

RP_i 的策略集为 $S_2(t_2) = \{s_1^{(2)}(t_2), s_2^{(2)}(t_2)\}$ ， $s_1^{(2)}(t_2)$ 表示 RP_i 与 L_{NID} 互连， $s_2^{(2)}(t_2)$ 表示 RP_i 与 L_{NID} 不互连。 RP_i 选用 $s_1^{(2)}(t_2)$ 策略的概率为 y ，选用 $s_2^{(2)}(t_2)$ 策略的概率为 $(1 - y)$ ， $y \in [0, 1]$ 。

设 RP_i 遇到高性能善意 L_{NID} 的概率为 a ， RP_i 遇到高性能恶意 L_{NID} 的概率为 $1 - a$ 。

$$a = \frac{\|score[i] > k\|}{l} \tag{7}$$

其中， $\|score[i] > k\|$ 表示超过性能阈值 k 的节点个数， l 为所获资源列表长度。

将 L_{NID} 为高性能善意节点时的期望收益记为 $E_1^G(x_1, y)$ ， L_{NID} 为高性能恶意节点时的期望收益记为 $E_1^B(x_2, y)$ ， RP_i 的期望收益记为 $E_2(x_1, x_2, y)$ ，则有

$$E_1^G(x_1, y) = (x_1, 1 - x_1) \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} (y, 1 - y)^T = x_1 y \tag{8}$$

$$E_1^B(x_2, y) = (x_2, 1 - x_2) \begin{bmatrix} 1 & -1 \\ 2 & -2 \end{bmatrix} (y, 1 - y)^T = x_2 + 4y - 2x_2 y - 2 \tag{9}$$

$$\begin{aligned}
 E_2(x_1, x_2, y) &= a(x_1, 1-x_1) \begin{bmatrix} 1 & -2 \\ -1 & 0 \end{bmatrix} (y, 1-y)^T + \\
 &\quad (1-a)(x_2, 1-x_2) \begin{bmatrix} -2 & 1 \\ -4 & 2 \end{bmatrix} (y, 1-y)^T \\
 &= (4ax_1 - 3ax_2 + 3x_2 + 5a - 6)y - \\
 &\quad 2ax_1 + (a-1)x_2 - 2a + 2 \quad (10)
 \end{aligned}$$

设 $((x_1, 1-x_1), (x_2, 1-x_2), (y, 1-y))$ ，即高性能善意节点、高性能恶意节点、请求节点的策略概率组合为混合策略贝叶斯纳什均衡解，由混合策略贝叶斯纳什均衡充分必要条件^[9]，可以得到一组不等式

$$\begin{cases} E_1^G(x_1=0, y) & E_1^G(x_1, y) \\ E_1^G(x_1=1, y) & E_1^G(x_1, y) \\ E_1^B(x_2=0, y) & E_1^B(x_2, y) \\ E_1^B(x_2=1, y) & E_1^B(x_2, y) \\ E_2(x_1, x_2, y=0) & E_2(x_1, x_2, y) \\ E_2(x_1, x_2, y=1) & E_2(x_1, x_2, y) \end{cases} \quad (11)$$

将 $x_1=0$ 和 $x_1=1$ 分别代入式 (8) 化简得到不等式组

$$\begin{cases} x_1 y & 0 \\ y(1-x_1) & 0 \end{cases} \quad (12)$$

将 $x_2=0$ 和 $x_2=1$ 分别代入式 (9) 化简得到不等式组

$$\begin{cases} x_2(1-2y) & 0 \\ (1-2y)(x_2-1) & 0 \end{cases} \quad (13)$$

将 $y=0$ 和 $y=1$ 分别代入式 (10) 化简得到不等式组

$$\begin{cases} [4ax_1 - 3x_2(a-1) + 5a - 6]y & 0 \\ [4ax_1 - 3x_2(a-1) + 5a - 6](y-1) & 0 \end{cases} \quad (14)$$

采用双矩阵博弈的求解方法可得如下结果。

1) 当 $a = \frac{1}{2}$ 时，原博弈的贝叶斯纳什均衡解的集合为 $\{(1,0), (0,1), (1,0)\} \cup \{(1,0), (1,0), (y, 1-y)\}$ ，

$$y \in \left[0, \frac{1}{2}\right]。$$

2) 当 $a > \frac{1}{2}$ 时，贝叶斯纳什均衡解为

$$\{(1,0), (0,1), (1,0)\} \cup \left\{ (1,0), \left(\frac{2-3a}{1-2}, \frac{2a-1}{1-a} \right), \left(\frac{1}{2}, \frac{1}{2} \right) \right\}。$$

3) 当 $a < \frac{1}{2}$ 时，无解。

3.3 RP_i 的节点选择策略

1) 当 RP_i 获得高性能善意节点 L_{NID} 的概率为 $\frac{1}{2}$ 时，存在 2 种策略。

纯策略贝叶斯纳什均衡：高性能善意 L_{NID} 节点为 RP_i 提供安全无污染资源；高性能恶意 L_{NID} 节点为 RP_i 提供病毒资源，而 RP_i 与 L_{NID} 节点互连。

无穷多个混合策略下的贝叶斯纳什均衡：高性能善意 L_{NID} 节点为 RP_i 提供安全无污染资源；高性能恶意 L_{NID} 节点为 RP_i 提供污染资源，而 RP_i 以概率 y ($0 < y < 0.5$) 和 L_{NID} 节点互连，以概率 $(1-y)$ 不和 L_{NID} 连接。

2) 当 RP_i 获得高性能善意节点 L_{NID} 的概率超过 $\frac{1}{2}$ 时，也存在 2 种策略。

纯策略贝叶斯纳什均衡：高性能善意 L_{NID} 节点为 RP_i 提供安全无污染的污染资源；高性能恶意 L_{NID} 节点为 RP_i 提供病毒资源，而 RP_i 和 L_{NID} 节点互连。

是无穷多个混合策略下的贝叶斯纳什均衡：高性能善意 L_{NID} 节点为 RP_i 提供安全无污染资源；高性能恶意 L_{NID} 节点以概率 $\frac{2-3a}{1-a}$ 为 RP_i 提供污染资源，以概率 $\frac{2a-1}{1-a}$ 为 RP_i 提供病毒资源，而 RP_i 以概率 $\frac{1}{2}$ 和 L_{NID} 节点互连，以概率 $\frac{1}{2}$ 不和 L_{NID} 连接。

3) 当 RP_i 获得高性能善意 L_{NID} 节点的概率低于 $\frac{1}{2}$ 时， RP_i 不和 L_{NID} 节点连接。

4 实验分析

4.1 环境配置

硬件环境为 1.73 GHz 双核处理器和 2 GB 内存。软件为 NS-2.29 仿真平台。仿真实验所需有关参数设置如表 2 所示。

4.2 效率测试

为验证应用本文算法资源节点失效率较低和实时性较高，将本文算法和 MIS 算法^[10]做测试比较如图 2 所示。

从图 2 可知，在相同运行时间内本文算法比 MIS 算法资源节点失效率低，2 种算法资源节点失效率随时间推移均变大，MIS 算法节点失效率增幅加大，而本文算法节点失效率增幅相对较慢，差异

程度约 45%。因此，采用本文算法请求资源节点可获目标资源节点活动周期长，网络更加稳定。

表 2 参数设置	
参数	值
节点总数 N_{total}	100
区域面积 S_{area}	800 m × 550 m
平均节点个数 $\bar{k}_{cluster}$	10
移动模型	Random Waypoint
节点移动速度	1.2 m/s
节点在线时间	5 000 s
初始恶意节点比例	5%
MAC	802.11
信道带宽	11 bit/s
数据分组大小	256 byte
传输距离	250 m
误码率 BER	10%
仿真时间	3 600 s

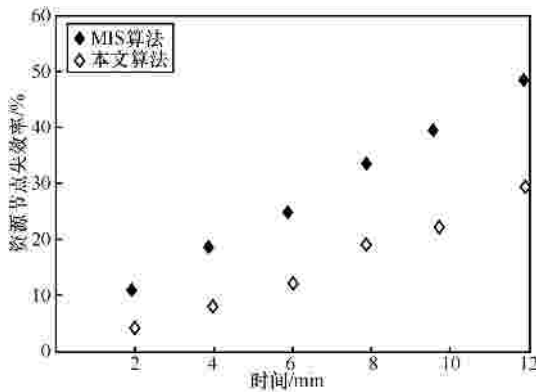


图 2 资源节点失效率

查询延迟是影响实时性的重要因素。好的节点选择算法不仅可提高任务执行的成功率，还能避免因节点离开或失效导致的任务重调度，降低查询延迟，提高系统实时性如图 3 所示。

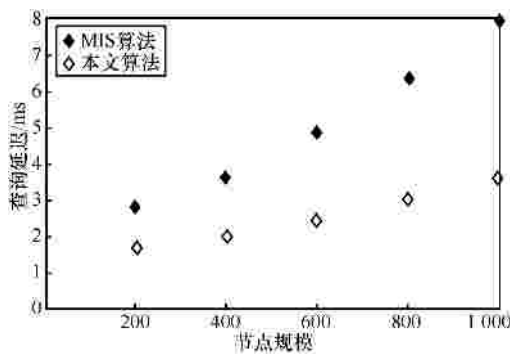
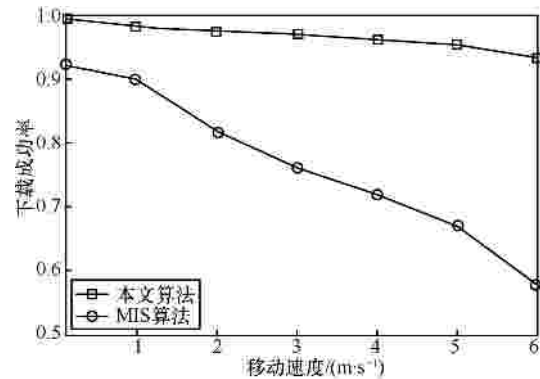


图 3 查询延迟

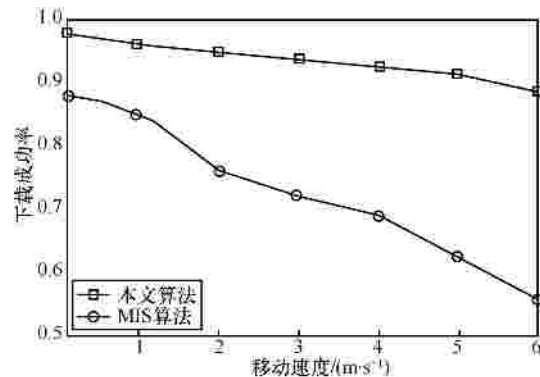
从图 3 可知，随着节点规模的增加，MIS 算法查询延迟增幅较大，而本文算法查询延迟增幅相对

较小。因为采用本文算法能够连接到高性能安全节点，可避免由节点失效以及恶意节点被入侵检测系统检测出来所引发的任务重调度。一方面，减少了节点失效而导致请求信息的发送次数，另一方面，减少了恶意节点提供病毒资源被入侵检测系统检测出来所消耗的时间，从而大大降低了查询延迟，系统的实时性较高。

考察恶意节点占节点总数 5%和 15%这 2 种情况下的下载成功率。横坐标表示节点的移动速度，纵坐标表示下载成功率。采用本算法后和采用 MIS 算法的下载成功率如图 4 所示。



(a) 恶意节点占节点总数 5%的情况



(b) 恶意节点占节点总数 15%的情况

图 4 下载成功率对比分析

从图 4 中曲线变化趋势分析可知，应用本文算法后，下载成功率曲线下降趋势放缓，能够适应不同速度的变化，这是由于在资源节点的选择策略上增加了对于相关指标因素的评价，而采用 MIS 算法的下载成功率随节点速度增加后下降很大。1.2 m/s 属于一个临界值。

为此，本文假定在通信范围内节点保持在线，并以 1.2 m/s 的移动速度移动，测试了该情况下恶意节点分别为 15%、35%、50%、70%的状态下资源下载成功率和资源下载成功平均时间如图 5 所示。

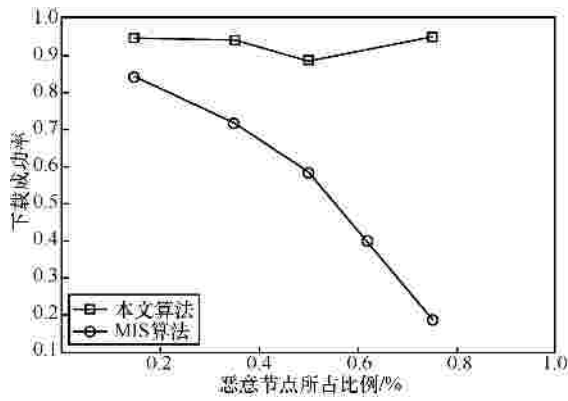


图 5 移动速度恒定时下载成功率随恶意节点变化趋势

从图 5 中可知，随着恶意节点增加，采用 MIS 算法的下载成功率锐减，当恶意节点占节点总数 70% 时，下载成功率较低为 19.8%。而本文算法当恶意节点达到 50% 时最低，其他情况下下载率基本在 85% 以上。从图 6 中曲线变化趋势分析可知，应用本文算法后，下载成功平均时间曲线增长趋势放缓，这是由于采用静态贝叶斯博弈节点选择策略总能连接高性能安全资源节点，将恶意节点隔离，节省连接恶意节点所消耗的时间，而采用 MIS 算法的下载成功平均时间随恶意节点比例增加增幅很大。

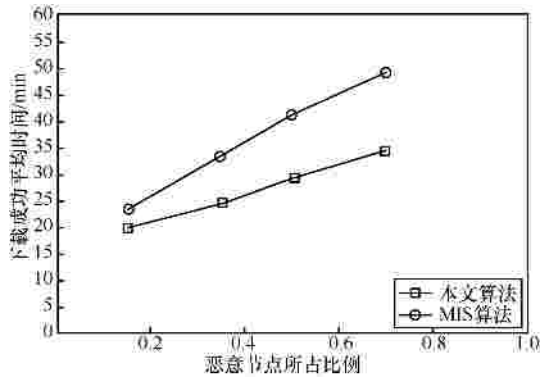


图 6 移动速度恒定时下载成功平均时间随恶意节点变化趋势

5 结束语

MP2P 网络中节点具有性能有限，高移动性，安全性未知等特点，选择高性能安全资源节点对保证网络稳定、降低系统开销、信息存储等方面起到关键作用。本文提出一种根据节点性能选择资源节点，并使用贝叶斯博弈理论与资源节点互连，保证资源节点的可靠性。理论分析和实验结果一致表明，使用该方法的资源请求节点总能选择连接高性能安全资源节点，保证资源无污染性和安全性，有

效降低资源节点失效率，提高整体网络效率。在之后的研究中，可将网络信誉机制灵活应用于实时任务调度，构建高效的实时性节点选择策略。

参考文献：

- [1] NIU X Z. Research on Key Issues of Mobile Peer-to-peer Networks [D].Chengdu: University of Electronic Science and Technology of China, 2008.
- [2] HAN J S, LEE K J, SONG J W, et al. Mobile peer-to-peer systems using super peers for mobile environments[C]//ICOIN ' 08. New York, USA, c2008: 1-4.
- [3] LIU S H. Research on Peer Selection Algorithm of Mobile P2P Networks [D].Chengdu: University of Electronic Science and Technology of China, 2012.
- [4] XIA H L, WANG N. Neighbour peer selection scheme based on effective capacity for mobile peer-to-peer streaming[J]. Digital Communications, 2013, 10(5):89-98.
- [5] PALOMAR E. Dealing with sporadic strangers, or the (un) stability of trust for mobile P2P security[C]//The 18th International Workshop on Database and Expert Systems Applications. Piscataway, IEEE Press, c2007: 779-783.
- [6] ZHENG Y. A conceptual architecture of a trusted mobile environment[C]//The Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing. Piscatawa , IEEE Press, c2006: 75-81.
- [7] PENG H. Research on Security Schemes in Complex Peer to Peer Network Systems [D].Shanghai: Shanghai Jiaotong University,2012.
- [8] YAO J, LI Z W, GUO B. Real-time performance of peer-to-peer network [J]. Application Research of Computers, 2011, 28(1):20-24.
- [9] WANG X Y, XIAO Y M. Game Theory and its Application[M]. Beijing: Science Press, 2008.
- [10] FENG W F, HUANG Y C. Research on MIS algorithm of SINR model in wireless sensor networks[J]. Microelectronics & Computer, 2014, 31(6): 166-170.

作者简介：



刘岩（1980-），男，山东莱州人，哈尔滨工程大学博士生，主要研究方向为移动对等网、人工免疫等。

张国印（1962-），男，山东黄县人，哈尔滨工程大学教授、博士生导师，主要研究方向为网络与信息安全、嵌入式系统等。

何金洲（1979-），男，黑龙江哈尔滨人，中国电信集团哈尔滨分公司助理工程师，主要研究方向为移动对等网、3G/4G 无线网络优化及协议等。

徐锋（1977-），男，河北沧州人，哈尔滨工程大学博士生，主要研究方向为移动对等网、信息系统安全等。