

# 基于协同进化免疫网络的云计算病毒检测算法

程春玲, 柴倩, 徐小龙

(南京邮电大学 计算机学院, 江苏 南京 210003)

**摘要:** 提出一种基于协同进化免疫网络的云计算病毒检测算法。算法引入测试集, 在免疫网络的构建和进化阶段分别通过检测器对测试集的适应度和检测器与抗原的刺激水平, 实现检测器之间的协同进化, 不断优化免疫网络中的检测器, 提高整个免疫网络对云平台的病毒检测能力和检测效率。给出基于 MapReduce 的免疫网络构建算法的实现。仿真结果表明, 基于协同进化免疫网络的云计算病毒检测算法能有效提高检测器的检测效率, 降低检测器集的冗余度, 提高了整个云计算平台的病毒检测率和安全性。

**关键词:** 云计算; 免疫网络; MapReduce; 病毒检测

中图分类号: TP309.5

文献标识码: A

文章编号: 1000-436X(2011)9A-0001-07

## Cloud computing virus detection algorithm based on co-evolution immune network

CHENG Chun-ling, CHAI Qian, XU Xiao-long

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

**Abstract:** A virus detection algorithm based on co-evolution immune network for cloud computing was proposed. The algorithm introduce the test set. In the immune network construction and co-evolution phases, detectors are co-evolved through the fitness between detectors and test set, and the stimulating level between detectors and antigens to optimize the detectors in immune network continuously. So the ability of virus detection in the cloud platform was improved. Furthermore, the implementation of the immune network construction algorithm based on MapReduce was presented. Simulation results show that the proposed algorithm can improve the detection efficiency and reduce the redundancy of detectors effectively. The virus detection rate and security of the entire cloud computing platform are improved.

**Key words:** cloud computing; immune network; MapReduce; virus detection

## 1 引言

在云计算平台中, 大量的低成本服务器通过网络互联在一起, 一旦一个节点遭受病毒攻击, 病毒很容易在云平台中快速蔓延, 威胁到互联的所有服务器的安全。因此, 必须通过有效的方法迅速检测

和处理云计算环境下的病毒, 保障云平台的安全。计算机免疫网络是对生物免疫系统的模拟, 它具备强大的信息处理能力, 且能自适应地识别已知和未知病毒, 可有效提高网络系统的安全性。另外, 云计算平台通过并行计算技术将庞大的计算处理程序自动拆分成无数个小个子程序, 交由多部服务器

收稿日期: 2011-04-15

基金项目: 国家自然科学基金资助项目(61071093, 60873231); 高等学校博士学科点专项科研基金资助课题(20093223120001); 江苏省科技支撑计划(BE2009158); 江苏省高校自然科学基金项目(09KJB520010)

Foundation Items: The National Natural Science Foundation of China(61071093, 60873231); The Research Fund for the Doctoral Program of Higher Education(20093223120001); The Science and Technology Support Program of Jiangsu Province(BE2009158); The Natural Science Fund of Higher Education of Jiangsu Province(09KJB520010)

经搜寻、计算、分析之后将处理结果合并后回传给用户<sup>[1]</sup>。云计算平台这种强大的处理能力为构建免疫网络提供了良好的基础。

本文对云计算平台提出一种基于协同进化免疫网络的病毒检测算法,通过测试集、抗原和检测器之间的协作,使组成免疫网络的检测器不断进化,从而实现整个免疫网络的协同进化。算法在免疫网络构建过程中引入测试集,通过计算检测器对测试集的适应度,消除网络中适应度低的检测器来降低检测器集的冗余度,提高免疫网络中记忆检测器的检测效率。免疫网络通过周期性地选择对抗原刺激水平高的检测器进行克隆变异,使云计算平台中的各个检测器集不断进化以实现整个免疫网络的协同进化,从而提高云计算平台对病毒的检测能力和检测效率。同时,给出了基于 *MapReduce* 的免疫网络构建算法的实现,通过服务器强大的并行处理能力,加速免疫网络构建。

## 2 相关工作

在云计算环境中,病毒检测主要是通过大量形成网状的客户端对网络中的软件行为进行异常监测来获取网络中病毒的最新信息,推送到云端服务器进行自动分析和处理,再将病毒的解决方案分发给每一个客户端。云计算技术拓宽了杀毒软件提供安全服务的范围和层次,每个用户通过云端服务器拦截病毒的同时向服务器提供可疑的病毒信息。文献[2]介绍了基于云安全相关技术,描述了计算机如何利用存储在互联网云服务器上的数据保护网络中的计算机安全。文献[3]提出了一种基于人工免疫系统的云安全模型,该模型结合了本地主机检测器代理和云端多检测引擎技术,实现多个检测引擎在云中并行检测病毒。文献[4]提出了一种基于云安全的军用网络病毒检测模型,通过引入云安全技术开发了一个新的军用信息网络安全保护系统。

目前,以自然免疫为原型的人工免疫模型在病毒检测中取得了较好的结果,成为一个可行的发展方向。人工免疫模型大致可以分成基于克隆选择理论和基于免疫网络理论的模型 2 类。在基于克隆选择理论的模型中,各个免疫细胞均为离散的,因此个别免疫细胞的识别能力突出,但忽略了免疫细胞整体的识别能力<sup>[5]</sup>。基于免疫网络理论的模型认为,免疫系统是一个由免疫细胞组成的能够互相识别、

刺激和协调的动态平衡网络。目前典型的免疫网络理论模型是 *Timmis* 等提出的资源受限人工免疫系统<sup>[6]</sup>和 *deCasto* 等人提出的 *aiNet* 人工免疫网络<sup>[7]</sup>。*aiNet* 免疫网络把整个免疫系统看成一个由免疫细胞组成的能够相互作用的网络,通过免疫细胞之间的连接相互协作,保持免疫网络中的细胞处于稳定状态。*aiNet* 免疫网络模型是一个边界加权图,该模型通过计算抗体与抗原之间的亲和力,对亲和力高的抗体进行克隆变异和网络抑制后,剩余抗体之间以亲和力为权值建立连接。但是,*aiNet* 免疫网络模型存在过分依赖网络抑制来降低冗余度、运算量大、执行速度慢等问题。本文认为若在记忆检测器生成过程中增加检测器与测试集之间的协同进化,可增加网络中检测器的多样性,同时通过网络抑制降低网络中检测器的冗余度,提高网络未知病毒检测效率。

## 3 基于协同进化的免疫网络病毒检测算法

### 3.1 设计思想

本文认为若在免疫网络中引入测试集,通过计算检测器对测试集的适应度删除免疫网络中适应度低的检测器,可降低检测器集的冗余度。在对检测器进行克隆变异前,通过计算检测器受抗原的刺激水平,选择刺激水平高的检测器进行克隆变异,不仅可增加记忆检测器的多样性,而且可使网络中检测器不断进化,从而通过测试集、抗原与检测器之间的协同达到整个免疫网络的进化,提高整个云计算平台的病毒检测能力。免疫网络的构建过程可基于 *MapReduce* 并行实现,能充分利用云平台对海量数据的高效分析处理能力,提高算法的运行效率。

因此,提出了检测器与测试集之间的适应度和检测器受抗原的刺激水平的概念,通过测试集和抗原与检测器之间的协作,使免疫网络中的记忆检测器集合协同进化,从而提高对云计算平台中病毒的识别能力。算法主要可以分为免疫网络构建、免疫网络的进化和病毒检测 3 个阶段。在免疫网络构建阶段,云平台中各服务器独立生成初始检测器,并将整个云环境中的初始检测器看作一个整体,以检测器之间亲和力为权值在所有服务器之间构建以检测器为节点的免疫网络。随后,进入免疫网络的协同进化阶段,云平台中的服务器各自周期性的执行免疫网络动态平衡算法

使整个免疫网络中的检测器集不断进化。最后，云平台中的服务器利用免疫网络中的记忆检测器检测云环境中的病毒，提高整个云计算平台的病毒检测率和安全性。

### 3.2 相关定义

**定义 1** 抗原集合：已知病毒的特征码经排列组合后得到的长度为  $L$  位的二进制字符串集合，用  $Ag$  表示。

**定义 2** 检测器：又称抗体，用于检测网络中异常的长度为  $L$  位的二进制字符串集合，用  $Ab$  表示。

**定义 3** 测试集  $T$ ：经预先处理的、与病毒特征库中的特征码相似的数据集合，每个元素均为长度  $L$  位的二进制字符串。可由云计算平台中的每个节点收集。

**定义 4** 亲和力：检测器集与抗原集合或测试集之间的匹配程度，可通过式(1)计算：

$$f_{i,j} = \text{Affinity}(F_i, F_j) = 1 / D_{ij} \quad (1)$$

其中， $F_i$  为检测器集中的个体、 $F_j$  为抗原集或测试集中的个体， $D_{ij}$  表示  $F_i$  与  $F_j$  之间的几何距离，

$$D_{ij} = \|F_i - F_j\|, \quad i, j = 1, \dots, N, \quad i \neq j$$

**定义 5** 适应度：检测器对测试集中所有元素的适应程度。

设测试集  $T$  中有  $q$  个元素，则检测器  $Ab_i$  对测试集  $T$  的适应度为

$$\text{fitness}(Ab_i) = \sum_{j=1}^q h_{i,j} \quad (2)$$

其中， $h_{i,j} = \begin{cases} 1, & f_{i,j} \geq d \\ 0, & \text{其他} \end{cases}$ ， $i, j = 1, 2, \dots, q, i \neq j$ ； $d$  为预先设定的阈值， $0 \leq d \leq 1$ ； $f_{i,j}$  为检测器  $Ab_i$  与测试集中的元素  $T_j$  之间的亲和力，按式(1)计算。

**定义 6** 刺激水平：描述检测器受一定比例的抗原的刺激程度，可以用  $\sum_{j=1}^m f_{i,j}$  与  $\sum_{k=1}^n f_{i,k}$  的和来衡量。检测器  $Ab_i$  的刺激水平可表示为

$$s_i = \sum_{j=1}^m f_{i,j} + \sum_{k=1}^n f_{i,k} \quad (3)$$

式中， $m$  为检测器接触的抗原的数量， $n$  是与该检测器相连的检测器数目， $f_{i,j}$  表示检测器  $Ab_i$  抗原  $Ag_j$  之间的亲和力， $f_{i,k}$  表示与检测器  $Ab_i$  与其相连的检测器  $Ab_k$  之间的亲和力。

## 3.3 基于协同进化的免疫网络病毒检测算法

### 3.3.1 免疫网络的构建

aInet 免疫网络模型中的检测器是通过克隆选择生成的，免疫细胞间缺乏相互协作，检测器之间仅通过相互抑制来减少检测器数量，降低冗余度。本文在免疫网络构建过程中引入测试集，通过计算检测器与测试集之间的适应度，删除免疫网络中适应度低的检测器。即在免疫网络构建过程中通过检测器与测试集之间的相互协作，消除网络中检测效率低的检测器，克服了 aInet 免疫网络仅通过网络抑制来降低冗余度的缺点。免疫网络的构建主要包括 3 个步骤。

1) 首先通过克隆变异和网络抑制生成记忆检测器集合；

2) 计算记忆检测器集合中各元素之间的亲和力，以亲和力为权值建立网络连接，并构建记忆检测器关系矩阵；

3) 计算各检测器对测试集的适应度，删除适应度低的检测器及其与其他检测器之间的连接，完成免疫网络的构建。

算法详细描述如下：

**算法 1** 免疫网络的构建算法

输出：记忆检测器集  $Ab_{(m)}$

Procedure Co-Evo\_ImNet\_algorithm ( $Ab_{(m)}$ )

Begin

If (count ( $Ab_{(m)}$ ) = 0)

Then Initial ( $Ab$ ) ;

//初始化，生成大量初始检测器

For (count ( $Ab_{(m)}$ ) < S) do

//初始构建的免疫网络中记忆检测器的数量为 S

Begin

For ( $Ag_j \in Ag$ ) do //对抗原集中每个元素  $Ag_j$

Begin

For ( $Ab$ ) do

Begin

Affinity ( $Ag_j, Ab_i$ ) ;

//计算  $Ag_j$  和检测器  $Ab_i$  的亲和力，

$i = 1, \dots, N$

Select ( $Ab \in Ab_{(n)}$ ) ;

//选择亲和力高的  $n$  个检测器为检测器

```

子集  $Ab_{\{n\}}$ 
Clone ( $Ab_{\{n\}}$  C ); //克隆  $Ab_{\{n\}}$  产生 C
Mutation (C C* ); //对 C 变异为 C*
End;
End;
For (C*) do //计算 C* 中各元素的亲和力
//并以亲和力为权值建立免疫网络
Begin
Affinity ( $C_i^*$ ,  $C_j^*$ ); //计算亲和力
Delete ( $C_i^*$ ,  $C_j^*$ );
//消除亲和力阈值高于  $d_d$  的检测器
Connect ( $C_i^*$ ,  $C_j^*$ );
//剩余检测器以亲和力为权值构建关系矩阵
Fitness ( $C_i^*$ , T); //计算适应度
Delete ( $C^* - > Ab_{\{m\}}$ );
//删除适应度低的检测器形成记忆检测器集
 $Ab_{\{m\}}$ 
End;
End;

```

### 3.3.2 基于协同进化的免疫网络动态平衡

免疫网络中记忆检测器越多，则维护免疫网络和检测病毒所需要的时间和空间开销越大，影响检测效率，为此在保持一定数量记忆检测器的同时，尽可能的提高所有检测器的检测能力。本文在免疫网络的进化阶段引入记忆检测器与抗原集合之间的协同进化，通过计算记忆检测器与抗原集合的刺激水平，选择刺激水平高的记忆检测器进行克隆变异，使其进化，产生检测效率高的记忆检测器。并选择变异后与原检测器差异较大的记忆检测器加入免疫网络，降低记忆检测器冗余度的同时增加网络中记忆检测器的多样性，提高免疫网络中检测器的整体检测能力。免疫网络的进化由基于协同进化的免疫网络动态平衡算法实现。免疫网络的动态平衡算法是免疫网络的一次动态调整过程，该过程通过协同进化策略提高免疫网络检测器的整体检测能力，从而提高云计算平台病毒检测的效率。云计算平台中的各服务器周期性的独立执行此算法以维护服务器之间免疫网络的动态平衡，其主要步骤如下。

1) 从抗原集合中随机选择一个抗原子集进入免疫网络，消除免疫网络中被抗原刺激但亲和力低

于阈值  $d_s$  的检测器，即清除网络中自然死亡的记忆检测器；

2) 计算所有亲和力高于阈值  $d_t$  的检测器的刺激水平。若刺激水平低于设定阈值  $I_1$ ，则从网络中删除该检测器及其与其他检测器之间的连接和对应权值。对网络中剩余检测器按刺激水平排序。

3) 选择网络中刺激水平大于设定阈值  $I_2$  的所有检测器，对其进行与它的刺激水平成反比的克隆变异。计算变异后的检测器与原检测器的亲和力，从变异后的检测器集合中选择与原检测器亲和力低于阈值  $d_d$  的检测器加入到免疫网络。

其中， $d_s$  为检测器与抗原之间的亲和力阈值，又称为检测器的自然死亡阈值，即若检测器与抗原之间的亲和力低于阈值  $d_s$ ，则该检测器被清除， $0 < d_s < 1$ ； $I_1, I_2$  为检测器受抗原的刺激水平阈值，且  $0 < I_1 < I_2 < 1$ ； $d_t, d_d$  为检测器之间的亲和力阈值，且  $0 < d_t < d_d < 1$ 。

具体算法描述如下：

#### 算法 2 基于协同进化的免疫网络动态平衡算法

```

Procedure D balance_ A lgorithm ()
Begin
Initial (); //设定初始参数;
Read ( $Ag^*$ ); //从抗原集合  $Ag$  中随机读取
一个子集  $Ag^*$  作为此次动态调整免疫网络的
训练集合
If (! Im m une _N etw ork ) //免疫网络未初
始化
Co-Evo_Im N et_ algorithm ( $Ab_{\{m\}}$ );
//调用免疫网络构建算法初始化免疫网络
For ( $Ab_{\{m\}}^i$   $Ab_{\{m\}}$ ) do
Begin
For ( $Ag_j^*$   $Ag^*$ ) do
/* 消除网络中自然死亡的检测器 */
Begin
If (A ffinity ( $Ab_{\{m\}}^i$ ,  $Ag_j^*$ ) <  $d_d$ )
Delete ( $Ab_{\{m\}}^i$ ,  $Ab_{\{m\}}^i$ );
//若亲和力高于阈值  $d_d$ ，则删除该
检测器
Else
Calculate ( $Ab_{\{m\}}^i$ ,  $Ab_{\{m\}}^j$ ,  $Ag^*$ );
//计算网络中所有检测器的刺激水平

```

```

Delete ( Ab{m}, Ab{m}i );
//消除网络中刺激水平较低的检测器
End;
For ( Ab{m}i, Ab{m} ) do
/*对刺激水平较高的检测器进行克隆变异*/
Begin
Mutation ( Ab{m}i, Ab{m}* );
Select ( Affinity ( Ab{m}i, Ab{m}j ) < dd );
//计算检测器之间的亲和力,选择与网络中的
原检测器亲和力小于阈值dd的检测器加入免疫网络
Update ( Ab{m} );
//更新免疫网络检测器关系矩阵
End;
End;

```

### 3.3.3 基于协同进化免疫网络的病毒检测算法

云计算平台中的服务器读取部署在其内部的免疫网络中的记忆检测器集合,计算待检测文件特征码与免疫网络中的记忆检测器之间的亲和力,若亲和力大于预先设定的阈值 $d$ ,则判断该样本文件为病毒,否则判断为正常文件。具体算法描述如下。

**算法3** 基于协同进化免疫网络的病毒检测算法

输入: 待检测文件特征码

输出: 检测结果, 1表示为已知病毒; 0表示正常文件。

```

Function co-evo_detect_algorithm (f)
Begin
Initial(); //设定初始参数
Read ( Ab{m} ); //读取网络中的记忆检测器集
Ab{m}
If ( Affinity ( f, Ab{m}i ) ≥ d ) //若 Ab{m}i 识别 f
Then Return 1; //判断为病毒
Else
Then Return 0; //判断为正常文件
End;

```

## 4 基于 MapReduce 的免疫网络构建算法实现

MapReduce 是云计算的关键技术,是一种简洁抽象的实现分布式计算任务的编程模型<sup>[8]</sup>。基于协同进化的协作免疫网络病毒检测算法中,构建免疫网络任务庞大,需要对大量数据进行计算处理。为

提高免疫网络的构建效率,采用 MapReduce 实现基于协同进化的免疫网络的构建,充分利用云计算平台下服务器对海量数据的分析处理能力,加快免疫网络的构建过程,从而提高云计算平台中对病毒的检测效率。

基于 MapReduce 的免疫网络构建算法的实现分为 Master、Map Worker、Collector、Reduce Worker 4 个步骤。首先,云计算平台下的服务器分别初始化网络中的所有检测器,由 Master 过程统计检测器的个数,并将网络中的初始检测器分配给  $M$  个 Map Worker,每个 Map Worker 分配相同的抗原集合。然后,每个服务器分别调用 Map() 函数,按照免疫网络检测器构建算法生成各自的记忆检测器集合;每个 Map() 函数运行一次会得到一个成熟的记忆检测器集合  $Ab_{\{m_i\}}$ 。各个 Map 并行计算  $M$  个任务数据后,会得到一组成熟的记忆检测器集合  $Ab_{\{m_1\}}, Ab_{\{m_2\}}, \dots, Ab_{\{m_M\}}$ ,由 Collector 过程收集这些记忆检测器集合。Reduce Worker 调用 Reduce() 函数将收集到的记忆检测器以亲和力为权值构建免疫网络,即计算 Reduce Worker 内记忆检测器的亲和力,根据亲和力值消除内部过于相似的检测器,并计算记忆检测器集合中的每个个体与测试集的适应度,选择适应度高的记忆抗体建立免疫网络。整个算法实现的核心为 Map 和 Reduce 函数,对 Map 和 Reduce 函数描述如下:

```

Map (Input detectors)
{
Read ( Ag ); //读取抗原集合
AbAg_affinity ( Ab, Ag );
//计算该 Map Worker 内检测器与抗原之间的亲和力
Select ( Ab, Ab{n} );
//选择该 Map Worker 内亲和力高的检测器
Process ( Ab{n}, Ab{m_i} );
//克隆变异 Ab{n} 中的检测器,进行网络抑制
}
Reduce ( m_id_ Result )
{
Ab_affinity ( Ab{m} );
//计算该 Reduce Worker 内记忆检测器的亲和力
Read ( T ); //读取测试集

```

```

Cal_fitness(Ab{m}, T);
//计算 Ab{m} 中个体元素的适应度
Select(fitness);
//选择 Reduce 过程中适应度高的检测器
汇总结果
}

```

### 5 仿真结果及其分析

本节对云计算平台中协同进化免疫网络中记忆检测器的检测率和利用 MapReduce 实现构建免疫网络的效率进行了仿真分析。

#### 5.1 记忆检测器的检测性能分析

仿真使用的抗原集合 Ag 是 100 个已知病毒的特征码，测试集 T 为 100 个正常系统文件与 100 个感染了实验中使用的病毒的样本文件，检测样本由通过网络收集到的 200 个代码的数据集及测试集 T 中的 200 个文件组成。其中，实验中所用到的特征码的二进制串均为 128bit，IBM 实验室证实 128bit (16byte) 长度的特征码已经足够，并且 128bit 特征码已经成为病毒检测工业的标准<sup>[9]</sup>；检测器的长度 L 也为 128bit。实验参数设置为：检测器自然死亡阈值  $d_s = 0.8$ ，检测器之间的抑制阈值  $d_d = 0.16$ ，检测器的检测半径  $d = 0.05$ 。

图 1 为其它条件相同的情况下，本文所提的协同进化免疫网络算法和 aiNet 免疫网络 2 种算法所生成的记忆检测器集对病毒的识别能力。从图中可以看出，随着记忆检测器集合的增长，基于协同进化免疫网络的记忆检测器集的识别能力增长更快。由于 2 种模型中使用的记忆检测器的数量相等，即 2 个模型在任意时刻对已知病毒的识别能力是一样，表明本算法生成的记忆检测器具有更强的识别未知病毒能力，即基于协同进化的免疫网络生成的记忆检测器集合具有更好的学习能力，每个周期的协同进化能够生成更有效的识别未知病毒的记忆检测器。

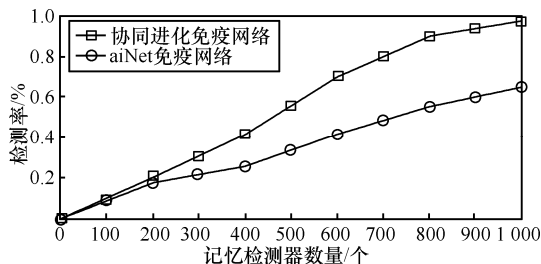


图 1 2 种免疫网络的检测率比较

#### 5.2 基于 MapReduce 的免疫网络构建效率分析

对基于 MapReduce 的免疫网络构建算法进行仿真分析，采用 Hadoop<sup>[10]</sup>作为 MapReduce 程序的分布式处理平台。实验环境为局域网内用 5 台装有 Linux 系统的电脑配置 Hadoop 分布式，每台 PC 机配置均是 CPU 为 Pentium 4 处理器，主频 1800MHz，内存 1GB，配置的操作系统为 Linux Ubuntu 9.04，Hadoop 版本为 0.19.1。实验采用美国哥伦比亚大学的数据测试集 (2D Synthetic Data)<sup>[11]</sup>。

图 2 为不同服务器数量下，生成相同数量的记忆检测器所需时间，图中显示了 3 种服务器部署情况下，每一种初始检测器集生成对应数量的记忆检测器所需的时间变化曲线。由图 2 可以看出，基于 MapReduce 的免疫网络构建算法具有更大的扩展空间。对于单机系统，随着初始检测器数量增大，运行时间近似呈线性增长，在多机情况下，生成相同数量的记忆检测器所需时间增长缓慢，随着机器增多，免疫网络的构建效率得到提升。实验结果表明，算法适用于云计算平台，并且随着云计算平台规模的增大，构建免疫网络的效率也将提高。

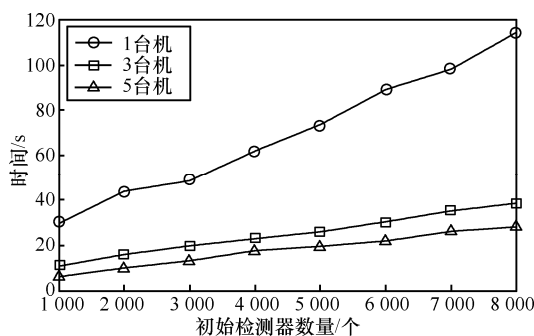


图 2 不同服务器数的处理时间比较

### 6 结束语

本文提出基于免疫网络理论的病毒检测算法，针对传统 aiNet 免疫网络模型免疫细胞之间缺乏相互协作的不足，引入协同进化思想提出了基于协同进化免疫网络的病毒检测算法，通过记忆检测器集与测试集之间相互协作，选择适应度高的记忆检测器个体加入免疫网络。通过免疫网络动态平衡算法中检测器与抗原之间的协同进化，使免疫网络中的检测器节点逐步进化生成最优检测器，从而提高整个网络中记忆检测器的检测效率。同时，给出了基于 MapReduce 的免疫网络构建算法的实现，利用

MapReduce 对大量数据集的并行处理能力, 加速免疫网络在云计算平台上的构建过程, 有效提高了病毒检测的效率。

### 参考文献:

- [1] HOFMANN P, WOODS D. Cloud computing: The limits of public clouds for business applications[J]. IEEE Internet Computing, 2010, 14(6): 90-93.
- [2] MUTTIK L, BARTON C. Cloud Security Technologies[R]. Information Security Technical Report. Elsevier Ltd, 2009: 1-6.
- [3] ZHENG X F, FANG Y H. An AIS-based cloud security model[A]. Proceeding of International Conference on Intelligent Control and Information Processing (IEEE 2010)[C]. Dalian, China, 2010: 13-15.
- [4] WANG X, HUANG T L, REN Z J. Research on the anti-virus system of military network based on cloud security[J]. Intelligent Computing and Integrated Systems (ICISS), 2010: 656-659.
- [5] KIM J, BENTLEY P J, ACKELIN U. Immune system approaches to intrusion detection — a review [J]. Natural Computing, 2007, 6(4): 413-466.
- [6] GONG B L, JUN Q H O, GIO R Q O S M. An artificial immune network approach to multi-sensor land use/land cover classification [J]. Remote Sensing of Environment, 2011, 2(15): 600-614.
- [7] CASTRO D, FEMANDO J. An evolutionary immune system network for data clustering[A]. Proceedings of the IEEE SBRN [C]. 2000. 84-89.
- [8] LIU Z Q, LI H Y, MAO G S. MapReduce-based Backpropagation Neural Network over large scale mobile data[A]. Proceedings of the 6th International Conference on Natural Computation [C]. ICNC 2010. 1726-1730.
- [9] HARMER P K, WILLIAMS P D, GUNSCH G H. An artificial immune system architecture for computer security applications[J].

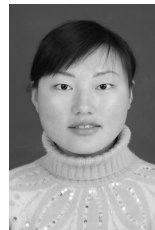
Special Issue on Artificial Immune Systems of the Journal IEEE Transactions on Evolutionary Computation, 2002: 6(3): 281-286.

- [10] KYRIACOS T, AKATERINI S, KONSTANTIOS C. Parallel collection of live data using Hadoop[A]. Proceedings of 14th Panhellenic Conference on Informatics [C]. PCI 2010: 66-71.
- [11] Columbia University. 2D synthetic data [EB/OL]. [http://www.zhouji.net/prof/2D Synthetic Data.zip](http://www.zhouji.net/prof/2D%20Synthetic%20Data.zip), 2009.

### 作者简介:



**程春玲** (1972-), 女, 陕西西安人, 南京邮电大学计算机学院副教授、硕士生导师, 主要研究方向为网络计算技术、信息安全技术、数据挖掘等。



**柴倩** (1986-), 女, 江苏徐州人, 南京邮电大学计算机学院硕士生, 主要研究方向为信息安全、计算机网络技术等。



**徐小龙** (1978-), 男, 江苏盐城人, 博士, 南京邮电大学计算机学院副教授、硕士生导师, 主要研究方向为新型网络计算技术、信息安全技术、智能 Agent 技术等。