doi:10.3969/j.issn.1000-436x.2013.09.020

基于粗糙集和人工免疫的集成入侵检测模型

张玲[1,2]，白中英[1]，罗守山[1,2]，谢康[2,3]，崔冠宁[1,2]，孙茂华[1,2]
(1. 北京邮电大学 信息安全中心，北京 100876；2. 云安全北京工程实验室，北京 100876；
3. 山东大学 信息科学与工程学院，山东 济南 250100)

摘 要：针对当前入侵检测存在的问题，通过引入粗糙集方法，综合误用检测和异常检测设计了一种基于粗糙集和人工免疫的集成入侵检测（RSAI-IID）模型，提出了一种在入侵检测中实现疫苗注入的方法。采用粗糙集方法获取疫苗，并保证了疫苗的优良性，优化检测性能；误用检测筛掉已知的入侵行为，提高检测的速度；异常检测针对未知攻击进行实时检测。最后在 KDD99 数据集上进行实验仿真，验证了模型的可行性和有效性。

关键词：粗糙集；人工免疫；误用检测；异常检测；RSAI-IID 模型
中图分类号：TP391.4 **文献标识码：**B **文章编号：**1000-436X(2013)09-0166-11

Integrated intrusion detection model based on rough set and artificial immune

ZHANG Ling[1,2], BAI Zhong-ying[1], LUO Shou-shan[1,2], XIE Kang[2,3], CUI Guan-ning[1,2], SUN Mao-hua[1,2]
(1. Information Security Center，Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Beijing Engineering Lab for Cloud Security, Beijing 100876, China;
3. College of Information Science and Engineering, Sha ng University, Ji'nan 250100, China)

Abstract: According to the problems of intrusion detection, an integrated intrusion detection model based on rough set and artificial immune (RSAI-IID) was proposed by using rough set and integrating misuse detection and anomaly detection. The rough set method was used to achieve the vaccine which was injected in the model, to get better vaccine, and to optimum the performances of detection; misuse detection was used to get off the known intrusions; anomaly detection was used to detect the novel intrusions. RSAI-IID model was validated on KDD 99 dataset. The experimental results show its feasibility and effectiveness.

Key words: rough set; artificial immune system; misuse detection; anomaly detection; integrated intrusion detection model based on rough set and artificial immune

1 引言

入侵检测是通过监控网络和系统的状态、行为以及使用情况来检测系统用户的越权使用以及系统外部的入侵者利用系统的安全缺陷对系统进行入侵的企图。在入侵检测中，检测率、虚警率、检测的速率是衡量入侵检测系统的重要指标。

根据检测的方法不同，入侵检测分为异常检测和误用检测。异常检测(anomaly detection）首先总结正常操作应该具有的特征，即对正常行为特征建立知识库，当用户与正常行为有重大偏离时，该用户行为被认定为入侵[1]。误用检测(misuse detection)：首先获取非正常操作的行为特征，建立初始特征库，当用户行为与库中的记录匹配时，系统认定该操作为入侵。异常检测和误用检测各自的优缺点对比如表 1 所示。

这 2 种检测技术集成的方案各有优缺点，将 2 种检测方式集成可以弥补检测中的缺陷，对已知和未知入侵行为检测[2]。为了进一步改善入侵检测的检测性能，如自适应性、检测率、虚警率以及检测

收稿日期：2013-04-20；修回日期：2013-08-02
基金项目：国家自然科学基金资助项目（61121061，61161140320）
Foundation Item: The National Natural Science Foundation of China (61121061, 61161140320)

速度，需要结合其他研究领域的知识进行研究。

表 1　异常检测和误用检测对比

类型	优点	缺点
异常检测	对未知攻击检测有效 对冒充合法用户的入侵检测率高	虚警率高 需要实时地建立和更新系统或用户的特征轮廓，计算量大
误用检测	技术比较成熟 对已知攻击检测率高，虚警率低 采用匹配模式，计算量小	不能检测未知入侵 漏警率比较高 特征库必须不断更新 对于系统内部攻击的越权行为，很难检测

在入侵检测中，很多学者提出了采用神经网络、模糊集理论、遗传算法、人工免疫原理和数据挖掘的方法对入侵检测进行研究。其中，人工免疫原理是从生物免疫系统演化而来的，具有分布性、自适应性的优点，已经被证明是用于入侵检测的一种有效技术方法。

生物免疫系统（BIS，biology immune system）是一个分布式、自组织和具有动态平衡能力的自适应复杂系统。1974 年，美国生物学家、医学家和免疫学家杰尼（Jerne N K）提出了免疫网络理论，并因此获得 1986 年的诺贝尔医学奖。MATZINGER 首先提出危险理论，他认为触发人体内产生免疫响应是由细胞非自然死亡时发出的危险信号引起的，不是非自体入侵导致的。树突状细胞(DC, dendritic cell)能够结合抗原引起的环境信号对抗原进行实时异常检测。之后受免疫系统的启示，许多学者在实际的工程应用中，开展了许多这方面的研究[3]。由此，人工免疫系统（AIS, artificial immune system）诞生了一个新的研究领域。表 2 列出了生物免疫系统、人工免疫系统的相似性分析。

表 2　免疫系统的类比分析

生物免疫系统(BIS)	人工免疫系统(AIS)
抗原	采集的在线数据
B 细胞、T 细胞	检测器
抗体对抗原的识别	抗体和抗原的绑定
记忆细胞	记忆细胞
协同刺激	人工确认信号
注射疫苗	更新特征库
抗原检测/免疫应答	抗原检测/应答

1) 免疫原理应用于入侵检测方面的研究现状。

人工免疫应用于入侵检测首先是由美国 University of New Mexico 的 FORREST 提出的，她发表的文章[4]为人们掀开了研究该领域理论的序幕，她将计算机系统保护问题与免疫系统学习区分自体一非自体相比较，提出了阴性选择算法，并陆续发表了多篇文章。1999 年，在其学生 HOMFEYR 协助及以前工作的基础上，提出了一个融合多种免疫系统性质的人工免疫系统(ARTIS, artificial immune system)模型。ARTIS 具有生物免疫系统的多样性、分布式计算、错误耐受、动态学习、适应性和自体检测等特征，是分布式自适应系统的一般框架，可以独立于任何特殊问题。为验证 ARTIS 的性能，2002 年，HOMFEYR 开发了网络轻量级入侵检测系统(LISYS，lightweight intrusion detection system)。LISYS 通过检测局域网(LAN)中 TCP 协议的同步(Syn)数据分组来实现对网络中异常的检测[5]。

文献[6]中将基于聚类的人工免疫应用于射频识别中，采用了免疫聚类算法 aiNet 进行聚类，对已知和未知的攻击进行识别。

文献[7]中提出了一个基于免疫原理的入侵检测模型，给出了自体、非自体、免疫细胞的定义，建立了由记忆细胞、成熟细胞、未成熟细胞集合构成的入侵检测模型。并对模型进行了仿真，对模型中的几个重要参数进行了分析。实验表明这种新型的入侵检测模型具有较好的自适应性。

文献[8]中受人工免疫系统危险学说的启发，基于人工智能的免疫系统代理 ABAIS 被用在入侵检测系统中。代理配合计算成熟环境抗原值(MCAV, mature context antigen value)，并且为了安全响应更新活跃门限值。树突状的细胞代理(DC agent)用来仿真内在免疫子系统和人工 T 细胞代理 (TC agent)来适应免疫子系统。

文献[9]中提出了一种集成树突状细胞算法和负选择算法的人工免疫系统，该方法具有进行实时入侵检测的优点。

文献[10]中受生物免疫响应中抗体浓度和入侵时网络流量模式相似性的启发，提出了一个新的入侵检测方法，在不影响检测率的情况下，降低了虚警率。

文献[11]中采用了动态克隆选择算法，提出了一种基于免疫移动代理的分布式入侵检测新方法，用来降低网络的负担、提高系统的实时性能。

基于人工免疫的入侵检测中，随机生成检测器

会导致一些问题：在系统达到稳定平衡之前，入侵检测系统检测率很低，此时，整个网络和主机系统遭到攻击的概率会增大。疫苗注入是解决这些问题的一种方法。而粗糙集是对数据库中的批量客观数据进行区分识别，从而更快速地获取知识规则。尤其是在缺乏先验知识时，以考察数据的分类能力为前提，对模糊或不确定的数据进行相应的分析和处理。为了获取有效的疫苗，粗糙集方法是一种有效的技术手段。

早在 1982 年，波兰华沙理工大学科学家 Pawlak Z 创先提出了粗糙集理论[12]。经过了多年的发展，粗糙集理论和其他学科相结合，如机器学习、模式识别、知识发现。粗糙集在数据挖掘方面主要体现在：使用不可分辨(等价)关系对数据进行聚类形成等价集合，对属性、对象进行约简计算，生成决策规则[13]。

在入侵检测中，采集来的日志数据量很大，并且特征数据中包含大量的冗余特征、不完备数据，势必加大检测的工作量，影响检测速度，从而最终导致异常行为不能得到及时的处理。粗糙集方法通过处理大数据量、处理不确定数据、消除冗余信息等步骤，约简训练数据，寻找最小属性集，得到有效的决策规则。正是鉴于粗糙集理论的这些优点，许多研究者将粗糙集理论应用于入侵检测中。

2) 粗糙集在入侵检测中的应用

文献[14]中提出了基于粗糙集和支持向量机的入侵检测分类方法，文中采用粗糙集方法（辨识矩阵）进行属性约简，采用支持向量机方法对数据进行分类。提出了启发式的属性约简算法，实验证明，该方法在不牺牲检测率的情况下，能提高检测的速度，减少数据存储的空间。

文献[15]中采用 RIPPER 规则建立真报警和误报警的分类器，开发出了一个降低误报警的原型系统 ALAC(adaptive learner for alert classification)，能够显著地降低误报警。

文献[16]中提出了一个基于粗糙集理论和支持模糊向量机的入侵检测模型。采用了粗糙集方法对知识属性进行约简，并过滤掉一些容易识别的日志数据；支持模糊向量机的方法对剩下的数据进行训练和分类。实验证明该方法能够提高检测的速度。

表 3 列出了相关文献对入侵检测研究方面所做的贡献。

表 3 入侵检测的相关研究

文献	贡献
文献[7~11]	使用人工免疫原理进行异常检测，能有效地对未知攻击进行检测，系统具有自适应能力
文献[14, 15]	将粗糙集算法用于异常检测中，可以有效地获取决策规则
文献[16]	将支持向量机和粗糙集方法进行结合研究，结合不同的机器学习方法

其中，文献[7~11]中存在的问题是在系统达到稳定之前需要浪费很长的时间进行试探性检测，收敛较慢。这些研究者将人工免疫应用于异常检测中，强调了对未知行为的检测，并没有考虑检测的速度问题。而入侵检测中，采集到的特征数据量很大，而绝大多数数据属于正常范畴，而未知行为（新的入侵行为）数量较少。因此需要对已知行为进行过滤，以提高检测速度。根据表 1 的分析可知，引入误用检测对已知行为进行过滤，能有效地减小异常检测的工作量。并且找到有效的疫苗能缩短异常检测的收敛时间速度。

文献[14~16]中提出的方法是基于传统的知识规则库进行检测，如果知识规则库中的攻击特征规则覆盖不全或者不能及时更新，势必出现漏检，并且这些方法缺乏自适应检测能力。因此，综合考虑异常检测对未知行为的检测能力以及误用检测对已知行为的检测能力，并且借鉴生物免疫学的原理，设计一个基于粗糙集和人工免疫的新的集成入侵检测模型对入侵检测的研究很有意义。

结合入侵检测的实际需求，本文对人工免疫模型进行了扩展和改进。借鉴粗糙集和人工免疫算法的机制，综合误用检测和异常检测 2 种模式，设计了基于粗糙集和人工免疫的集成入侵检测(RSAI-IID)模型。提出了基于粗糙集方法的疫苗注入解决方案。最后，在 KDD99 数据集上进行实验仿真。实验结果表明，RSAI-IID 模型能对入侵行为进行实时的检测；疫苗注入的方案能有效地减少检测器的长度，提高检测速度；误用检测和异常检测相结合的方法能有效地保证检测的稳定性，提高检测速度。

2 RSAI-IID 模型设计

RSAI-IID 模型是在参考通用入侵检测架构(CIDF，common intrusion detection frame)的基础上设计的。RSAI-IID 模型如图 1 所示，该模型包括 4

个模块：数据采集（抗原采集）、规则库（胸腺）、规则匹配（组织）和数据分析中心（淋巴结）。

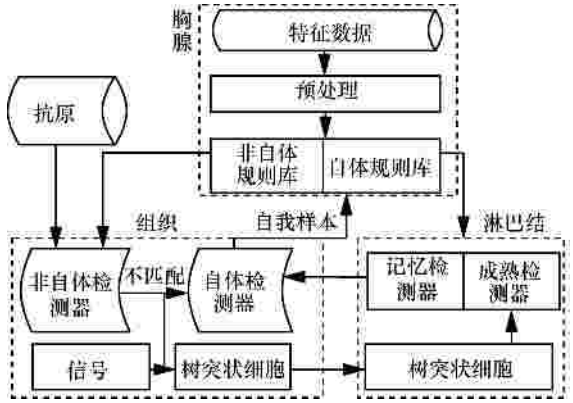

图 1　RSAI-IID 模型

在图 1 中，抗原模块负责采集主机和网络中的特征数据，并进行预处理，转化成表示抗原的二进制字符串，传给组织模块进行检测。

在胸腺模块中，生成有效的疫苗，采用粗糙集算法对批量的特征数据进行训练，形成自体规则和非自体规则，并将自体规则注入淋巴结模型中，形成成熟检测器，非自体规则注入非自体检测器中执行误用检测。

组织模块的功能是对抗原进行误用检测，如果与非自体检测器中的规则不匹配，该行为可能为正常行为或未知攻击行为，如果匹配，该行为判定为入侵行为，产生告警信号（以 E-mail 的方式发送危险信息）。通过误用检测筛除一些已知的攻击行为，未筛除的抗原传给自体检测器进行异常检测。同时该抗原的信号数据输入给树突状细胞，组织中的树突状细胞(DC, dendritic cell)分析获取每类抗原的异常指标，根据输出信号判断该树突状细胞的状态。如果协同刺激信号超过阈值，并且成熟信号值大于半成熟信号值，则树突状细胞由半成熟转为成熟，并将成熟的树突状细胞提呈到淋巴结中。

淋巴结模块实时地分析树突状细胞中抗原信号，动态地获取抗原的匹配阈值。另外一个重要的功能就是对成熟检测器中的检测器根据活跃状态生成记忆检测器，注入自体规则库中。RSAI-IID 模型的工作流程如图 2 所示。

RSAI-IID 模型的实现包括 5 个算法：RSAI-IIDA、NSA、RSA、DCA。对比图 1，RSAI-IIDA 是整个模型的实现算法；RSA 在胸腺中生成疫苗对非自体规则库和自体规则库进行疫苗注入；在组织和淋巴结中，采用 DCA 获得动态的异常检测阈值；组织中采用 NSA 实现对抗原的异常检测。

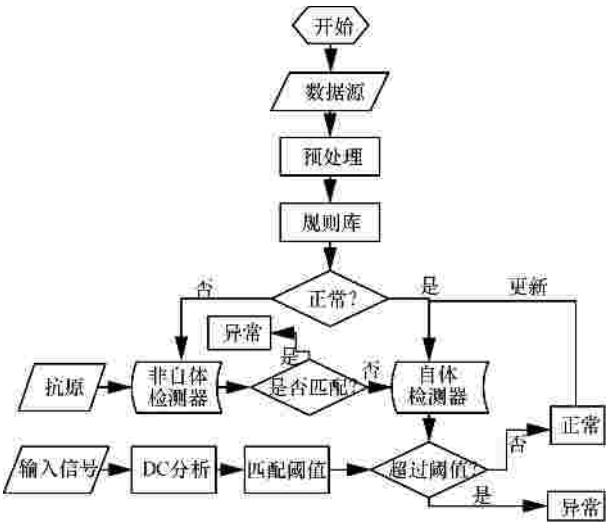

图 2　RSAI-IID 模型工作流程

3　模型实现

3.1　RSAI-IIDA

算法 1(RSAI-IIDA)

1) 输入：抗原流，经过预处理的信号流
2) 输出：检测到的异常抗原
3) RSA 生成规则库
4)规则库按照决策属性分成自体规则库和非自体规则库
5) while 输入数据 do
6) 抗原与非自体规则进行匹配//误用检测
7) if 不匹配 then
8) if 组织状态正常 then
9) 将抗原加入自体集合
10) else 将抗原加入非自体集合
11) 更新自体规则库和非自体规则库
12) end if
13) NSA 算法生成检测器
14) DCA 处理抗原和信号
15) 实时分析得到异常指标
16) 根据动态异常指标计算匹配阈值
17) 通过 NSA 执行异常检测
18) else 产生告警信号
19) end if
20) end while

RSAI-IIDA 描述了整个模型的工作过程。对抗

原进行误用检测和异常检测，动态地更新自体和非自体规则库。下面分别介绍 RSA I-IID A 中的 4 个算法 RSA、DCA、采用 NSA 生成自体检测器算法、NSA 检测算法。

3.2 RSA

借鉴文献[17]和文献[18]，定义抗体集合的信息决策表、等价关系、下近似、抗体属性依赖度和抗体属性重要度。

定义 1 五元组 $DT=<U,C\cup D,V,f>$ 是一个表示抗体集合的信息决策表，其中，

$U=\{x_1,x_2,\L,x_n\}$ 表示抗体对象的非空有限集合，即论域；

$C=\{a_1,a_2,\L,a_m\}$，C 表示抗体对象的条件属性，为非空有限集合；

$D=\{d\}$，D 表示抗体决策属性的非空有限集合，其中，$A=C\cup D;C\cap D=f$ ；

V 为抗体属性值的集合，V_a 是属性 $a\in C\cup D$ 的值域；

f 是 $U\times(C\cup D)\to V$ 的信息函数，即每个抗体对象的属性值。即 $\forall a\in C\cup D$，$x\in U$，有 $f(x,a)\in V$。

定义 2 其中的每一个抗体属性子集 $B\subset A$ 决定一个二元等价关系 $IND(B)$，用公式表示为

$$IND(B)=\{(x,y)\in U\times U\,|\,\forall b\in B,f(x,b)=f(y,b)\}$$

$IND(B)$ 将 U 划分为 k 个类 $X_1,X_2,\L,X_k$，代表不同的抗体类型，即

$$IND(B)=[X]_{IND(B)}=\{X_1,X_2,\L,X_k\} \tag{1}$$

定义 3 在抗体决策表 $DT=<U,C\cup D,V,f>$ 中，对每个子集 $X\subseteq U$，和不可区分关系 $\forall B\subseteq A$，集合 X 关于 B 的下近似定义为

$$B*(X)=\cup\{Y_i\,|\,Y_i\in U/IND(B)\wedge Y_i\in X\} \tag{2}$$

定义 4 在决策表 $DT=<U,C\cup D,V,f>$ 中，$A=C\cup D$，$\forall B\subseteq A$，$X\subseteq U$，用 $B*(X)$ 表示抗体集合 X 的下近似集合，决策属性 D 的 B 正域 $POS_B(D)$ 定义为

$$POS_B(D)=\bigcup_{X\in U/D}B*(X) \tag{3}$$

定义 5 抗体属性的依赖度定义为

$$r(C,D)=|POS(C,D)|/|U| \tag{4}$$

其中，$|POS(C,D)|$ 为正域 $POS(C,D)$ 元素的个数，$|U|$ 为整个抗体对象集合的个数。

定义 6 决策表中抗体属性的重要度：给定一个决策表 $DT=<U,C\cup D,V,f>$，$a\in C$，抗体属性 a 关于抗体决策 D 的重要度定义为

$$SGF(a,C,D)=r(C,D)-r((C-\{a\}),D) \tag{5}$$

RSA 是基于 pawlak 属性重要度的抗体决策表属性约简算法。介绍了粗糙集的一些基本知识，下面给出粗糙集算法的实现过程。

算法 2(RSA)

1) 输入：抗体形成的决策表 DT
2) 输出：自体规则库，非自体规则库
3) 由式(1)计算抗体条件属性 $X\{x_1,x_2,\L,x_n\}$ 的等价集
4) 计算抗体决策属性 D 的等价集
5) for 每一等价集 do
6) 由式(2)计算抗体决策属性的下近似集
7) 由式(3)计算 $POS(X,D)$
8) 由式(4)计算抗体属性依赖度 $r(X,D)$
9) end for
10) for 每个属性 x_i do//属性约简
11) 计算条件属性 $X-x_i$ 的等价集
12) 由式(2)计算抗体属性的各等价集的下近似集
13) 由式(3)计算 $POS(X-\{x_i\},D)$
14) 由式(4)计算 $r(X-\{x_i\},D)$
15) 由式(5)计算抗体属性 x_i 的重要度
16) if $SGF(X-\{x_i\},D)=POS(X,D)$
17) then exit
18) else if $SGF(X-\{x_i\},D)=0$
19) then 删除 x_i //该属性不重要
20) i++；
21) $POS(X,D)=POS(X-\{x_i\},D)$
22) $r(X,D)=r(X-\{x_i\},D)$
23) end else
24) end if
25) end for
26) 计算约简后的条件属性的等价集：E_1'，E_2'，$\L$，E_n'
27) 计算决策表属性 $D(d)$ 的等价集 Y_1'，Y_2'
28) while 抗体条件属性等价集 E_i' do//获取规则
29) if $E_i'\cap Y_1'=E_i'$ then
30) $Des(E_i')\to Des(Y_1')$
31) else $E_i'\cap Y_2'=E_i'$ then
32) $Des(E_i')\to Des(Y_2')$
33) end while
34) for x_i do

35) for x_j do//规则化简

36) if $Des(E_i') = Des(E_j')$ 且 $Des(Y_i') = Des(Y_j')$

37) delete $Des(E_j') \to Des(Y')$

38)　　end if

39) j++;

40)　　end for

41)　　i++;

42)　end for

43) 存储自体规则库

44) 存储非自体规则库

由 RSA 获取检测器的长度值，自体规则库中执行负选择算法获取成熟检测器，非自体规则执行误用检测。

3.3　NSA

NSA 包括 2 部分 异常检测和自体检测器生成。检测器生成如算法 3 所示，异常检测如算法 4 所示。3.2 节中采用 RSA 获取自体规则库，填充自体规则库，如果自体规则库中自体检测器数量没有达到容量阈值，则用 NSA 随机生成的候选检测器。

定义 7[19]　抗原与抗体的亲和度计算采用欧拉(euclidean)形态空间的欧拉距离计算方法，即

$$D = \sqrt{\sum_{i=1}^{L} (x_i - y_i)^2} \tag{6}$$

其中，x_i 为抗原的第 i 个特征位，y_i 为抗体的第 i 个特征位。

算法 3　NSA 检测器生成算法

1) 输入：自体规则集合，自体半径，检测器数量初始值 m，自体规则库容量 n，检测器长度；

2) 输出：检测器集合；

3) if $m < n$ then

4)　　随机生成 n- m 个候选检测器

5)　　for 每个自体样本 do

6)　　由式(6)计算候选检测器和自体样本的亲和度

7)　　if 候选检测器不在自体半径之内 then

8)　　将候选检测器加入自体规则库

9)　　m++

10)　　end if

11)　end for

12) end if

13) return 自体规则库

算法 4　负选择检测算法

1) 输入：误用检测输出的未知抗原，检测器集合

2) 输出：检测结果

3) while 输入数据 do

4)　　for 每个检测器 do

5)　　计算抗原与检测器（抗体）的亲和度

6)　　if 抗原在检测器的匹配阈值之内 then

7)　　抗原异常

8)　　else 抗原正常

9)　　end if

10)　end for

11) end while

3.4　DCA

DC 可以接收 4 类输入信号：病原体相关分子模式信号(PAMP，pathogen-associated molecular pattern)，代表出现异常行为；安全信号（safe signal），表示行为是正常模式，该信号增强，代表行为正常的可能性增强；危险信号（danger signal），表明可能存在异常行为，该信号增加，表示行为异常的可能性增强；炎症信号（inflammation signal），该信号用于放大其他信号。输入信号的预处理参考文献[9]的处理过程，做归一化处理。

DC 收集组织中的抗原，对 3 类信号（PAMP、安全信号、危险信号）进行计算得到 3 个输出信号：协同刺激信号(CSM)、半成熟信号（SEMI）和成熟信号（MAT）。由输入信号到输出信号的转换如式(7)所示[20]。公式推荐的权值参考表 4。

$$C_{[\mathrm{CSM,SEMI,MAT}]} = \frac{(W_{\mathrm{P}}C_{\mathrm{P}}) + (W_{\mathrm{S}}C_{\mathrm{S}}) + (W_{\mathrm{D}}C_{\mathrm{D}})}{\left|W_{\mathrm{P}}\right|\left|W_{\mathrm{S}}\right|\left|W_{\mathrm{D}}\right|} \cdot \frac{1+I}{2} \tag{7}$$

当 CSM 的累加值超过 DC 的迁移阈值时，DC 迁移到淋巴结，形成抗原提呈，系统记录 DC 所收集到的的抗原与 DC 的状态，并加入新的 DC。由式(7)计算每个抗原的 MCAV(mature context antigen value）值。对超过阈值的异常抗原提交响应中心进行处理。

定义 8　动态异常指标的计算公式如(8)所示。

$$C_a = \frac{m_a}{\sum_{i=1}^{A} A_i} \tag{8}$$

其中，a 是所有具有相同值的抗原集合，m_a 是抗原类型 a 被提呈为成熟抗原的总数。A_i 是抗原类型 i 被提呈的总数，A 是抗原总的类型数。

定义 9　抗原匹配阈值的定义如式(9)所示[9]。

$$Y_a = (L - r)\mathrm{e}^{-\partial(C_a - d)} \tag{9}$$

其中，L 为检测器长度，$?$ 为常数，d 是异常检测中的异常阈值，r 为自体半径，C_a 为抗原类型为 a 的动态异常指标。对于记忆检测器 $?$ 取更大的值。

算法 5 DCA

1) 输入：抗原流，经过预处理的信号流
2) 输出：抗原的异常指标
3) 初始化 M 个 DC 种群
4) while 输入数据 do
5) 更新组织中的抗原结构
6) 更新输入的 3 类信号值
7) for 每个树突状细胞 do
8) 获取并存储抗原
9) 获取并存储输入信号
10) 由式(7)计算 3 个输出信号（PAMP、危险信号和安全信号）
11) 随机产生 DC 的迁移阈值(一般在[100,500]之间产生)
12) if（DC_i 的输出信号 CSM 累加值≥DC_i 的迁移阈值） then
13) if（累计成熟信号≥累计半成熟信号）
14) then *context*=1//DC 为成熟状态
15) else
16) *context*=0//DC 为半成熟状态
17) end if
18) DC_i 迁移到淋巴结
19) i++
20) end for
21) end while
22) for DC_i do
23) 计算每种抗原类型的异常指标 A_i
24) end for
25) 由式(8)计算抗原类型及动态异常指标 C_a
26) Return 动态异常指标值

根据 DC 从未成熟转化为成熟状态，并迁移到淋巴结中，执行抗原提呈。

3.5 算法复杂度分析

针对以上算法，分析算法的时间复杂度和空间复杂度。通过算法的复杂度讨论算法的性能。假设 RSA 中决策表条件属性个数为 M，决策属性值个数为 2，训练样本数为 N_1，待检测的抗原总数量为 N，经过误用检测后的抗原数量为 N_2，自体检测器个数为 K，误用检测器个数为 K_1，检测器长度为 L，L_1 为输入抗原信号长度。

误用检测的时间复杂度为 $O(NLK_1)$，空间复杂度为 $O(LK_1)$。综合表 4，由于训练样本数 N_1 远远小于 N，RSAI-IIDA 的时间复杂度为 $\max(O(NLK_1), O(N_2(L_1N_{22}+LN_2K)))$。异常检测中的计算复杂度较高，即为 $O(N_2(L_1N_{22}+LN_2K))$，空间复杂度为 $O(MN_1K_1)$。IAIS 的时间复杂度为 $O(N(L_1N_2+LNK))$，空间复杂度为 $O(MN_1K_1L)$。RSAI-IID 与文献[9]中的 IAIS 相比较，时间复杂度降低，空间复杂度增加。在检测初始阶段，空间复杂度增加，为了提高检测速度，耗费部分空间的代价是值得的，在后续检测过程中，空间复杂度相当。

表 4 算法复杂度分析

算法名称	时间复杂度	空间复杂度
DCA	$O(35N_2^2)$	$O(500(L+1))$
NSA	$O(LN_2K)$	$O((L+1)K)$
RSA	$O(M(M+1)N_1)$	$O(MN_1K_1L)$
IAIS	$O(N(L_1N_2+LNK))$	$O(MN_1K_1L)$
RSAI-IIDA	$O(N_2(L_1N_{22}+LN_2K))$	$O(MN_1K_1)$

4 实验仿真

采用美国林肯实验室提供的 KDD99 数据集进行实验仿真，研究 RSAI-IID 模型的性能。RSAI-IIDA 用 MATLAB 实现，所有的实验在 Windows 7（Intel Pentium Dual CPU E2180，2 GB RAM）平台下运行。

4.1 测试数据

1998 年，麻省理工学院林肯实验室建立了一整套入侵检测的基准数据。1999 年，为 KDDM（knowledge discovery and data minning）竞赛所建立的数据样本就是有名的 KDD99 数据，包括 41 维向量特征。实验中采取数据集中的 kddcup.data_10_percent 作为数据源。根据文献[23]中对数据域的定义，对数据集进行预处理，得到抗原和信号。抽取约 10%的训练集记作 S 作为实验数据。其中将 S 分成两部分，20%的数据记作 S_1 用来训练，获取决策规则，80%的数据集记为 S_2 用来作为测试数据集。在数据集中加入时间戳，按照每秒采样数据。为了验证 RSAI-IID 模型对未知攻击的检测性能，将数据集中的 2 类攻击 xlock 和 xsnoop 的全部数据集作为测试数据集。

1) 抗原

将数据域转换成二进制字符串，用来表示抗原，抗原构造如表 5 所示。

表 5　抗原构造表

数据域	转换	位数
2	TCP、UDP 和 ICMP 分别为 01、11、11 表示	2
3	按首字母编号 1~66，转换成二进制	7
4	按首字母编号 1~11，转换成二进制	4
{7,12,14, 15,21,22}	编码不变，分别为 0 和 1	1
8	转化成二进制	2
9	转化成对应的二进制	2
11	共含 5 类，用 0~4 的二进制表示	3
17	转化成二进制	4
18	转化成二进制	2
19	转化成二进制	3
31	原始值乘以 100，再转化成二进制	7
其他	按低 00，中 01，高 10 和极高 11 分类	2

2) 输入信号

选择作为输入信号的数据域与文献[7]相同。10 个数据域分成 3 类。

PAMP：数据域 serror rate、srv serror rate、same srv rate、dst host same src port rate 和 dst host serror rate。

危险信号：数据域 count 和 srv count。

安全信号：数据域 logged in、srv diff host 和 dst host count。

设 x 为数据域的值，若 x 在$[m,n]$区间内表现为正常，这个域为 PAMP 或危险信号；如果表现为正常，则为正常信号。对这些数据处理方法参照式(10)采用归一化处理，归一化到[0,100]之中进行处理。

$$f(x)=\begin{cases}0, x\in[0,m)\\ 100\dfrac{x}{n-m}, x\in[m,n]\\ 100, x\in(n,+\infty)\end{cases} \tag{10}$$

其中，m 和 n 分别取该数据域类的最小值和最大值。

3) 实验参数设置

DCA 算法：树突状细胞数量设置为 15，迁移阈值为[100,500]之间产生的随机数，异常阈值 d 由后面的实验获取。

NSA 算法：常数 ? 的值，当为记忆检测器时为 1，当为普通检测器时为 0.5。检测器的长度 L 为训练数据集属性约简后的规则字符串的长度。式(7)的推荐权值如表 6 所示[20]。

表 6　推荐权值

W(权值)	协同刺激信号 (CSM)	半成熟信号 (SEMI)	成熟信号 (MAT)
PAMP(P)	2	0	2
安全信号(S)	1	0	1
危险信号(D)	2	3	-3

4.2　检测器长度

条件属性共 41 个，如果全部数据项用来作为检测器长度，将加大异常检测的工作量，导致检测速度缓慢。RSA 对 41 个特征属性进行属性重要度计算，获取约简属性集，获得检测器的长度。运行数据集 S_1，约简后获得的最简属性集合的数据域为 11 个，分别为：2、3、4、25、26、28、29、30、31、35、36。对照表 5，在后面的实验中检测器的长度值 L 设置为 30。

从表 7 可以看出，通过 RSA 约简后提取的规则数明显减少。将获取的规则分成自体规则和非自体规则，分别存储自体规则库和非自体规则库。按照规则重要度排序，选择 1 000 条自体规则注入自体规则库。820 条非自体规则全部注入误用规则库中。

表 7　RSA 约简前后的规则数对比

规则数	约简前	约简后
自体规则数	15 100	1 341
非自体规则数	62 600	820

4.3　自体半径

ROC（reciever operation characteristic）曲线来表示检测的虚警率和检测率。横坐标代表正常行为被误判为攻击的比率，即虚警率；纵坐标表示正确识别攻击的比率，即检测率。在实验中，使用 KDD-CPU99 数据中的 S_2 进行测试，每次测试重复运行 10 次，将运行结果取平均值，用 ROC 曲线表示。

自体半径 r 的数值决定了每个检测器的覆盖范围，当自体半径为 0 时，抗原与检测器完全匹配。当检测器与抗原之间的亲和度大于 $L-r$ 时，则认为检测器和抗原相匹配。为了研究自体半径 r 在不同的取值下对 Artificial Immune 性能的影响，在集合 S_2 中测试自体半径分别取 0、1、2、…、16 时，对应的检测率和虚警率。改变 r 时的 ROC 曲线如图 3 所示。

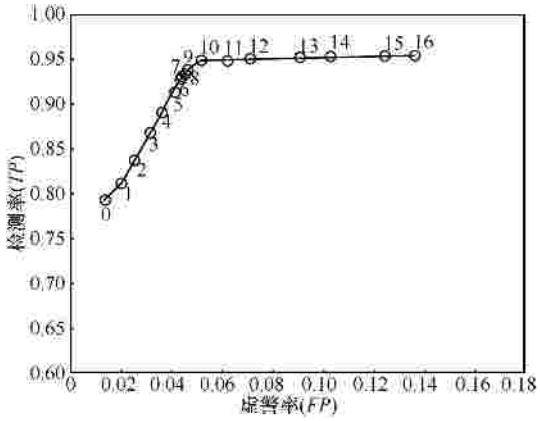

图 3 不同自体半径对应的 ROC 曲线

从图 3 可以看出，随着 r 值的不断增加，检测率不断地增加，虚警率也不断地变大。当 r 为 10 时，检测率趋于平稳，虚警率却不断变大。根据 ROC 曲线显示，越靠近左上角的取值，对应的检测率越高，虚警率越低。下面的实验中，r 值取 10，即自体半径值为 10。

由于 RSAI-IID 模型集成了误用和异常 2 种检测模式，抗原先采用误用检测过滤掉一些已知的攻击行为，一方面减少了异常检测的计算量，提高了异常检测的速度；另一方面保证了检测率始终不低于误用检测的检测率。从图 3 中可以看出，无论自体半径设置值为多少，检测率均高于 78%，检测率比较稳定。

4.4 异常阈值

由于异常检测是先建立正常的特征轮廓并以此作为比较的基准，这个基准即异常阈值，异常阈值 d 是用来判断抗原是否异常的关键，阈值选的过大，检测率会很低；阈值选的过小，虚警率会很高。在子集 S_2 上针对不同的异常阈值来计算检测率和虚警率。测试的阈值包括 0.1、0.2、…、1.0，每次实验运行 10 次，取均值和方差进行分析，实验的结果如图 4 所示。

从图 4 中可以看出，当异常阈值为 1.0 的时候，平均检测率为 0.698 4，虚警率均值为 0.023；当异常阈值为 0.1 时，平均检测率为 0.982 1，平均虚警率为 0.065。由于系统是误用检测和异常检测集成的，平均检测率均在 0.698 4 以上。从检测率和虚警率的方差数值分析，方差均低于 0.004，RSAI-IID 性能比较稳定。高阈值导致低的检测率和低的虚警率，为了平衡检测率和虚警率，需要取一个合适的异常阈值。从图 4 中可知，当阈值 d 为 0.4 时，检测率为 0.978 6，虚警率为 0.026 8。

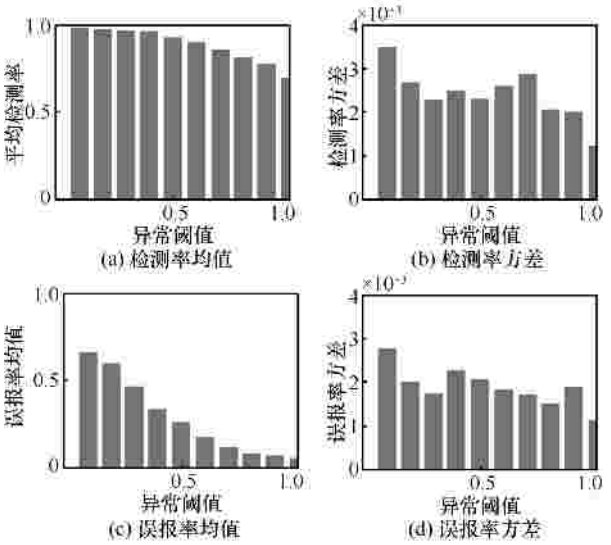

图 4 不同异常阈值对应的检测率和虚警率

4.5 性能比较

很多学者将其他的智能方法应用在入侵检测中，例如免疫原理、粗糙集、人工神经网络、遗传算法、模糊集、支持向量机等，下面将本文提出的 RSAI-IIDA 与其他方法的检测结果比较，包括与免疫算法和粗糙集算法进行横向对比以及与其他的机器学习算法进行纵向对比。实验中测试 RSAI-IIDA 模型的性能，并与其他的方法进行了对比。尽管实验设置各不相同，下面就检测率和虚警率进行对比，结果如表 8 所示。

将 RSAI-IIDA 与免疫算法进行比较。文献[6]中在 RFID 环境下进行异常检测，获得较高的检测率和低的虚警率；和其他的免疫算法进行对比，可见本文提出的 RSAI-IIDA 检测率明显增加；在文献[11]中提出的代理检测机制对 Dos 和 Probe 攻击检测比较有效；和经典算法 NSA 进行比较，检测率提高了 0.027 8，虚警率增加了约 0.016 8；和 DCA 比较，检测率提高 0.22 以上，虚警率增加了 0.026 8。通过与以上 2 种算法相比，算法的检测率提高，虚警率增加；和 IAIS 相比较，检测率提高和虚警率减少。

RSAI-IIDA 与其他的粗糙集算法对比，检测率增加，虚警率降低。文献[19]中，与 RSSVM 方法相比，检测率相当，虚警率降低；与文献[21]中的粗糙集与神经网络相结合的综合分类器相比，检测率提高；与文献[16]中的 RS-FSVM 方法相比，检测率提高，虚警率降低。

表 8　　算法性能对比

类别	方法	文献	检测率	虚警率
免疫原理	RFID	[6]	约 0.98	约 0.006
	克隆免疫	[7]	大于 0.95	约 0.14
	IAIS	[9]	0.969 1	0.032 1
	NIDAAC	[10]	0.956 2~0.960 6	0.019 5~0.040 4
	免疫代理	[11]	0.084~0.995	无
	NSA	[19]	约 0.95	约 0.01
	DCA	[21]	约 0.75	约 0
粗糙集	RSSVM	[19]	约 0.98	约 0.05
	综合分类算法	[21]	94.24	0.28
	RS-FSVM	[16]	0.90	14.24
其他算法	AdaBoost	[22]	0.900 4~0.908 8	0.065 5~0.089
	K-NN	[23]	0.910 0	0.080 0
	HMM	[24]	0.951 6（平均）	0.013 2（平均）
	PNrule	[25]	0.911 0	0.004 0
	FSA	[26]	0.987(误用)	0.042 8
			0.944(异常)	0.122
	RSAI-IID	本文	0.978 6	0.026 8

RSAI-IIDA 与其他机器学习算法进行纵向对比，本文提出的算法检测率较高。其中，FSA 算法对误用检测的检测率高，虚警率低，但是异常检测中检测率比较低，并且虚警率较高。HMM 在误用检测中检测率较高，虚警率也比较高；异常检测中检测率比 RSAI-IIDA 低，虚警率比 RSAI-IIDA 要高，并且 RSAI-IIDA 能对入侵行为进行自适应检测。

综合 4.3 节和 4.4 节的实验可以得出，RSAI-IIDA 的检测率始终高于 68%，检测相对稳定。由 3.5 节算法复杂度比较结果可知，RSAI-IIDA 时间复杂度减少，在检测之前，空间复杂度较高，执行检测时的空间复杂度相当。

4.6　模拟环境中的检测

为了验证 RSAI-IID 模型在新的网络环境下的检测性能。在借鉴麻省理工学院林肯实验室成功经验的基础上，搭建小型的实验平台。获取设计并实现了在新的软硬件环境下的入侵检测仿真实验。获取 120 条数据作为测试数据集 S_3。参数不变，同样每次实验运行 10 次，测试结果如表 9 所示。

针对 5 种攻击行为分别进行检测，从检测结果可以得出，RSAI-IIDA 对模拟环境下的检测率达到 0.958。

表 9　　检测明细表

类别	样本数	类型	明细	TP	平均 TP
正常	85	Normal	85	1.00	0.958
攻击数据	35	Probe	3	1.00	
		R2L	5	0.60	
		Vulnerability	13	0.923	
		Dos	6	0.677	
		U2R	8	1.00	

综上所述，RSAI-IID 模型是可行的，并且综合性能良好。RSAI-IID 模型集成了误用检测和异常检测 2 种检测模式，能够保证检测的稳定性；采用了粗糙集方法获取有效的疫苗，一方面保证了误用检测的有效性，另外一方面减少了异常检测的计算量；采用免疫原理方法保证了系统的自适应性，同时综合免疫原理和异常检测机制实现了对未知攻击行为的检测，并且在模拟环境中也得到了较高的检测率。

5　结束语

入侵检测系统普遍存在缺乏自适应能力、入侵检测速率低、高检测率和低虚警率之间平衡的问题。针对这些问题，本文在免疫入侵检测中引入了疫苗注入，综合误用检测和异常检测 2 种检测模式，设计了基于粗糙集和人工免疫的集成入侵检测模型。

由于 RSAI-IIDA 中参数比较多，对关键的参数：检测器长度、自体半径和异常阈值分别进行了仿真测试，通过对比分析确定参数值，通过实验获得检测率和虚警率。最后与其他方法分别进行了横向和纵向比较。实验证明，RSAI-IID 模型中，采用 RSA 获取疫苗的方法以避免纯随机方法的缺点，提高了检测速度，减少了收敛的时间；误用检测对已知攻击进行检测，过滤部分攻击行为，减少异常检测计算量，提高整体检测速度和稳定性；基于免疫算法的异常检测对未知攻击进行实时动态检测；并且对模拟环境中的数据集检测率也达到 95.8%。进一步的研究为，建立大型的模拟网络环境，获取全面数据分组进行分析，将提出的模型在实际网络环境中进行研究。

参考文献：

[1] ANDERSON J P. Computer Security Threat Monitoring and Surveillance[R]. Pennsylvania, 1980.

[2] 卿斯汉，蒋建春，马恒太. 入侵检测技术研究综述[J]. 通信学报，2004, 24(7):19-29.
QING S H, JIANG J C, MA H T. Research on intrusion detection techniques: a survey[J]. Journal on Communications,2004, 24(7):19-29.

[3] DENNING DOROTHY E. An intrusion deteetion model[J]. IEEE Transaction on Software Engineer on Software Engineering, 1987, 13 (2):222-232.

[4] FORREST S,PERELSON A, ALLEN L, *et al*. Self-nonself diserimination in a computer[A]. Proeeedings of the 1994 IEEE Symposium on Research in Security and Privacy[C]. Los Alamitos, 1994. 202-212.

[5] HOFMEYR S, FORREST S. Architecture for an artificial i mune system[J]. Evolutionary Computation, 2000, 8(4):443-473.

[6] YANG H,GUO J H, DENG FQ. Collaborative RFID intrusion detection with an artificial immune system[J]. Journal of Intelligent Information Systems, 2011,36(1):1-26.

[7] 梁可心,李涛,刘勇. 一种基于人工免疫理论的新型入侵检测模型[J]. 计算机工程与应用, 2005, 41(2):129-133.
LIANG K X,LI T,LIU Y. A new model of intrusion detecti based on artificial immune theory[J]. Computer Engineering and Applications, 2005, 41(2):129-133.

[8] OU C M. Host-based intrusion detection systems adapted from agent-based artificial immune systems[J]. Neuro Computing, 2011,88(1):1-9.

[9] 陈岳兵,冯超,张权.面向入侵检测的集成人工免疫系统[J]. 通信学报, 2012,33(2):125-131.
CHEN Y B,FENG C,ZHANG Q. Integrated artificial immune system for intrusion detection[J]. Journal on Communications, 2012,33(2): 125-131.

[10] ZENG J, LIU X J,LI T, *et al*. A novel intrusion detection approach learned from the change of antibody concentration in b logical immune response[J]. Springer Applied Intelligence, 2011, 35(1):41-62.

[11] LI Y Z, JING C W, XU J. A New Distributed Intrusion Detection Method Based on Immune Mobile Agent[R]. Berlin Springe , 2010. 233-243.

[12] PAWLAK Z. Rough sets[J]. International Journal of Comp and Information Science, 1982, 11(5):341-356.

[13] PAWLAK Z,GZYMALA BUSSE J,SLOWINSKI R. Rough sets[J]. Communications of the ACM, 1995, 38(11):88-95.

[14] GU C H, ZHANG X Q. A rough set and SVM based intrusion detection classifier[A]. 2009 the Second International Workshop Computer Science and Engineering[C]. Qingdao, China, 2009.155:106-110.

[15] 朱有产，熊伟，静永文. 基于 Rough Set 理论的综合分类器设计与实现[J]. 通信学报,2006, 24(11):63-67.
ZHU Y C,XIONG W,JING Y W. Design and realization of integrated classifier based on Rough Set[J]. Journal on Communications, 2006, 24(11):63-67.

[16] LI L, ZHAO K N. A new intrusion detection system based on rough set theory and fuzzy support vector machine[A]. IEEE I lligent Systems and Applications (ISA)[C]. Wuhan, China, 2011.1-5.

[17] 前进,苗夺谦,张泽华. 云计算下知识约简算法[J]. 计算机学报,2011, 34(12):2332-2343.
QIAN J, MIAO D Q, ZHANG Z H. Knowledge reduction algor thms in cloud computing[J]. Chinese Journal of Computers, 2011,34(12): 2332-2343.

[18] 苗夺谦,李道国.粗糙集理论、算法及应用[M]. 北京：清华大学出版社,2008.
MIAO D Q,LI D G. Rough Sets Theory Algorithms and Applications[M]. Beijing: Tsinghua University Press, 2008.

[19] GONZALEZ F A, DASGUPTA D. Anomaly detection using real-valued negative selection[J]. Genetic Programming and Evolvable Machine,2003, 4(4):383-403.

[20] GREENSMITH J, TWYCROSS J, AICKELIN U. Dendritic cells for anomaly detection[A]. IEEE Congress on Evolutionary Computation (CEC2006)[C]. Vancouver, Canada, 2006.664-671.

[21] GU F, GREENSMITH J, AICKELIN U. Further exploration of the dendritic cell algorithm[A]. International Conference n Artificial Immune System[C]. Phuket Thailand, 2008. 142-153.

[22] HU W M,HU W, MAYBANK S. Adaboost-based algorithm for network intrusion detection[A]. IEEE Trans Syst Man Cybern Part B-Cybern[C]. Beijing, China, 2008.577-583.

[23] KAYACIK H G, ZINCIR-HEYWOOD A N，HEYWOOD M I. Selecting features for intrusion detection: a feature relevance analysis on KDD 99 intrusion detection datasets[A]. The Third Annual Conference on Privacy, Security and Trust[C]. New Brunswick, Canada, 2006. 85-89.

[24] 邬书跃,田新广. 基于隐马尔可夫模型的用户行为异常检测新方法[J]. 通信学报, 2007, 28(4):38-43.
WU S Y, TIAN X G. Method for anomaly detection of user behaviors based on hidden Markov models[J]. Journal on Communications, 2007, 28(4):38-43.

[25] AGARWAL R, JOSHI M V. PNrule: a new framework for lear ing classifier models in data mining (a case-study in network intrusion detection)[A]. The First SIAM Conference on Data Mining[C]. Chicago, USA, 2001.1-17.

[26] SHINGO M, CHEN C,LU N N. Intrusion-detection model based on fuzzy class-association-rule mining using genetic programming network[J]. IEEE Transactions on Systems, Man, and Cybernetics,2011, 41(1):130-139.

作者简介：

张玲（1979-），女，湖北随州人，北京邮电大学博士生，主要研究方向为数据挖掘、云计算安全防护、进化算法与智能信息处理等。

白中英（1941-），男，甘肃永靖人，北京邮电大学教授、博士生导师，主要研究方向为网络安全、体系结构、人工智能等。

罗守山（1962-），男，安徽肥东人，北京邮电大学教授、博士生导师，主要研究方向为多方计算、密码学等。

谢康（1987-），女，山东菏泽人，山东大学博士生，主要研究方向为人工智能、网络安全。

崔冠宁（1990-），男，河北沧州人，北京邮电大学硕士生，主要研究方向为网络安全。

孙茂华（1986-），女，山东临沂人，北京邮电大学博士生，主要研究方向为多方计算。