群体智能算法及其在信息安全中的应用探索

杨义先, 李丽香, 彭海朋, 袁 静, 陈永刚, 张 浩

北京邮电大学信息安全中心 网络与交换技术国家重点实验室 北京 中国 100876

摘要 由于其在解决复杂问题尤其是 NP 难问题上的优势, 群体智能算法一经提出, 就备受关注。在动物行为的启发下, 目前已经设计出了包括蚁群、粒子群、蜂群、人工鱼群等一系列算法。同时, 这些算法也已被广泛运用到金融管理、交通运输、信息科学、航天工程、航海领域等各个工程领域。本文则将重点探索群智能算法在网络空间安全方面的潜在应用。首先简单回顾了几种典型的群体智能算法, 接着分析了它们在密码学、网络入侵检测等分支中的可能应用, 希望能够借助这些最优算法解决网络空间安全方面的一些基础问题, 特别是那些与复杂巨系统相关的问题。

关键词 群体智能; 蚁群优化; 粒子群优化; 网络入侵检测; 密码学
中图法分类号 TP309.2

Swarm Intelligence Algorithms and Study on its Application in Information Security

YANG Yixian, LI Lixiang, PENG Haipeng, YUAN Jing, CHEN Yonggang, ZHANG Hao

Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract Because of its advantages in solving complex problems, especially in the NP problem, the swarm intelligence algorithms has been put forward, and it is concerned widely. Inspired by animal behavior, lots of meta-heuristic algorithms has been designed include ant colony, particle swarm, bees swarm, artificial fish swarm and so on. At the same time, these algorithms have been widely used in financial management, transportation, information science, aerospace engineering, navigation field and other engineering fields. This paper will focus on the potential application of swarm intelligence algorithms in cyber space security. Firstly, several typical swarm intelligence algorithms are briefly reviewed. Then, their potential applications were analyzed in cryptography and network intrusion detection and other branches. Some basic problems of network space security can be solved by using the help of these algorithms, especially those related to complex systems.

Key words swarm intelligence; ant colony optimization; particle swarm optimization; network intrusion detection; cryptography

1 引言

教育部规划的“网络空间安全”一级学科的第一个研究方向就是: 网络空间安全基础理论。这里的“基础理论”是什么意思呢? 由于该规划中还有另一个研究方向是“现代密码学”, 因此, 所指的“基础理论”应该不仅仅是“密码理论”。那么, 到底是什么基础理论呢? 虽然此问题没有标准答案, 但是, 以下两点事实是铁定成立的: 1)网络空间绝对是一个复杂的巨系统; 2)整个网络中, 运行着海量的设备(此处, 将用户、黑客等人也看成是特殊的“设备”), 因此, 任何单台(套)设备相对于整个网络来说, 都可以看成是“大群体”中的一个单体。如果这个网络巨系统的协同性或稳定性出了问题, 那么, 肯定不安全; 如果这个网络巨系统失控了, 那么, 肯定也不安全, 等等。由于群体智能的方法和思路, 在研究巨系统的可控性、协同性、稳定性等方面扮演着十分重要的角色, 并且, 网络空间安全中的许多核心问题(比如, 搜索问题、内容发现问题、优化问题等)也是网络动力学中正在研究的问题。总之, 将“网络空间安全”与“网络动力学”这两个过去“井水不犯河水”的领域连接起来, 肯定是“网络空间安全基础理

通讯作者: 杨义先, 博士, 教授, Email: yxyang@bupt.edu.cn。本课题得到国家自然科学基金项目(下一代互联网安全与隐私关键技术的研究, No.61411146001))资助。收稿日期: 2015-11-23; 修改日期: 2015-12-07; 定稿日期: 2016-01-06

论”应该关注的课题。本文的目的就是想来牵这根“红线”，但愿在国内外同行们的共同努力下，“网络空间安全”与“网络动力学”这对有情人能够终成眷属，并生下诸如“安全控制论”等健康宝宝。由于假定本文读者以安全界学者为主，假定读者对安全的知识已经比较丰富，所以，下面重点介绍“网络动力学”的相关内容。

生物群体行为模式及最优化算法的研究，源于自然界中广泛存在的群体协同合作现象[1]。当从甲地迁徙到乙地时，大雁群会排成整齐的人字型队伍，并通过灵活调整队形，来自动躲避敌人或超越障碍；鹿群在逃避老虎追击时，并非作鸟兽散，而是形成某种合理的队形，即使某只鹿虽然看不到老虎，它仍然能根据附近鹿的奔跑形式，来决定自己的行为；蜜蜂在筑巢时，并无设计蓝图，也没有“工程师”监督指导，但最终筑成蜂巢的结构强度却是最优的；蚂蚁群能在巢和食物之间形成一条“高速公路”，当路上出现障碍时，它们会设法绕过，并很快找出最优路径；人脑的智能行为，也是由大量简单的神经元有机组织和协调而构成的群体行为。

无智能或低智能的个体，通过群体协同和自组织来完成个体难以完成的复杂任务。研究这种群体智能行为的理论，称为群体智能理论。群体智能算法的鲁棒性强，灵活性高，具有良好的环境适应性和天然的并行性，在非线性复杂问题中具有强大的搜索能力等。这些优点，不但具有重要的理论价值，而且为解决复杂网络问题提供了新方法和思路。

1987，Craig Reynolds 用计算机研究了鸟群的飞行规则，提出了人工鸟系统模型。随后国际上许多学者对群体智能理论进行了研究，设计了不少著名的群体智能优化算法，比如：蚁群优化算法[2,3]、粒子群优化算法[4]、菌群优化算法[5]等。现在这些算法已经被成功应用于旅行者商问题(TSP)、车间任务调度问题、资源受限的工程调度问题、多机器人系统的任务分配、目标聚类、通信网的路由选择、图着色和分割等最优化问题。由于群体智能算法在解决困难问题，尤其是 NP-C 问题上展现出来的优势，国内外学者已经开始考虑将群体智能运用到网络安全的多个方面，比如，构造极高时间复杂度的最优 S 盒[6]、生成具有高随机性的强不可预测性密钥[7]、减少公钥密码的时间复杂度[8]，入侵检测系统的高精度数据聚类分析[9]等。

下面介绍几个著名的群体智能算法，并探讨它们在网络空间安全中的潜在应用。

2 几类著名的群体智能算法

群体智能算法主要研究，个体如何通过与群内其它个体的连接、信息交流、沟通、组织和自组织，产生群体的智能优化行为。其特点有：1.鲁棒性：由于没有中心的控制与数据，群体智能优化系统更具有鲁棒性,它不会因某个或某几个单体的故障而影响整体求解；2.灵活性：由于群体可以更好地适应环境的变化,所以群体智能优化系统具有更强的灵活性;3.简单性：系统中个体的能力比较简单,这样每个个体的执行时间比较短，并且实现也比较简单;4.分布性：群体中，相互合作的个体是分布的，更能适应当前的网络环境下的工作状态;5.可扩充性：个体之间通过直接或间接通信进行合作，“因系统个体的增加，而引起的通信开销”的增加很小，这样的系统具有可扩充性。

2.1 粒子群算法

粒子群优化(PSO)算法，是一种基于种群的随机优化技术，由 Eberhart 和 Kennedy 于 1995 年提出。其思想来源于对鸟群捕食行为的研究。一群鸟在随机搜寻食物时，如果这个区域里只有一块食物，那么，找到食物的最简单有效的策略，就是搜寻目前距离食物最近的那只鸟的周围区域。

在粒子群算法中，每个粒子(鸟)都有自己当前的位置 x 和速度 v (决定飞行的方向和距离)，以及每个鸟自身找到的最佳位置 p_i 和种群的最佳位置 p_g。在每个时间步骤 t，每个粒子按如下公式更新速度和位置。

$$v_i(t+1)=\alpha v_i(t)+c_1r_1\left(p_i-x_i(t)\right)+c_2r_2\left(p_g-x_i(t)\right), \quad (1)$$

$$x_i(t+1)=x_i(t)+v_i(t+1) \quad (2)$$

其中 α 为惯性权重因子，c_1, c_2 为加速因子，r 为 0 到 1 之间的随机数。每个粒子的搜索示意图如图 1 所示。

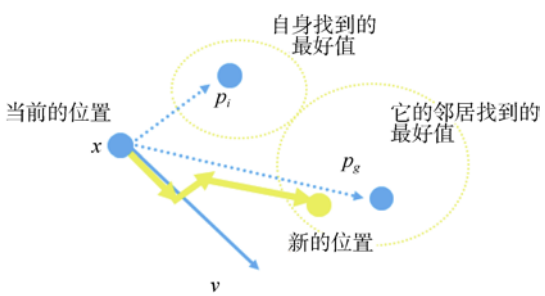

图 1 粒子群搜索示意图

粒子群优化算法的优势在于概念简单、收敛速度快、所需调整的参数少、可直接采用实数编码、

算法结构简单, 容易实现。因此, 粒子群优化算法一经提出便引起了信息和演化计算科学等领域学者们的广泛关注和重视, 并在短短的几年时间里出现大量的研究成果[10-18], 已被用于多种工程领域[19-29]。

但是粒子群算法容易出现陷入局部最优, 早熟收敛或停止现象。为了解决相关问题, 人们做了适当改进。如: 拉伸粒子群[30], 小生境粒子群[31,32], 协同粒子群[33,34]和混沌粒子群[35-37]等算法。

粒子群优化算法已经成了当前一个新的研究热点。例如: 中国科学院文献情报中心与汤森路共同发布的《2014 研究前沿》报告中指出, 在数学、计算机科学与工程领域, “基于粒子群算法的搜索优化”是 2014 年最年轻的热点前沿。在《2015 研究前沿》报告中, 又说: “粒子群优化与差分进化算法”和“忆阻器、忆阻电路及忆阻神经网络的相关研究”入选 2015 年热点前沿。

2.2 蚁群算法

生物学研究表明, 蚂蚁具有找到蚁穴与食物源之间最短路径的能力。这种能力是靠其在所经过的路上, 留下一种挥发性分泌物—信息素。蚂蚁寻找最短路径的原理如图 2 所示。1991 年意大利学者 Dorigo. M 等受蚁群觅食行为启发, 提出了基于概率理论的蚁群算法 (ACO 算法), 用以解决计算机算法学中经典的旅行商 TSP 问题。其数学模型如下所示。

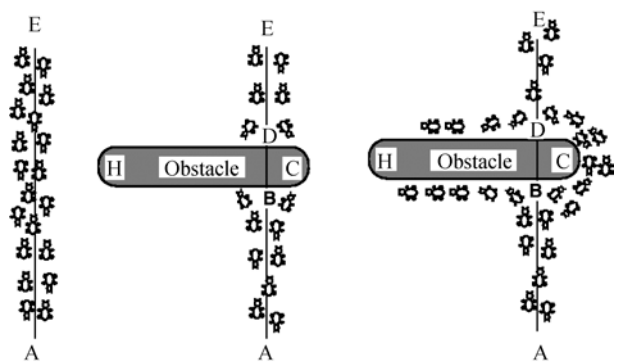

图 2 蚂蚁最短路径实验

$$\tau_{ij}(t+n)=\rho\times\tau_{ij}(t)+\Delta\tau_{ij}, \tag{3}$$

$$\Delta\tau_{ij}=\sum_{k=1}^{m}\Delta\tau_{ij}^{k}, \tag{4}$$

$$p_{ij}^{k}(t)=\begin{cases}\dfrac{(\tau_{ij}(t))^{\alpha}(\eta_{ij})^{\beta}}{\sum\limits_{k\in allowed_k}(\tau_{ik}(t))^{\alpha}(\eta_{ik})^{\beta}} & \\ \text{如果} j\in allowed_k & \\ 0 \qquad\qquad \text{其他} & \end{cases} \tag{5}$$

其中 $\tau_{ij}(t)$ 是时间 t 路径 (i,j) 上的信息素强度, $\rho(0\leqslant\rho\leqslant1)$ 是一个常数, 它表示信息素痕迹挥发后的剩余度, 即轨迹的持久性, $1-\rho$ 表示在时间 t 和时间 $t+n$ 内信息素的蒸发, $\Delta\tau_{ij}^{k}$ 表示蚂蚁 k 在时间间隔 $(t,t+n)$ 内在路径 (i,j) 上留下的单位长度的路径的信息素数量, $\eta_{ij}=\dfrac{1}{d_{ij}}$ 为路径 (i,j) 的能见度。α 和 β 是控制路径和能见度相对重要性的参数。$allowed_k=\{N-tabu_k\}$, 其中 $tabu_k(s)$ 是禁忌表中的第 s 个元素, 表示在现在的一次旅行中 k 个蚂蚁访问的第 s 个城市。

Dorigo 的蚁群算法可以简单表述为: 首先进行初始化, 即蚂蚁分别被放置在不同的城市, 每一条边都有一个初始的外激素强度值 $\tau_{ij}(0)$。每只蚂蚁的禁忌表的第一个元素设置为它的开始城市。然后, 每只蚂蚁从城市 i 移动到城市 j, 蚂蚁依据两城市之间的转移概率函数选择移动城市。在 n 次循环后, 所有蚂蚁都完成了一次周游, 禁忌表将被填满; 此时, 计算每只蚂蚁 k 旅行过的路径的总长度 L_k, τ_{ij} 依据方程(3)更新。同时, 保存蚂蚁找到的最短路径并清空所有禁忌表。这一过程重复直到周游计数器达到最大周游数 $NC_{\max}$ 或者所有蚂蚁都走同一路线。

蚁群优化算法提出了一种解决 TSP 的新思路, 至今, 它已被成功应用于解决许多组合优化问题, 比如, 解决数据挖掘[38,39]、图着色[40]、分配问题[41,42]、网络路由优化[43,44]、车辆路径问题[45,46]、车间作业调度[47,48]、系统参数辨识[49]等问题[50-53]。由于 Dorigo 在蚁群算法的出色研究, 2000 年 Nature 杂志特别邀请他撰写了一篇关于蚁群算法的进展报告[54]。

2.3 混沌蚁群算法(CAS)

Dorigo 基于蚁群的最短路径选择试验, 建立起了著名的蚁群优化模型 ACO。ACO 算法是基于概率搜索的算法; 但 Cole 等生物专家观测到单个蚂蚁的低维混沌行为以及整个种群的周期性动力学行为, 这些现象无法用基于概率理论的 Dorigo 的模型来解释。

从动力学的角度来说,单个蚂蚁的混沌行为和种群强大的自组织能力以及蚁群建立起的最短路径之间必然存在着某种内在的关系。那么, 单个蚂蚁的混沌行为与蚁群能找到最佳食物路径之间的内在关系是什么? 它们是如何组织和觅食的? 基于这些问题, 我们提出了蚁群新模型——混沌蚁群算法[55]。

在混沌蚁群模型中, 蚂蚁捕食过程是一个混沌搜索的过程, 如图 3 所示, 而最短食物路径的建立过

程则是由混沌搜索逐渐过渡到暂态混沌直到收敛到最短食物路径的过程。也就是说，蚂蚁处于一个在信息素和混沌共同作用下的自组织过程，一个类似于退火的过程，我们提出了“蚁群由混沌态经过混沌退火建立最优路径”的新观点，揭示了蚂蚁由混沌到周期行为的内在转变机制。在整个过程中蚂蚁通过不断地分泌信息素来传递最好路径信息，并通过信息素形成自组织。这个思想完全不同于 Marco Dorigo 的关于蚁群通过概率选择来建立最短路径的思想。

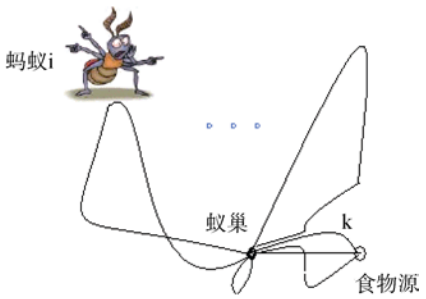

图 3　蚂蚁 i 的搜索过程

当第 i 个蚂蚁找到食物源后，这个蚂蚁爬回巢，此时蚂蚁在路径上留下信息素用来标记食物源和巢之间的关系。爬回巢后，这只蚂蚁会召集增援蚂蚁来进行增援，此时招来的蚂蚁在“食物源-巢-食物源”之间爬行的过程中留下信息素。信息素会在路径上形成一个以食物路径为中心的信息素路径场。由于信息素的挥发，使得信息素在最短路径上留下的信息素强度更大，而信息素强度对蚂蚁行为的影响更大，吸引越来越多的蚂蚁，形成了一个正反馈。在这个过程中，初始阶段对信息素场的强度较小，对蚂蚁的“混沌爬行”影响较小，蚂蚁具有更多的对路径的选择性，随着时间的推移和蚂蚁爬行次数的增多，信息素场的强度逐渐加强。短路径对蚂蚁的吸引逐渐变大，蚂蚁的混沌爬行行为逐渐消失，此时蚂蚁处于一个在信息素和混沌共同作用下的自组织过程，一个暂态混沌的过程，一个类似于混沌退火的过程，这个过程图 4-C 所示。然后蚂蚁经过进一步搜索，从而建立起最佳食物路径，如图 4-D 所示。

基于上述思想，建立了蚁群优化新模型:

$$y_i(t)=y_i(t-1)^{(1+r_i)},$$

$$z_{id}(t)=z_{id}(t-1)\exp\Big(\big(1-\exp(-ay_i(t))\big)\big(3-\psi_{id}z_{id}(t-1)\big)\Big)+\exp\big(-2ay_i(t)+b\big)\big(p_{id}(t-1)-z_{id}(t-1)\big), \tag{6}$$

其中，$Z_{id}(t)$ 表示第 i 个蚂蚁当前状态，$P_{id}(t)$ 表示第 i 个蚂蚁和邻居找到的最好位置，$y_i(t)$ 为组织变量，r_i 为组织因子控制组织的过程，a 和 b 为常数。

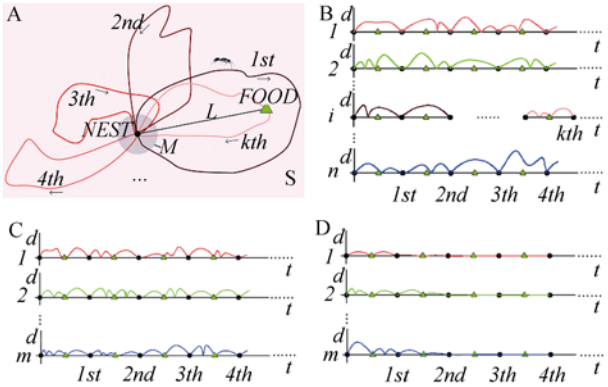

图 4　蚂蚁的混沌搜索

混沌蚁群优化算法开辟了一条利用蚂蚁的混沌动力学进行智能搜索的新途径，它在网络搜索、舆情发现与跟踪等方面都大有应用潜力。该算法及其改进算法[56-59]已被广泛应用于求解旅行商问题[60]、传感器网络任务分配[61]、web 数据分类[62]和聚类分析[63]、动力系统辨识[64-68]、电力系统机组调度[69]等十几个领域[70-71]。

我们在此方面的成果已经发表在美国科学院院刊(PNAS)上，并得到了包括美国《时代周刊》(Time)、《每日科学》(Science Daily 等 100 余家媒体和网站的长篇报道，也得到国内包括《科技日报》等 100 余家媒体的报道。

除了前面提到的几种算法以外，近年来群体智能算法发展迅速，目前已提出了一系列算法包括人工蜂群算法[72]，萤火虫算法[73]和布谷鸟搜索算法[74]等一系列的算法。

3　群体智能算法在密码学中的应用

在密码的设计与分析中,存在着许多复杂的搜索和优化问题。这些问题直接关系到密码的安全强度和应用的领域及范围。下面综述群体智能算法应用于分组密码中 S-box 的设计和优化、序列密码中密钥生成等的情况。

3.1　密钥生成

密钥是密码系统的最重要的参数，直接关系到整个密码系统的安全。因此设计出优秀的密钥一个重要课题。

1) 流密码密钥生成

流密码加密是安全通信的一个重要过程，它是将明文字符串和与密钥流序列作用加密，解密密钥流进行同步解密。1949 年，香农从理论上严格证明了：如果流密码密钥流序列是一个真正的随机序列，那么相应的流密码加密是绝对安全的[75]。但在实际

中，很难产生一个真正的随机序列，只能使用伪随机序列来代替真正的随机序列。因此序列密码的安全强度完全依赖于密钥流产生器所产生的密钥的不可预测性。影响不可预测性的因素很多，例如串分布、自相关值、周期和线性复杂度等，但是，它们都不是充分条件，而只是必要条件，因此高随机性序列的分析和产生问题并没有得到很好解决。

具有强随机性和不可预测性的密钥的分析和产生问题，可以归结为在密钥空间搜索最优序列的问题。群体智能在空间搜索方面展现了巨大的优越性，因此群体智能算法应该可用于构造流密码密钥生成器。2008 年，Sreelaja.N.K 等人将“人工蚁群优化算法”用于文本加密生成密钥[7]，通过二进制流明文中的字符分布来生成密钥，并通过一个互字符码表进行编码，从而提高了系统的安全性。Sreelaja.N.K 等人还将基于蚁群优化的密钥生成器运用到了二进制图像加密中[76]。2009 年，Sreelaja.N.K 基于同样的思想，将粒子群算法运用到了文本加密中[77]。2011 年 Ismail K. Ali 应用粒子群算法来搜索既满足非相关性，又满足高线性复杂性的适应函数，并通过仿真验证了其算法的有效性[78]

2) 分组密钥生成

群体智能在分组密码中也有应用。2013 年，Mishra 和 Bali 将遗传算法引入公钥密码学的密钥选择过程[79]，其中密钥可根据算法的适应度进行分类，并产生了随机且不重复的最终密钥，从而增强了密钥的强度和安全性。Jhajharia 等人用混合粒子群和遗传算法，设计了一个新的密钥生成算法[80]。2015 年，J.SaiGeetha 等人，基于人工蜂群设计了一个随机数生成器，能够快速的生成可行的随机数，并且提高了密钥强度和安全性[81]。

3.2 S-box 设计

S 盒是许多分组密码算法中的唯一非线性部件，因此,它的密码强度决定了整个分组密码算法的安全强度。S 盒本质上就是多输出布尔函数，构造具有某些特质的 S 盒，也是群体智能优化方法在密码学中最为成功的应用之一。

由于搜索拥有极高时间复杂度的最优 S 盒是一个 NP 问题，因此，可以考虑利用群智能算法来生成 S 盒。早在 1999 年, W.Millan 等人就利用遗传算法来设计了具有高非线性和低自相关性的 S 盒[82]。该方法通过调节遗传算法的参数，从已有的两个不相似的父 S 盒中产生出新的 S 盒。其结果显示遗传算法能比穷举搜索更快地搜索到性能优异的 S 盒。殷新春[83]等，于 2006 年使用快速收敛遗传算法对 S 盒进行优化。2008 年，黄银峰[84]等设计了一种利用免疫算法构造 S 盒的方法，该方法拥有很强的搜索较优值的能力。许向阳[85]，邹茜[86],尹向东[87]等，都各自提出了利用遗传禁忌算法的 S 盒优化方法。他们将 S 盒的雪崩准则和扩散特性等性能作为演化的目标，实验表明所构造的 S 盒不但是有效可行的，而且具有高非线性度和低差分均匀度，同时能有效地减少冗余计算量，加快收敛速度。2015 年，人工蜂群算法和粒子群算法，也有被运用到 S-box 的设计中[88-89]。

3.3 在密码学中的其他应用

群体智能算法也被用在各种密码算法中，以减少加密运算量。公钥密码的最大的缺点是运行速度慢，所以 Arindam Sarkar 等人利用粒子群算法来减少模幂乘法的次数，从而减少了加密时间，由此设计了一种更快的公钥密码[90]。在 Khan S 等人的文章中，蚁群算法被用于提高 DES 算法的运行效率[91]。

近几年，群体智能算法也被用于数字水印当中，如 2011 年 Yuh-Rau Wang[92]等提出了基于粒子群优化智能水印，其方法克服了数字水印在小波域上的不安全性、水印互相无法感知冲突和水印鲁棒性等多个问题。同年 Khaled Loukhaoukha[93]等，用多目标蚁群算法提升了小波水印的性能，在不丧失水印的透明性的情况下，保持了强鲁棒性。群体智能算法，还被用于设计端对端的安全密码分析[94,95]。显然群体智能算法和思想，已经开始向密码学的方方面面渗透。

4 群体智能算法在网络入侵检测中的应用

入侵检测系统应该具有很高的攻击检测率、很低的误报率、很少的资源占用，且需要足够的智能来识别出未知攻击。这些颇具挑战性的要求，为群体智能提供了发挥优势的潜能，因为，群体智能可基于一系列能力有限的简单个体，完成非常复杂的任务，并且，能够在巨变环境下正常运行。因此，群体智能算法运用于入侵检测系统具有天然的合理性，并且已经取得了成果，比如:

4.1 攻击源定位

Fenet 和 Hassas 利用蚁群优化算法的思想，提出了入侵定位的框架[96]。在该系统中，信息素服务器负责在网络遭到入侵时，向整个网络传播警告消息，这个消息被称作蚂蚁信息素。观察者负责监测每个主机的进程，以及网络连接情况。观察者是整个系统检测部分的核心部件。淋巴细胞，负责在网络间随机游走搜索信息素。如果信息素消息被发现，淋巴细胞

将收敛到危险主机，并采取相应的防护措施。在该系统中，类似于蚁群的部分，被用来迅速且有效地检测入侵，整个系统是一个分布式地检测和响应系统。如图 5 给出了攻击者被检测到的过程。Foukia 也采取了一种相似的机制，来识别和响应网络攻击[97]。Banerjee 于 2005 年提出了 IDEAS 系统，将 Foukia 的方法成功移植到了无线传感网络中[98]。Chang－Lung 等人描述了一种基于蜜罐和蚁群的入侵分析模型[99]。

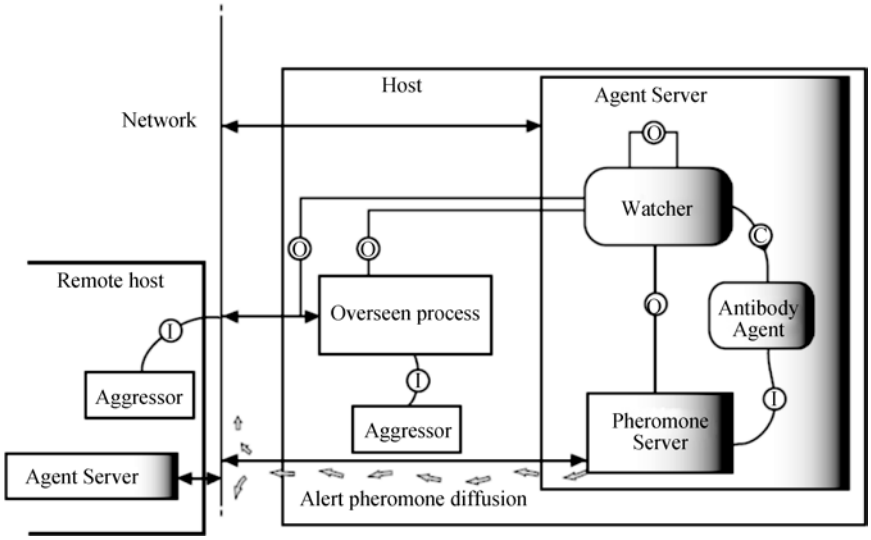

图 5　攻击者被检测到的过程[92]

2006 年, Abadi 和 Jalali 提出了[100]基于蚁群优化算法的入侵检测 AntNag 算法。该算法针对攻击者利用系统的多重漏洞进行攻击的模式，将多种攻击情形转化成一个有向的网络攻击图，从而入侵检测问题转化成了从该图中寻找最小子集以截断所有可能攻击的问题，一个 NP 难题[101-103]。

4.2　制定入侵分类规则

群体智能算法，还可为入侵检测系统制定分类规则。比如，可将正常的网络拥堵和攻击导致的网络拥堵区别开来。Soroush 等人[104]根据蚂蚁算法的“能将数据划分到某些既定类别”的思想，构建了候选规则，设计了 Ant-Miner 分类规则提取算法[105]，进而构造了相应的分类系统。何俊兵等人同样提出了基于 Ant-Miner 的多蚁群分类系统[106]。Fork 系统是基于群智能蚂蚁 Ant-Miner 算法的另一个入侵检测系统[107]。

M.S.Abadeh 等人将模糊系统和蚁群优化过程相结合，设计出了高质量的模糊分类规则。经过标准集测试，该系统可以达到 94.33%的准确率[108]。Y. Y. Chung 等人则提出了一种混合入侵检测系统，该系统利用基于模糊集的智能动态蚁群进行特征选取，同时利用简化的蚁群优化算法来进行入侵数据的分类；测试结果显示，该混合系统可以实现较高的分类准确率[109]。

由于移动自组织网拓扑结构的高变化性，传统的入侵检测思路常常不能很好用于移动自组织网中。F. Barani 等人将人工蜂群算法和负选择算法引入到移动自组织网，提出了一种动态的入侵检测系统。人工蜂群算法主要被运用在训练阶段，负选择算法用来产生一个父检测子集。实验结果发现，该算法与其他动态算法相比，可以更好地实现检测效率和误报率之间的平衡[110]。G. Indirani 等人设计了一种移动自组织网环境下的入侵检测系统，该系统运用蚁群优化来选取具有最高信任值的活跃节点。该活跃节点将检测邻节点的信任值，如果发现某信任值低于最低门限时，就判定这个邻居节点为恶意节点。仿真结果发现，该方案可以减少移动自组织网的通信负载[111]。P. Amudha 等人结合人工蜂算法和粒子群算法提出了一个用来预测网络入侵的混合算法。该混合算法可以用来选择代表网络流量模型的相关特征，实现了高达 99.5%的准确率[112]。Osama Alomari 等人，提出了一种新的 wrapper-based 特征选取方法，它采用蜂群算法为子集生成搜索策略，同时利用 SVM 作为分类器。结果显示，通过该方法产生的特征子集可以用来构造高质量的入侵检测系统[113]。

4.3　优化分类器参数

入侵检测系统中的核心部件是分类器，而分类器的性能很大程度上取决于参数的选取。将群体智能算法运用到分类器的参数优化中，可以大大提高入侵检测系统的性能。

Michailidis 等人将粒子群算法和神经网络相结合，运用到入侵检测系统中[114]。在该系统中，用粒子

群算法训练神经网络的参数，提高了系统的效率。刘华平等人将粗糙集理论和改进的二进制粒子群优化算法用于优化 SVM 模型的参数，提高了分类准确率的同时也减少了训练时间[115]。2014 年，A.C. Enache 等人将粒子群算法和人工蜂算法用于 SVM 参数的选取，实现了性能更好的 SVM 分类器[116]。匡芳君等人利用混沌粒子群算法提出了新的 SVM 模型用来处理入侵检测问题。该模型中，多层 SVM 分类器用来评估一个动作是否是攻击。在这里，改进的混沌粒子群算法被用来优化核心参数。实验结果显示该改进的 SVM 模型速度更快、预测精度更高[117]。Feng 采用多重标准线性规划分类方法，利用粒子群算法调节分类器的参数，使得分类器的正确率得到了提高[118]。

M. S.MAHMOD 等人，采用多层感知机和人工蜂算法，建立了有效的入侵检测系统。在这里，多层感知机作为分类器，被用来区分网络中的正常和异常的分组包；而人工蜂算法通过优化连接权值来训练感知机参数[119]。A．A．Aburomman 等人提出了一种新的集合构建方法，通过粒子群优化算法调节分类集的权值，提高了入侵检测准确率。Wang 等，采用混合 BP 神经网络和人工鱼优化算法，来设计入侵检测方案，它将人工鱼优化算法引入到了 BP 神经网络的训练中，缩短了采样训练时间，也提高了 BP 神经网络的分类准确率[120]。还有很多其他文献，将粒子群算法运用到分类器参数优化中[121-124]。

4.4 聚类分析

除了分类，入侵检测系统的另一个重要方面是数据聚类。入侵检测系统的数据量往往很大，为了克服数据量增大的问题，Ibrahim Aljarah 等人提出了一个基于 MapReduce 方法的并行粒子群优化的聚类算法[125]。通常带有权值的聚类方法被考虑为多目标函数，N.Cleetus 将粒子群优化算法引入到了多目标函数的优化中，提出了一种基于粒子群优化的的入侵检测机制，该机制具有较强的全局搜索能力。“随机森林”被用作模拟攻击和合法数据集的分类器，实现了较高的检测精度[126]。N.K. Sreelaja 等人运用蚁群优化来识别 nodeids 的隧道攻击，并对识别出的隧道攻击进行警报，还将恶意节点聚集在一起[127]。

对于零日攻击(zero-day attacks)，目前群体智能也有一些相关研究，如: Aman Jantan 等将蜂群算法应用于零日攻击分析[128]。而对于高级持续性威胁攻击 APT (Advanced Persistent Threat)，目前我们还没见到相关成果，希望相关学者尝试用一下群体智能进行相关研究，希望本文起到抛砖引玉的作用。

5 总结与展望

群体智能算法具有高灵活性，天然的分布式特性以及强鲁棒性等优点，它们必然可以在网络安全、复杂网络、大数据、云计算等系统中获得广泛应用。但是，过去国内外网络安全界，在这方面考虑不多，重视不够。

如何构建可控、可管的安全互联网？如何精准分析诸如黑客攻击、主页篡改、隐私发现、大数据挖掘、病毒传播等行为? 如何对海量信息进行更高效率的存储、备份与管理? 这些都是网络安全的关键技术问题，但是，过去人们对这些问题，一直都是进行独立研究，主要依靠若干巧妙的技术手段来寻找最佳解决方案，从未认真考虑过“是否存在统一的网络空间安全基础理论”。通过研究群体智能，我们发现，其实上述许多问题的核心，都可以归纳为非线性优化问题，更直观地说，可以归纳为极低智商的“蚂蚁”在现实世界中“求生存”的最优解问题。

参考文献

[1] J.Kennedy, J.F.Kennedy and R. C.Eberhart ,“Swarm intelligence”, *Morgan Kaufmann press*, 2001.

[2] G.Di Caro, and M. Dorigo. "Ant colony optimization: a new meta-heuristic."*Proceedings of the 1999 Congress on Evolutionary Computation*, 1999.

[3] M. Dorigo and L. M. Gambardella , “Ant colony system: a cooperative learning approach to the traveling salesman problem.”*IEEE Trans.Evolutionary Computation*, vol. 1, no. 1, pp. 53-66, Apr. 1997.

[4] J. Kennedy and R. Eberhart,“Particle Swarm Optimization.”in *Proc. IEEE Int.Conf. Neural Networks(NN 1995)*, pp. 33-57, 1995.

[5] K.M.Passino, “Biomimicry of bacterial foraging for distributed optimization and control.” in *Proc. IEEEControl Systems,vol. 22, no.* 3, pp. 52-67, Jun. 2002.

[6] G.Qin, X.Cheng and J. Ma. “Multiobjective Artificial Bee Colony Algorithm for S-box Optimization.”*International Conference on Automation Mechanical Control and Computational Engineering (AMCCE 2015)*, pp. 1738-1743, 2015.

[7] N. K.Sreelaja and G.Pai,. “Swarm intelligence based key generation for text encryption in cellular networks.” in *Proc. IEEE Int. Conf. In Communication Systems Software and Middleware and Workshops (CSSMW 2008)*, pp. 622-629, 2008.

[8] A. Dadhich, A. Gupta and S.Yadav, “Swarm Intelligence based linear cryptanalysis of four-round Data Encryption Standard algorithm.” in *Proc. Int’l Conf.Issues and Challenges in Intelligent Computing Techniques (ICICT 2014)*, pp. 378-383, 2014.

[9] Y. Feng, Z. F. Wu, K. G.Wu, Z. Y.Xiong and Y.Zhou,“An unsupervised anomaly intrusion detection algorithm based on swarm intelligence.” in *Proc. Int’l Conf.Machine Learning and Cybernetics (MLC 2005)*, pp. 3965-3969, 2005.

[10] W. N. Chen, J. Zhang, Y. Lin, N.Chen, Z. H. Zhan, H. S. H. Chung and Y. H.Shi, "Particle swarm optimization with an aging leader and challengers." *IEEE Trans. Evolutionary Computation*, vol. 17, no. 2, pp. 241-258, Apr. 2013.

[11] M. Hu, T. F.Wu and J. D.Weir, "An adaptive particle swarm optimization with multiple adaptive methods." *IEEE Trans. Evolutionary Computation*, vol. 17, no. 5, pp. 705-720, Oct. 2013.

[12] Z. Ren, A.Zhang, C.Wen and Z. Feng "A scatter learning particle swarm optimization algorithm for multimodal problems." *IEEE Trans. Cybernetics*, vol. 44, no. 7, pp. 1127-1140, Jul. 2014.

[13] S.Helwig, J.Branke and S.Mostaghim,"Experimental analysis of bound handling techniques in particle swarm optimization." *IEEE Trans. Evolutionary Computation*, vol. 17, no. 2, pp. 259-271, Apr. 2013.

[14] W. H.Lim and N. A. M.Isa"Particle swarm optimization with adaptive time-varying topology connectivity." *Applied Soft Computing*, vol. 24, pp. 623-642, Nov. 2014.

[15] Z. H.Zhan, J.Zhang, Y.Li and Y. H.Shi,"Orthogonal learning particle swarm optimization." *IEEE Trans.Evolutionary Computation*, vol. 15, no. 6, pp. 832-847, Dec. 2011.

[16] H.Haklıüseyin and H.Uğuz, "A novel particle swarm optimization algorithm with Levy flight." *Applied Soft Computing*, vol. 23, pp. 333-345, Oct. 2014.

[17] Y.Li, Z. H.Zhan, S.Lin, J.Zhang and X.Luo,"Competitive and cooperative particle swarm optimization with information sharing mechanism for global optimization problems." *Information Sciences*, vol. 293,no. 1, pp. 370-382, Feb. 2015.

[18] W.Zhang, D.Ma, J. J.Wei and H. F.Liang"A parameter selection strategy for particle swarm optimization based on particle positions." *Expert Systems with Applications*, vol. 41, no. 7,pp. 3576-3584, Oct. 2014.

[19] Z. L. Gaing, "A particle swarm optimization approach for optimum design of PID controller in AVR system." *IEEE Trans. Energy Conversion*, vol. 19, no. 2, pp. 384-391, Jun.2004.

[20] B.Liu, L.Wang and Y. H.Jin, "An effective hybrid PSO-based algorithm for flow shop scheduling with limited buffers." *Computers and Operations Research*, vol. 35, no. 9, pp. 2791-2806, Sept. 2008.

[21] J.Cai, X.Ma, Q.Li, L.Li and H.Peng,"A multi-objective chaotic particle swarm optimization for environmental/economic dispatch." *Energy Conversion and Management*, vol.50, no. 5,pp. 1318-1325, May. 2009.

[22] J.Cai, Q.Li, L.Li, H.Peng and Y.Yang"A hybrid CPSO–SQP method for economic dispatch considering the valve-point effects." Energy Conversion and Management, vol.53, no. 1, pp. 175-181, Jan. 2012.

[23] [23]K.Ishaque and Z.Salam"A deterministic particle swarm optimization maximum power point tracker for photovoltaic system under partial shading condition." *IEEE Trans. Industrial Electronics*, vol.60, no. 8,pp. 3195-3206, Aug. 2013.

[24] L.Cagnina, M.Errecalde, D.Ingaramo and P.Rosso, "An efficient particle swarm optimization approach to cluster short texts." *Information Sciences*, vol. 265, no. 1, pp. 36-49, May. 2014.

[25] M.Gong, Q.Cai, X.Chen and L.Ma, "Complex network clustering by multiobjective discrete particle swarm optimization based on decomposition." IEEE Trans. Evolutionary Computation, vol. 18, no. 1, pp. 82-97, Feb. 2014.

[26] M.Shen, Z. H.Zhan, W. N.Chen, Y. J.Gong, J.Zhang and Y.Li, "Bi-velocity discrete particle swarm optimization and its application to multicast routing problem in communication networks." *IEEE Trans. Industrial Electronics*, vol. 61, no. 12, pp. 7141-7151, Dec. 2014.

[27] Y.Zhou, G.Zeng and F.Yu,"Particle swarm optimization-based approach for optical finite impulse response filter design." *Applied optics*, vol. 42, no.8, pp. 1503-1507, 2003.

[28] X.Zhang, L.Yu, Y.Zheng, Y.Shen, G.Zhou, L.Chen and B. Yang,"Two-stage adaptive PMD compensation in a 10 Gbit/s optical communication system using particle swarm optimization algorithm." *Optics Communications*, vol.231, no.1, pp. 233-242, 2004.

[29] P. Y.Yin,"A discrete particle swarm algorithm for optimal polygonal approximation of digital curves." *Journal of visual communication and image representation*, vol. 15, no.2, pp. 241-260, Jun. 2004.

[30] K. E.Parsopoulos and M. N.Vrahatis,"On the computation of all global minimizers through particle swarm optimization." IEEE Trans. Evolutionary Computation, vol. 8, no.3,pp. 211-224, Jun. 2004.

[31] R.Brits, A. P.Engelbrecht and F.Bergh, "A niching particle swarm optimizer." *Proceedings of the 4th Asia-Pacific conference on simulated evolution and learning(SEL 2002)*, pp. 692-696, 2002.

[32] R.Brits, A. P.Engelbrecht and F.Bergh,"Locating multiple optima using particle swarm optimization." *Applied Mathematics and Computation*, vol. 189, no.2,pp. 1859-1883, Jun. 2007.

[33] F.Bergh and A. P.Engelbrecht,"A cooperative approach to particle swarm optimization." *IEEE Trans. Evolutionary Computation*,vol. 8, no.3,pp. 225-239, Jun. 2004.

[34] S.Baskar and P. N.Suganthan, "A novel concurrent particle swarm optimization." *IEEE Congress. Evolutionary Computation (CEC 2004)*, Vol. 1, pp. 792-796, 2004.

[35] J.Chuanwen and E.Bompard,"A hybrid method of chaotic particle swarm optimization and linear interior for reactive power optimisation." *Mathematics and Computers in Simulation*, vol. 68, no.1, pp. 57-65, Feb. 2005.

[36] J. Cai, Q.Li, L.Li, H.Peng and Y.Yang, "A hybrid CPSO–SQP method for economic dispatch considering the valve-point effects." *Energy Conversion and Management*, vol. 53, no. 1, pp. 175-181, Jan. 2012.

[37] L. D. S.Coelho and B. M.Herrera, "Fuzzy identification based on a chaotic particle swarm optimization approach applied to a nonlinear yo-yo motion system." *IEEE Trans. Industrial Electronics*, vol. 54, no.6,pp. 3234-3245, Dec. 2007.

[38] R. S.Parpinelli, H. S.Lopes and A. A.Freitas, "An ant colony algorithm for classification rule discovery." *Data mining: A heuristic approach*, pp. 191-208, 2002.

[39] R. S.Parpinelli, H. S.Lopes and A.Freitas, "Data mining with an ant colony optimization algorithm." IEEE Trans. Evolutionary Computation, vol. 6, no.4, pp. 321-332, Aug. 2002.

[40] D.Costa and A.Hertz, "Ants can colour graphs." *Journal of the operational research society*, vol. 48, no.3, pp. 295-305, Mar. 1997.

[41] H. R.Lourenço and D.Serra,“Adaptive search heuristics for the generalized assignment problem.” *Mathware and soft computing*, vol. 9, no.3, pp. 209-234, 2002.

[42] Y. C.Liang and A. E.Smith,“An ant colony optimization algorithm for the redundancy allocation problem (RAP).”*IEEE Trans. Reliability*, vol. 53, no.3, pp. 417-423, Sept. 2004.

[43] G.Di Caro and M.Dorigo,“AntNet: Distributed stigmergetic control for communications networks.” *Journal of Artificial Intelligence Research*, vol. 9, pp. 317-365, 1998.

[44] G. N.Varela and M. C.Sinclair, “Ant colony optimisation for virtual-wavelength-path routing and wavelength allocation.” *IEEECongress. Evolutionary Computation (CEC 1999)*, 1999.

[45] S.Salhi and M.Sari,“A multi-level composite heuristic for the multi-depot vehicle fleet mix problem.” *European Journal of Operational Research*, vol. 103, no.1, pp. 95-112, Nov. 1997.

[46] R.Bent and P.Van Hentenryck, “A two-stage hybrid algorithm for pickup and delivery vehicle routing problems with time windows.” *Computers and Operations Research*, vol. 33, no.4, pp. 875-893, Apr. 2006.

[47] A.Colorni, M.Dorigo, V.Maniezzo and M.Trubian,“Ant system for job-shop scheduling.” *Belgian Journal of Operations Research, Statistics and Computer Science*, vol.34, no. 1, pp. 39-53, Jan. 1994.

[48] D.Merkle and M.Middendorf,“An ant algorithm with a new pheromone evaluation rule for total tardiness problems.” *Real-World Applications of Evolutionary Computing. Springer Berlin Heidelberg*, pp. 290-299, 2000.

[49] W.Lei and W.Qidi,“Linear system parameters identification based on Ant system algorithm.” in *Proc. IEEE Int’l Conf. Control Applications (CCA 2001)*, pp.401-406, 2001.

[50] C. F.Juang and C. H.Hsu, “Structure and parameter optimization of FNNs using multi-objective ACO for control and prediction.” in *Proc.Int’l Conf.Fuzzy Systems (FUZZ 2014)*, pp. 928-933, 2014.

[51] W. N.Chen and J.Zhang,“Ant colony optimization for software project scheduling and staffing with an event-based scheduler.” *IEEE Trans. Software Engineering*, vol. 39, no.1, pp. 1-17, Jan. 2013.

[52] R. A.Mahale and S. D.Chavan,“Throughput aware ACO based routing protocol for wireless sensor network.” *IEEE Global Conf. Wireless Computing and Networking (GCWCN 2014)*, pp.234-238, 2014.

[53] Z.Gong, S.Ying, L.Li and X.Jia,“ACO based deployment optimization for software in clouds.”in *Proc. Int’l Conf. Mechatronic Sciences, Electric Engineering and Computer (MEC 2013)*, pp. 2043-2046, 2013.

[54] E.Bonabeau, M.Dorigo and G.Theraulaz,“Inspiration for optimization from social insect behaviour.” *Nature*, vol.406, no. 6791, pp. 39-42, Jul.2000.

[55] L. X. Li, “An optimization method inspired by CHAOTIC ant behavior and it’s applications [PhD.dissertation]”*Information and Communication Engineering Beijing University of Posts and Telecommunications*, 2006.
李丽香. 一种新的基于蚂蚁混沌行为的群智能优化算法及其应用研究 [D]. Diss. 北京: 北京邮电大学, 2006.

[56] Y. Y.Li, L. X.Li and H. P.Peng,“Improving Chaotic Ant Swarm Performance with Three Strategies.”*Lecture Notes in Computer Science*,vol.7928, pp.268-277, 2013.

[57] Y. Y. Li, Q. Y. Wen, L. X. Li,H. P. Peng and H.Zhu, “Improved chaotic ant swarm algorithm.”*Chinese Journal of Scientific Instrument*, vol. 30, no. 4, pp. 733-737, Apr. 2009.
(李玉英, 温巧燕, 李丽香, 彭海朋, 改进的混沌蚂蚁群算法, 仪器仪表学报, Vol. 30, No. 4, pp. 733-737, Apr. 2009)

[58] Y. Y.Li, Q. Y.Wen and L. X.Li,“Modified chaotic ant swarm to function optimization.”*The Journal of China Universities of Posts and Telecommunications*, vol. 16, no. 1, pp. 58-63, Jan. 2009.

[59] Y.Li,”Hybrid chaotic ant swarm optimization.” *Chaos Solitons and Fractals*, vol. 42, no. 2, pp. 880-889, Oct. 2009.

[60] Z.Wei, F.Ge, Y.Lu, L.Li and Y.Yang, “Chaotic ant swarm for the traveling salesman problem.” *Nonlinear dynamics*, vol. 65, no.3, pp. 271-281, Aug.2011.

[61] F. Z. Ge, Z. Wei, Y.Lu, W.Q.Lin and L.X.Li, “Chaotic ant based decentralized task allocation in wireless sensor networks”*Chinese Journal of Scientific Instrument*, vol. 33, no. 5, pp. 961-969, May. 2012.
(葛方振, 魏臻, 陆阳, 吴其林, 李丽香. “基于混沌蚂蚁的传感器网络分布式任务分配[J].” 仪器仪表学报 33.5 (2012): 961-969.)

[62] M.Wan, L.Li, J.Xiao, Y.Yang, C.Wang and X.Guo,“CAS based clustering algorithm for Web users.” *Nonlinear Dynamics*, vol. 61, no.3, pp. 347-361, Jan.2010.

[63] M.Wan, C.Wang, L.Li and Y.Yang,“Chaotic ant swarm approach for data clustering.” *Applied Soft Computing*, vol. 12, no.8, pp. 2387-2393, Aug. 2012.

[64] L.X.Li, H. P. Peng, Y.X.Yang and X.D.Wang, “Parameter estimation for Lorenz chaotic systems basedon chaotic ant swarm algorithm” *ACTA PHYSICA SINICA*, vol. 56, no. 1, pp. 51-55, Jan. 2007.
(李丽香, 彭海朋, 杨义先, 王向东. “基于混沌蚂蚁群算法的 Lorenz 混沌系统的参数估计.” 物理学报 56.1 (2007): 51-55.)

[65] L.Li, Y.Yang, H.Peng and X.Wang, “Parameters identification of chaotic systems via chaotic ant swarm.” *Chaos, Solitons and Fractals*, vol. 28, no.5, pp. 1204-1211, Jun. 2006.

[66] L.Li, Y.Yang and H.Peng, “Fuzzy system identification via chaotic ant swarm.” *Chaos, Solitons and Fractals*, vol.41, no.1, pp. 401-409, Jul.2009.

[67] Y.Tang, M.Cui, L.Li, H.Peng and X.Guan, “Parameter identification of time-delay chaotic system using chaotic ant swarm.” *Chaos, Solitons & Fractals*, vol. 41, no.4, pp. 2097-2102, Aug. 2009.

[68] H.Peng, L.Li, J.Kurths, S.Li and Y.Yang,“Topology identification of complex network via chaotic ant swarm algorithm.” *Mathematical Problems in Engineering*, 2013.

[69] J.Cai, X.Ma, L.Li, Y.Yang, H.Peng and X.Wang, “Chaotic ant swarm optimization to economic dispatch.” *Electric Power Systems Research*, vol. 77, no.10,pp. 1373-1380, Aug. 2007.

[70] Y. Li, L. Li, Q. Wen and Y. Yang, “Data fitting via chaotic ant swarm.” *Advances in Natural Computation, PT 2 Lecture Notes in Computer Science*, vol. 4222, pp. 180-183, 2006.

[71] Y. Li, L. Li, Q. Wen and Y. Yang, “Integer Programming via Chaotic Ant Swarm.” *The third international conference on Natural*

Computation (ICNC 2007), Vol. 4, pp. 489-493, Aug. 2007.

[72] D. Karaboga, "An idea based on honey bee swarm for numerical optimization." Erciyes university, 2005.

[73] X. S.Yang "Nature-inspired metaheuristic algorithms." Luniver press, 2010.

[74] X. S.Yang, and S.Deb "Cuckoo search via Lévy flights." IEEE World Conf. Nature and Biologically Inspired Computing (NaBIC 2009), pp. 210-214, 2009.

[75] C. E.Shannon, "Communication theory of secrecy systems*." *Bell system technical journal*, vol. 28, no. 4,pp. 656-715, Oct. 1949.

[76] N. K.Sreelaja and G. V.Pai, "Stream cipher for binary image encryption using Ant Colony Optimization based key generation." Applied Soft Computing, vol. 12, no. 9, pp. 2879-2895, Sept. 2012.

[77] N. K.Sreelaja and G. V.Pai, "Design of Stream Cipher for Text Encryption using Particle Swarm Optimization based Key Generation."

[78] I. K.Ali and A. I. Jarullah, "A New Keystream Generator Based on Swarm Intelligence."

[79] S.Mishra and S.Bali, "Public key cryptography using genetic algorithm." International Journal of Recent Technology and Engineering vol. 2, no. 2, pp. 150-154, 2013.

[80] S.Jhajharia, S.Mishra and S.Bali "Public key cryptography using neural networks and genetic algorithms." in *Proc. Int'l Conf.Contemporary Computing (IC3)*, pp. 137-142, 2013.

[81] D. I. Amalarethinam, and J. S. Geetha, "Image encryption and decryption in public key cryptography based on MR." in in *Proc. Int'l Conf.Computing and Communications Technologies (ICCCT)*, pp. 133-138, 2015.

[82] W.Millan, L.Burnett, G.Carter, A.Clark and E.Dawson, "Evolutionary heuristics for finding cryptographically strong S-boxes." *Information and Communication Security. Springer Berlin Heidelberg*, vol.1726, pp. 263-274, 1999.

[83] X. C. Yin and J. Yang, "Optmium algorithm of S-boxes based on fast convergence speed genetic algorithm"*ComputerApplications*, vol. 26, no. 4, pp. 803-805,Apr. 2006.
(殷新春, &杨洁. (2006). 基于快速收敛遗传算法的 S 盒的优化算法. 计算机应用, 26(4), 803-805.)

[84] Y. F. Huang "Construction of S-Boxes based on Intelligent Algorithms [Master's. dissertation]"*Information and Communication Engineering Beijing University of Posts and Telecommunications*, 2008.
(黄银锋. (2008). 基于智能算法的 S 盒设计研究 (Master′s thesis, 北京邮电大学))

[85] X. U. Xiangyang, "A new genetic algorithm and tabu search for S-box optimization." in *Proc. Int'l Conf.Computer Design and Applications (ICCDA)*, pp.492-495, 2010.

[86] Q. Zou, H. Y. Lu and W. Huang, "Genetic Tabu Search Algorithm for S-Box Optimization"*Natural Science Journal of Xiangtan University*, vol. 32, no. 2, pp. 118-122, Jun. 2010.
(邹茜, 卢涵宇, &黄伟. (2010). 基于遗传禁忌算法的 JS 盒优化算法. 湘潭大学自然科学学报, 32(2), 118-122.)

[87] X.Yin, "S box construction and result analysis based on optimal tabu-genetic algorithm." in *Proc. Int'l Conf. Education Technology and Computer (ICETC)*, pp. 539-542, 2010.

[88] A.Kadhim and S.Khalaf, "Proposal New S-box for AES Algorithm Depend on AI Bee Colony." *Eng and Tech.Journal*, vol. 33, no.1, pp. 12-24, 2015.

[89] X.Xiangyang, "The block cipher for construction of S-boxes based on particle swarm optimization." in *Proc. Int'l Conf. Networking and Digital Society (ICNDS)*, pp. 612-615, 2010.

[90] A.Sarkar and J. K.Mandal, "Swarm Intelligence based Faster Public-Key Cryptography in Wireless Communication (SIFPKC)." *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 3, no. 7, pp. 267-273, 2012.

[91] S.Khan, W.Shahzad and F. A.Khan, "Cryptanalysis of four-rounded DES using Ant Colony Optimization." in *Proc. Int'l Conf. Information Science and Applications (ICISA)*, pp. 1-7, 2010.

[92] Y. R.Wang, W. H.Lin and L.Yang, "An intelligent watermarking method based on particle swarm optimization." *Expert Systems with Applications*, vol. 38, no. 7, pp. 8024-8029, Jul. 2011.

[93] K.Loukhaoukha, J. Y.Chouinard and M. H.Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization." *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 4, pp. 303-319, Nov. 2011.

[94] D.Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks." *IBM journal of research and development*, vol. 38, no. 3, pp. 243-250, May. 1994

[95] S.Pandey and M.Mishra, "Particle swarm optimization in cryptanalysis of DES." *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 1, no. 4, pp. 379-81, Jun. 2012.

[96] S.Fenet and S.Hassas, "A distributed Intrusion Detection and Response System based on mobile autonomous agents using social insects communication paradigm." *Electronic Notes in Theoretical Computer Science*, vol. 63, pp. 41-58, May. 2002.

[97] N.Foukia, "IDReAM: intrusion detection and response executed with agent mobility architecture and implementation." In *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, pp. 264-270, 2005.

[98] S.Banerjee, C.Grosan and A.Abraham, "IDEAS: intrusion detection based on emotional ants for sensors." in *Proc. Int'l Conf. Intelligent Systems Design and Applications(ISDA 2005)*, pp. 344-349, 2005.

[99] C. L.Tsai, C. C.Tseng amd C. C.Han, "Intrusive behavior analysis based on honey pot tracking and ant algorithm analysis." in *Proc. Int'l Conf.Security Technology (ST 2009)*, pp.248-252, 2009.

[100] M.Abadi and S. Jalili, "An ant colony optimization algorithm for network vulnerability analysis." *Iranian Journal of Electrical and Electronic Engineering*, vol. 2, no. 3, pp. 106-120, Dec.2013.

[101] O.Sheyner, J.Haines, S.Jha, R.Lippmann and J. M.Wing, "Automated generation and analysis of attack graphs." in *Proc. IEEE Symp. Security and privacy (SP 2002)*, pp. 273-284, 2002.

[102] S.Jha, O.Sheyner and J. M.Wing, "Minimization and reliability analyses of attack graphs." *CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE*, 2002.

[103] S.Jha, O.Sheyner and J.Wing, "Two formal analyses of attack graphs." in *Proc. IEEE.Computer Security Foundations Workshop (CSFW 2002)*, pp. 49-63, 2002.

[104] E.Soroush, M. S.Abadeh and J.Habibi, “A Boosting Ant-Colony Optimization Algorithm for Computer Intrusion Detection.” in *Proc.Int’l Symp. Frontiers in Networking with Applications (FINA 2006)*, 2006.

[105] R. S.Parpinelli, H. S.Lopes and A.Freitas, “Data mining with an ant colony optimization algorithm.” *IEEE Trans. Evolutionary Computation,actions*, vol. 6, no. 4, pp. 321-332, Aug. 2002.

[106] J.He and D.Long, “An improved ant-based classifier for intrusion detection.” *IEEE Conf. Natural Computation (ICNC 2007)*, pp.819-823, 2007.

[107] C.Ramachandran, S.Misra and M. S.Obaidat, “FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks.” *Computer Communications*, vol. 31, no. 16, pp. 3855-3869, Oct. 2008.

[108] M. S.Abadeh and J.Habibi, “A hybridization of evolutionary fuzzy systems and ant colony optimization for intrusion detection.” *The ISC International Journal of Information Security*, vol. 2, no. 1, 2015.

[109] Y. Y.Chung and N. Wahid, “A hybrid network intrusion detection system using simplified swarm optimization (SSO).” *Applied Soft Computing*, vol. 12, no. 9, pp. 3014-3022, Sept. 2002.

[110] F.Barani and M.Abadi, “BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms.” *The ISC International Journal of Information Security*, vol. 4, no. 1, 2015.

[111] G.Indirani and K.Selvakumar, “Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks.” *International Journal of Computer Applications*, vol. 50, no. 19, pp. 1-7, Jul. 2012.

[112] P.Amudha, S.Karthik and S.Sivakumari, “A Hybrid Swarm Intelligence Algorithm for Intrusion Detection Using Significant Features.” *The Scientific World Journal*, 2015.

[113] O.Alomari and Z. A.Othman, “Bees Algorithm for feature selection in Network Anomaly detection.” *Journal of Applied Sciences Research*, vol. 8, no. 3, pp. 1748-1756, 2012.

[114] E.Michailidis, S. K.Katsikas and E.Georgopoul, “Intrusion detection using evolutionary neural networks.” in *IEEE Panh Conf. Informatics (PCI 2008)*, pp. 8-12, 2008.

[115] H.Liu, Y.Jian and S.Liu, “A new intelligent intrusion detection method based on attribute reduction and parameters optimization of SVM.” in *IEEE Int’l Work. Education Technology and Computer Science (ETCS 2010)*, pp. 202-205, 2010.

[116] A. C.Enache and V. V.Patriciu, “Intrusions detection based on Support Vector Machine optimized with swarm intelligence.” in *Proc. IEEE Symp.Applied Computational Intelligence and Informatics (SACI)*, pp.153-158, 2014.

[117] F.Kuang, S.Zhang, Z.Jin and W. Xu, “A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection.” *Soft Computing*, vol. 1, no. 13, pp.1187-1199, May. 2015.

[118] W.Feng, Q.Zhang, G.Hu and J. X.Huang, “Mining network data for intrusion detection through combining SVMs with ant colony networks.” *Future Generation Computer Systems*, vol. 37, pp. 127-140, Jul. 2014.

[119] M. S.Mahmod, Z. A. H.Alnaish and I. A. A.Al-Hadi, ”Hybrid Intrusion Detection System Using Artificial Bee Colony Algorithm and Multi-Layer Perceptron.” *International Journal of Computer Science and Information Security*, vol.13, no. 2, pp. 1-7, Feb. 2015.

[120] A. A.Aburomman and M. B. I.Reaz, “A novel SVM-kNN-PSO ensemble method for intrusion detection system.” *Applied Soft Computing*, vol. 38, pp. 360-372, Jan. 2015.

[121] T.Wang, L.Wei and J.Ai, “Improved BP Neural Network for Intrusion Detection Based on AFSA.” *2015 International Symposium on Computers and Informatics.Atlantis Press*, 2015.

[122] G.Wang, S.Chen and J.Liu, “Anomaly-based Intrusion Detection using Multiclass-SVM with Parameters Optimized by PSO.” *International Journal of Security and Its Applications*, vol. 9, no. 6, pp. 227-242, 2015.

[123] A. C.Enache and V. V.Patriciu, “Intrusions detection based on Support Vector Machine optimized with swarm intelligence.” in *IEEE Symp. Applied Computational Intelligence and Informatics (SACI 2014)*, pp. 153-158, 2014.

[124] L.Wang, C.Dong, J.Hu and G.Li, “Network Intrusion Detection Using Support Vector Machine Based on Particle Swarm Optimization.” *International Symposium on Computers and Informatics (ISCI 2015)*, pp.373-380, 2015.

[125] I.Aljarah and S.Ludwig, “MapReduce intrusion detection system based on a particle swarm optimization clustering algorithm.” *IEEE Cong. Evolutionary Computation (CEC)*, pp.955-962, 2013.

[126] N.Cleetus and K. A.Dhanya “Multi-objective functions in particle swarm optimization for intrusion detection.” in *Proc. Int’l Conf. Advances in Computing, Communications and Informatics (ICACCI)*, pp. 387-392, 2014.

[127] N. K.Sreelaja and G. V.Pai, “Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks.” *Applied Soft Computing*, vol. 19, pp. 68-79, Jun. 2014.

[128] A. Jantan and A. A. Ahmed, “Honey Bee Intelligent Model for Network Zero Day Attack Detection.” *International Journal of Digital Content Technology and its Applications*, vol. 8, no. 6, pp. 45, Dec. 2014.

杨义先 北京邮电大学, 教授, 博士生导师。长江学者奖励计划特聘教授、国家杰出青年基金获得者、国家级教学名师。在编码密码学、信息与网络安全、信号与信息处理等领域有深厚的造诣。已经承担了国家级和省部级重点科研项目四十余项, 发表了高水平的论文300余篇, 完成出版了学术专著二十余部。
Email: yxyang@bupt.edu.cn

李丽香 北京邮电大学, 教授, 博士生导师。全国百篇优秀博士学位论文获得者, 教育部新世纪优秀人才, 霍英东教育基金会资助者, 香江学者奖获得者, 北京高等学校青年英才计划获得者, 多年来一直从事群体智能、网络安全等研究工作, 近五年发表论文 80 余篇, 出版专著一部, 主持或参研国家级课题10项。