doi:10.3969/j.issn.1000-436x.2013.03.013

基于混沌粒子群的 IDS 告警聚类算法

胥小波[1,2]，蒋琴琴[2]，郑康锋[2]，武斌[2]，杨义先[2]
（1. 中国电子科技集团公司 第三十研究所，四川 成都 610041；2. 北京邮电大学 信息安全中心，北京 100876）

摘 要：为了提高入侵检测系统(IDS)的告警质量，减少冗余报警，提出了一种基于混沌粒子群优化的 IDS 告警聚类算法。算法将混沌融入到粒子运动过程中，使粒子群在混沌与稳定之间交替运动，逐步向最优点靠近。该算法能够克服粒子群算法的早熟、局部最优等缺点，指导聚类中心寻找到全局最优解。通过理论分析与实验测试，验证了该算法在入侵检测系统中，能够大量减少告警数量，提高告警质量，具有较高的检测率和较低的误报率。
关键词：入侵检测系统；告警聚类；混沌；粒子群优化
中图分类号：TP393.08 **文献标识码：**A **文章编号：**1000-436X(2013)03-0105-06

IDS alert clustering algorithm based on chaotic particle swarm optimization

XU Xiao-bo[1,2], JIANG Qin-qin[2], ZHENG Kang-feng[2], WU Bin[2], YANG Yi-xian[2]
(1. The 30th Institute of China Electronics Technology Group Corporation, Chengdu 610041, China;
2. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In order to improve the quality of alerts in intrusion detection system (IDS) and reduce the large number of redundant alarms, an IDS alerts clustering algorithm based on chaotic particle swarm optimization was proposed. It made the motion of particles with characteristics of chaos，so as to make particles move between the state of chaos and stable, and gradually close to the optimal value. The CPSO algorithm could overcome the problem of premature and local optimization, and take the center of cluster to find the global optimal solution. The analysis and experiment show that the algorithm can significantly reduce the number of alerts improve its quality, and has a high detection rate and low false detection rate.
Key words: intrusion detection system; alert clustering; chaos; particle swarm opti ization

1 引言

随着信息时代的发展，网络和通信技术不断进步，计算机网络和操作系统的漏洞与安全隐患日益暴露在人们面前，网络信息安全状况日益恶化。入侵检测是对攻击行为进行检测的主要工具，是维护网络安全的重要技术手段之一。

入侵检测系统收集和分析网络数据分组，识别可能存在的攻击事件，并对攻击事件产生报警。然而，IDS 每天可能会产生数以万计的告警[1~3]。如果没有适当的告警管理，安全分析人员将被淹没于大量的网络入侵告警中。

大量的网络告警数据不仅无法真实地反映网络所遭受的攻击情况，反而增加了安全人员的工作负担，过多的无用告警将有用信息淹没，使得安全分析人员无法找到系统的漏洞和防范的重点，从而导致入侵检测的可用性大大降低。因此，需要一种有效的方法，将大量冗余告警去除，分析出系统受到的真实攻击行为，有利于安全人员对系统进行安全管理和防护。

收稿日期：2011-09-25；**修回日期：**2012-06-29
基金项目：中央高校基本科研业务费专项基金资助项目（BUPT2009RC0218**）；总装基金资助项目（**9140A15060109DZ082**）；教育部科学技术研究重点基金资助项目**
Foundation Items: The Fundamental Research Funds for the Central Universities (BUPT2009RC0218)；The Research Foundation of CPLA General Equipment Department (9140A15060109DZ082)；The Key Project of Chinese Ministry of Education

2 相关工作

数据挖掘技术在入侵检测中的应用日益广泛，特别是在管理 IDS 告警显示方面。相关研究者把模式识别、数据挖掘等知识运用到告警的分析上来，对告警信息进行聚合和关联分析，得出了较好的研究成果。聚类是一种广泛使用的数据挖掘技术，在处理海量的告警方面有着大量的研究及应用。

Viinikka[4]等提出基于时间序列模型融合大规模告警的方法，将特定时间序列的告警进行融合；Vaarandi[5]等提出基于频率集数据挖掘的告警分类算法，从大量告警中提取频繁项集；Njogu[6]等提出告警聚类方法减少告警数量，根据告警的相关性、重要性、频率等方面的相似程度进行聚类。Fei[7]等提出了一种利用变长染色体的遗传算法对 IDS 告警进行层次化聚类的方法，聚类数量与染色体长度相等，能够对告警进行较好的分类。李永忠[8]等提出了基于粒子群优化的聚类入侵检测算法，克服传统的 K 均值算法易陷入局部极小值的缺点，使算法具有较好的全局收敛性，将粒子群优化算法应用于入侵检测，给出了基于粒子群优化的 K 均值聚类算法。

粒子群算法(PSO)由于算法概念简单、实现容易，获得了很大发展。相对遗传算法而言，PSO 不需要进行交叉和变异，操作较为简单，而且在迭代过程中，粒子运动的思路与人类决策相似，易于理解[9]。但是，传统粒子群算法初期收敛较快，而在后期容易陷入早熟、局部最优。针对这一特点，本文提出了一种新的混沌粒子群优化算法，不同于已有的混沌粒子群算法的简单粒子序列替换，该算法将混沌融入到粒子运动过程中，使粒子群在混沌与稳定之间交替运动，逐步向最优点靠近。

本文将混沌粒子群算法与 K 均值算法结合，对 IDS 告警进行聚类，并对 KDDCUP99 数据集进行测试，实验结果表明，该算法在入侵检测中能获得理想的检测率和误检率，能够减少告警数量，改善告警质量，最终生成攻击场景。

3 混沌粒子群算法

在文献[10]中，针对混沌蚁群（CAS）算法[11]进行改进，并结合粒子群算法，提出了混沌粒子群优化(CPSO)系统动力学模型。现将其应用于告警聚类算法中，以改善聚类效果。CPSO 模型如式(1)~式(3)所示。混沌粒子群具体的数学模型定义如下

$$v_{id}(t+1)=w\times v_{id}(t)+c_1\times\mathrm{rand}()\times[p_{id}(t)-x_{id}(t)]+c_2\times\mathrm{rand}()\times[p_{gd}(t)-x_{id}(t)] \tag{1}$$

$$c_{id}(t) = c_{id}(t-1)^{(1+r_{id})} \tag{2}$$

$$x_{id}(t) = (x_{id}(t-1) + y_d\times M_i)\times \exp((1-\exp(-200\times c_{id}(t)))\times(3-\frac{7.5}{y_d}(x_{id}(t-1) + y_d\times M_i)))-y_d\times M_i+\exp(-400c_{id}(t))\times v_{id}(t) \tag{3}$$

其中，式(1)为粒子速度更新算法。式(2)为混沌变量，影响粒子的混沌程度。r_{id} 是一个小于 1 的正常数，定义为第 i 个粒子的第 d 维混沌因子。式(3)在粒子群的位置更新中引入混沌。t 表示迭代次数，ψ_d 表示搜索测度，M_i 表示粒子 i 的搜索空间向负方向移动的比例，如：ψ_d=100，M_i=0.5，则表示搜索空间为[－50,50]。

一直处于混沌或稳定状态对于寻找最优值没有任何意义，只有在混沌与稳定的交替中才能不断向最优结果靠近。也就是说，要在粒子稳定时，引入混沌，跳出局部最优；在粒子不稳定时，加速向最优值靠近，加快收敛过程。混沌算法采用了文献[11]中的混沌算法，即 Sole 等给出的混沌系统[12]，混沌迭代式如式(4)所示。

$$x = x\exp(m(1-x)) \tag{4}$$

该算法将混沌融入到粒子运动过程中，不同于已有的混沌粒子群算法的简单粒子序列替换，使粒子群在混沌与稳定之间交替向最优点靠近，将混沌运动与粒子群运动结合到一起，并通过混沌因子来调节混沌程度，具有较好的全局搜索能力。数值结果表明该方法用于解决函数最优化问题的有效性，并且能有效避免粒子群优化算法的早熟收敛问题，能跳出局部最优，极大提高了计算精度和全局寻优能力[10]。

4 告警聚类算法

4.1 问题描述

告警聚类需要解决的问题：将大量的 IDS 告警进行分类整合，每个集群产生一个告警作为代表，阐述网络正在发生的攻击行为。将 IDS 告警聚类定义为：给定一个告警数据集 $X=\{x_1, x_2, \cdots, x_n\}$，将其分为 K 个聚类 $C_1, C_2, \cdots, C_k$，满足式(5)所给出的条件。

$$\begin{cases}\bigcup_{i=1}^{k} C_i = X; C_i \neq \varnothing \\ C_i \cap C_j = \varnothing; (i, j = 1,2,\cdots,k; i \neq j)\end{cases} \tag{5}$$

本文采用最小均方误差法（MSE）作为聚类评判标准，如式(6)所示。

$$MSE = \sum_{i=1}^{k} \sum_{x_j \in C_i} \left\| x_j - z_i \right\|^2 \tag{6}$$

其中，z_i 为聚类中心。聚类的目标就是使均方误差达到最小。

4.2　告警空间定义

为了实现 IDS 告警的聚类，首先需要将告警映射为 N 维向空间上的点集。针对研究中广泛采用的开源软件 Snort，将其每条告警映射为(AID，Atime，Aproto，AsrcIP，AsrcPort，AdestIP，AdestPort，Amsg，Acontent，Aclasstype)。

定义告警之间的距离为

$$DIS(X,Y)=\sqrt{\sum_{i=1}^{n}(\mathrm{DIS}(XA_i,YA_i))^2} \tag{7}$$

其中，X、Y 为告警，XA_i 为告警 X 的 A_i 属性值，当属性值取实数值时，其距离定义如式(8)所示。其中，a、b 为告警的属性值。

$$DIS(a,b)=\frac{|a-b|}{|a\max-a\min|} \tag{8}$$

当属性值为字符串时，距离定义如式(9)所示。

$$DIS(a,b)=\begin{cases}1, a=b\\ 0, a\neq b\end{cases} \tag{9}$$

4.3　聚类算法流程

该算法将每组聚类中心对应到一个粒子，然后利用粒子群方法进行搜索，找到最优告警分类结果。具体步骤如下。

Step1　初始化粒子群，在搜索空间范围内随机产生 N 个粒子，每个粒子对应一组聚类中心。初始粒子的速度和方向随机产生。

Step2　根据聚类中心位置，将告警以最近原则分配到各个聚类中。然后利用式(6)~式(9)计算 SSE 值。更新 Pid(个体历史最优)和 Pgd(全局历史最优)。

Step3　根据式(1)、式(3)更新粒子速度、位置，进行混沌搜索，并根据式(2)更新粒子群混沌变量。

Step4　判断终止条件是否满足，如果满足，则记录 Pid 和 Pgd 值并退出程序；否则转至 Step 2。

算法代码如图 1 所示。算法初始化粒子群为 1)~6)行，其中，N 为粒子个数，K 为聚类个数。7)~25)行为粒子群混沌搜索过程，15)~18)行为保存个体最优值 P_{id}，19)~23)行为保存全局最优值 P_{gd}。26)~33)行为存储分类结果。fitness(x，D)实现了具有 D 维的粒子群中心按式(6)对适值进行计算。

混沌粒子群算法

输入:

告警集: $X=\{x_1, x_2, \cdots, x_n\}$

聚类数量: k

输出:

Clusters:$\{C_1, C_2, \cdots, C_k\}$

初始化 K **个聚类中心**:

1) for i=1:N
2) for j=1:k
3)　$v(i,j)=\Psi_j*M_i*(-1+2*\mathrm{rand})$;
4)　$x(i,j)=\Psi_j*M_i*(-1+2*\mathrm{rand})$;
5) end for
6)end for

混沌粒子群迭代:

7)for t=1:MaxDT
8) for i=1:N
9) $v(i,:)=\mathrm{wight}*v(i,:)+c1*\mathrm{rand}*(y(i,:)-x(i,:))+c2*\mathrm{rand}*(pg-x(i,:))$;
10)　for l=1:D
$x(i,:)=x(i,:)+v(i,:)$;
11)　if move<10^{-6}
12)　$w(i,l)=0.999$;
13)　end
14)　$x(i,l)=(x(i,l)+((7.5)*M_i/\Psi_l))*\exp((1-\exp(-a.*w(i,l)))*(3-\mathrm{vq}(l)*(x(i,l)+((7.5)*M_i/\Psi_l))))-((7.5)*M_i/\Psi_l)+(\exp(-2*a*w(i,l)+b))*v(i,l)$;
15)　if fitness($x(i,:),D$)<$p(i)$
16)　$p(i)$= fitness($x(i,:),D$);
17)　$y(i,:)=x(i,:)$;
18)　end if
19)　if $p(i)$<fitness(pg,D)
20)　$pg=y(i,:)$;
21)　end if
22)　end for
23)　Pbest(t)=fitness(pg,D);
24) end for
25)end for

存储分类结果:

26)for t=1:n
27)　for c=1:k
28)　$DIS_c=\|x_t-z_c\|$；
29)　end for
30)　$d=\{d_1,d_2, \cdots, d_k\}$；
31)　find min(d);
32)　C_p.add(x_t);
33)end for

图 1　混沌粒子群告警聚类算法

4.4 攻击场景构建

攻击场景构建在上述告警聚类基础上，采用“行为+位置+目的”的三段式攻击行为表述方法，构建攻击场景，还原攻击入侵过程。

4.4.1 攻击行为提取

行为是指攻击者采用何种方法进行攻击，主要从告警消息的 MSG 字段进行提取。该算法将攻击行为分为以下几类：probe(探测)、scan(扫描)、flood(洪泛)、overflow(溢出)、authenticate(鉴别)、bypass(迂回)、spoof(欺骗)、read(读取)、copy(拷贝)、steal(盗取)、modify(修改)、delete(删除)。

通过以上关键字对规则的 MSG 字段进行分类，得出可以采用的行为关键字为：Probe、Scan、Flood、Overflow、Bypass、Spoof。而 Read、Copy、Steal、Modify、Delete 等信息可以从主机端获得。

4.4.2 攻击位置提取

位置是指攻击者攻击的作用点，主要分为 2 类：网络（IP 地址、端口、协议、应用）、主机（注册表、进程、文件）。

IP 地址和端口均可以从告警信息 MSG 的地址字段中获取。icmp、pop2、ftp、smtp、imap、netbios、P2P 等协议类型，均可以从告警中 MSG 信息的开始的大写字符串获得。因为规则文件是通过协议来命名的，如 P2P.rules 里面都是针对 P2P 协议的攻击，而每一条规则的 MSG 都以已所在文件名字符串的大写形式开始。如$HOME_NET any -> $EXTERNAL_NET any (msg:"P2P GNUTella client request"; flow: to_server,established; content: "GNUTELLA"; depth:8; metadata:policy security-ips drop; classtype: policy-violation; sid:1432; rev:7)。

告警中的 MSG 信息还包括如下应用程序位置：聊天工具（chat）、游戏(game)、mail、oracle 数据库、策略(policy)、http 服务器(sql-injection、web-attacks)、mysql 数据库、多媒体(windows media)等，均可从规则开始的大写字符串获得。

4.4.3 攻击目的提取

目的是指攻击者的攻击意图，即攻击者希望得到的攻击效果，这个要素的信息主要从 classtype 字段来获得。将目的分为以下 14 类。

尝试获取权限（用户、管理员）：attempted-user\ attempted-admin。

成功获得权限（用户、管理员）：successful-user\ successful-user\ unsuccessful-user。

尝试非法登录（口令猜测，暴力破解）：suspicious-login\ default-login-attempt。

尝试窃取信息：attempted-recon。

窃取信息成功\失败：successful-recon-limited\ successful-recon-largescale。

扫描：network-scan\protocol-command-decode。

尝试植入恶意内容（代码、命令、木马）：shell code-detect\system-call-detect\string-detect\trojan-activity。

实施拒绝服务攻击：attempted-dos\denial-of-service\successful-dos。

木马通信：trojan-activity。

正在实施拒绝服务攻击：attempted-dos\ denial-of-service\successful-dos。

针对 Web 应用的攻击：web-application-attack\ web-application-activity\non-standard-protocol。

违反内部策略：policy-violation。

RPC 服务攻击：rpc-portmap-decode。

潜在可能攻击、存在安全隐患或者无法识别的流量：unknown\bad-unknown。

4.4.4 攻击场景还原

攻击场景还原存在不能从告警信息中获得完全的 3 个要素的情况。以端口扫描为例，一般情况下，端口扫描是为以后的攻击打基础，往往伴随着后续的攻击，如扫描一些特定的漏洞或者端口。但是如果只是单纯的扫描 IP 地址则看不出攻击的目的。

攻击描述字符串不需要三要素都兼备。若三要素齐全，攻击描述字符串为：行为+位置+“以”+目的；若没有行为要素，攻击描述字符串为：“针对”+位置+“以”+目的；若没有目的要素，攻击描述字符串为：行为+位置。具体攻击场景还原实例见 5.2 节。

5 实验测试

5.1 告警聚类算法测试

为了验证算法的应用效果，入侵检测测试数据采用 KDDCUP99 网络数据集进行实验。混沌粒子群参数设置为：w =0.729 8，$c1$=$c2$=1.496 2，T=1 000，$r(i,d)$=0.5+0.005rand，N=20，Cid(t)=0.999，$?_d$ 为各自搜索空间长度，Mi=0.5，粒子初始值为 $?_d \times Mi \times (2*\text{rand}()-1)$。

其中，粒子群算法结果来自文献[9]。对比表 1

的结果可以看出：本文所提出的混沌粒子群告警聚类算法结果明显好于粒子群告警聚类算法。本文平均告警检测率为 80.35%，高于 POS-KM 聚类算法的 74.43%。而平均误警率为 1.35%，低于 POS-KM 聚类算法的 1.86%。可见，CPOS-KM 聚类算法更有效地检测入侵攻击行为。

表 1　　告警聚类算法比较结果

聚类数 K	PSO-KM 聚类算法		本文 CPSO-KM 聚类算法	
	检测率	误警率	检测率	误警率
20	73.7	0.91	75.4	0.82
30	86.7	1.36	90.3	1.13
40	85.3	2.47	88.9	1.87
50	76.4	2.58	81.6	1.94
60	69.8	2.12	75.3	1.53
70	69.7	1.78	76．5	1.08
80	69.7	1.78	74.5	1.05
平均	74.43	1.86	80.35	1.35

5.2　攻击场景构建测试

在真实网络环境中，对攻击场景构建进行测试，在主机 192.168.1.108 上利用 MS08-067 漏洞，对主机 192.168.1.114 进行攻击。聚合后告警有如下 3 条。

ALEART 1: 04/09-14:51:43.051508 [**] [1: 648:10] SHELLCODE x86 NOOP [**] [Classification: Executable code was detected] [Priority: 1] {TCP} 192.168.1.108:3169 -> 192.168.1.114:135。

场景构建步骤 1：针对 SHELLCODE x86 漏洞，以尝试植入可执行代码。

ALEART 2: 04/09-14:51:43.051508 [**] [1: 3397:8] NETBIOS DCERPC NCACN-IP-TCP ISystemActivatorRemoteCreateInstance attempt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.1.108:3169 -> 192.168.1.114:135。

场景构建步骤 2：探测 NETBIOS 漏洞。

ALEART 3: 04/09-14:51:30.112161 [**] [1: 7209: 10] NETBIOS DCERPC NCACN-IP- CP srvsvcNetrPathCanonicalize overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.108:3161 -> 192.168.1.114:445。

场景构建步骤 3：溢出 NETBIOS 漏洞以尝试获得管理员权限。

结合主机入侵告警信息：最后一步为开启目标端口，攻击成功。终上所述，入侵过程与告警场景构建结果步骤相符合。

6　结束语

本文利用混沌的遍历性和粒子群收敛快的特点，提出了一种新的混沌粒子群算法。该算法将混沌融入到粒子运动过程中，不同于已有的混沌粒子群算法的简单粒子序列替换，使粒子群在混沌与稳定之间交替向最优点靠近。利用混沌粒子群算法指导 K 均值算法的初始聚类中心的选择，从而使得聚类容易收敛到全局最优，摆脱了初始聚类中心点选择对最终聚类结果的影响。相对于目前的混沌粒子群算法，本文提出的混沌粒子群算法具有更好的跳出局部最优，寻找全局最优解的能力。通过对 KDDCUP99 数据集进行测试，实验证明本文提出的混沌粒子群优化告警算法具有较高的检测率和较低的误警率。在此基础上，本文还引入了由聚类后的告警还原出攻击场景的方法，经实验证明，该方法可以有效地还原攻击步骤。

参考文献：

[1] VAARANDI R. Real-time classification of IDS alerts with data mining techniques[A]. MILCOM 2009[C]. Boston, Massachusetts: IEEE Press, 2009. 1-7.

[2] AI-MANIRY S O, ZHANG H L, ABBAS A R. IDS alarms reduction using data mining[A]. WCCI 2008[C]. Hong Kong, China: IEEE Press, 2008. 3564-3570.

[3] PIETRASZEK T. Using adaptive alert classification to reduce false positives in intrusion detection[A]. RAID 2004[C]. Sophia Antipolis, France: Springer-Verlag. 2004. 102- 124.

[4] VIINIKKA J, DEBAR H, ANSSI L, *et al*. Processing intrusion detection alert aggregates with time series modeling[J]. Information Fusion Journal, 2009, 10(4): 312-324.

[5] VAARANDI R, PODINS K. Network IDS alert classification with frequent item-set mining and data clustering[A]. CNSM 2010[C]. Niagara Falls, Canada, IEEE Press, 2010. 451-456.

[6] NJOGU H W, LUO J W. Using alert cluster to reduce IDS alerts[A]. ICCSIT 2010[C]. Chengdu, China, IEEE Press, 2010. 467-471.

[7] FEI A, DONG X L. Hierarchically clustering IDS alarms using a GA with vary-lengthed chromosomes[A]. ISIP 2010[C]. China: IEEE Press, 2010.172-177.

[8] LI Y Z, YANG G, XU J, *et al*. Anomaly detection for clustering algo-

rithm based on particle swarm optimization[J]. Journal of Jiangsu University of Science and Technology(Natural Science Edition), 2009, 23(1): 51-55.

[9] WEN Z W, LI R J. Fuzzy C-means clustering algorithm based on improved PSO[J]. Application Research of Computers, 2010, 27(7): 2520-2522.

[10] XU X B, ZHENG K F, LI D, *et al*. A new chaos-particle swarm optimization algorithm[J]. Journal on Communications, 2012,33(1):24-30.

[11] LI L X, YANG Y X, PENG H P, *et al*. An optimization method inspired by chaotic ant behavior[J]. International Journal of Bifurcation and Chaos, 2006, 16: 2351-2364.

[12] SOLE R V, MIRAMONTES O, GOODWIN B C. Oscillations and chaos in ant societies[J]. Journal of Theoretical Biology, 1993, 161(3): 343-357.

作者简介：

胥小波（1985-），男，四川盐亭人，北京邮电大学博士生，主要研究方向为信息安全、人工智能算法。

蒋琴琴（1987-），女，浙江金华人，北京邮电大学硕士生，主要研究方向为人工智能、数据挖掘。

郑康锋（1975-），男，山东烟台人，北京邮电大学教授，主要研究方向为网络与信息安全。

武斌（1981-），男，山东泰安人，北京邮电大学讲师，主要研究方向为网络与信息安全。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授、博士生导师，主要研究方向为信息安全、密码学。

（上接第 104 页）

[5] SEOL D, KWON U, IM G. Performance of single carrier transmission with cooperative diversity over fast fading channels[J IEEE Transactions on Communications, 2009, 57(9): 2799-2807.

[6] EGHBALI H, MUHAIDAT S, AL-DHAHIR N. A novel receiver design for single-carrier frequency domain equalization in broadband wireless networks with amplify-and-forward relaying[J]. IEEE Transactions on Wireless Communications, 2011, 10(3): 721-727.

[7] AMIN O, GEDIK B, UYSAL M. Channel estimation for amplify-and-forward relaying: cascaded against disintegrated estimators[J]. IET Communications, 2010, 4(10): 1207-1216.

[8] CHU C. Polyphase codes with good periodic correlation properties[J]. IEEE Transactions on Information Theory, l972, 18(7): 531-532.

[9] SAYED H. Fundamentals of Adaptive Filtering[M]. New York: Wiley-IEEE Press, 2003. 658-665.

[10] FRAGOULI C, AL-DHAHIR N, TURIN W. Training- based channel estimation for multiple-antenna broadband transmissions[J]. IEEE Transactions on Wireless Communications, 2003, 2(2): 384-391.

作者简介：

王永川（1977-），男，河北元氏人，博士，军械工程学院讲师，主要研究方向为通信信号处理、协作通信等。

陈自力（1964-），男，山西永济人，硕士，军械工程学院教授、博士生导师，主要研究方向为信号处理、遥控遥测等。