引入偏移量递阶控制的网络入侵HHT检测算法

章武媚 陈庆章
(浙江工业大学计算机科学与技术学院 杭州 310023)

摘 要 在强干扰背景低信噪比下对网络潜质入侵信号的准确检测是决定网络安全的关键。传统的Hilbert-Huang变换(HHT)入侵信号检测算法在求解入侵信号的瞬时频率特征时,因包络线失真引起的边界控制误差,会造成频谱泄漏,从而导致检测性能较差。提出了一种基于时间-频率联合分布特征和偏移量递阶控制HHT匹配的网络入侵信号检测算法,即构建网络潜质入侵数学演化模型,把复杂的入侵信号分解成IMF单频信号,得到入侵检测系统的状态转移方程,基于Hilbert变换对入侵信号进行离散解析化处理,构建入侵信号解析模型。对每个入侵信号经验模态分解后的解析模型IMF分量用Hilbert变换进行谱分析,通过递阶控制调整HHT频谱偏移,将残差信号投影与入侵信号的Hilbert边际谱进行匹配,减小包络线失真引起的边界控制误差,抑制频谱泄漏,实现对入侵信号的精确检测和参数估计。实验表明,该算法进行网络入侵信号检测时,具有较强的抗干扰性,能从低信噪比背景下有效检测出入侵信号,检测性能有较大提高。

关键词 网络入侵,检测算法,递阶控制
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.023

Network Intrusion Detection Algorithm Based on HHT with Shift Hierarchical Control

ZHANG Wu-mei CHEN Qing-zhang
(College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract In the strong interference background and low signal-to-noise, the accurate detection of network intrusion potential signal is the key of network security. The traditional Hilbert-Huang transform (HHT) intrusion signal detection algorithm has boundary control error resulted from envelope distortion, and spectrum leakage is occurred which leads the bad detection performance. An improved detection algorithm was proposed based on the time-frequency distribution feature and offset hierarchical control network HHT matching. The network potential intrusion mathematical evolution model is constructed, and the complex signals are decomposed into IMF single frequency signal. The intrusion detection system state transfer equation is obtained. The discrete analytical processing of the intrusion signal is taken based on Hilbert transform, and the signal model is obtained. The intrusion signal is decomposed with empirical mode, and the IMF component is analyzed by Hilbert spectrum. The HHT frequency shift is adjusted by hierarchical control mechanism, and residual projection and intrusion signal Hilbert marginal spectrum are matched. The envelope distortion is reduced, and the spectral leakage is suppressed. The accurate detection and parameter estimation of intrusion signal are achieved. Experiments show that this algorithm has strong anti-interference performance in intrusion signal detection, which can detect intrusion signal with low SNR effectively, and the performance of detection is improved.

Keywords Network intrusion, Detection algorithm, Hierarchical control

1 引言

随着计算机网络技术和信息技术的快速发展,计算机网络和信息技术在给人们带来极大便利的同时,网络安全问题日益凸显。目前,针对网络的攻击和入侵形式呈现多样化和频繁化发展态势,网络入侵信号通过植入木马病毒,对计算机用户发动主动攻击,导致用户系统崩溃,从而窃取用户的账户信息和商业秘密等。防御网络入侵最基本的方法为网络防火墙,后来发展为更高级的网络入侵容忍系统和入侵检测系统。然而,在网络安全对抗与反对抗的发展过程中,网络潜质入侵信号表现为一种隐蔽特征很强的微弱攻击信号,背景杂波干扰性强,通常在信噪比极低的背景下对用户发动攻击,传统的入侵信号检测系统和算法难以对这类入侵信号实现有效检测,计算机网络用户面临的安全威胁增大,因此,研究一种有效的网络入侵信号检测算法,对提高计算机系统和网络用户的安全性能具有重要意义[1]。

近年来,对微弱网络入侵信号的检测逐渐进入人们研究视野,特别是随着网络攻击行为的日益猖獗,引入现代信号处

到稿日期:2014-01-22 返修日期:2014-03-26 本文受浙江水利科技项目(RC1226,RC1421),浙江省科技创新团队项目(2012R10022-09)资助。
章武媚(1971-),女,硕士,副教授,主要研究方向为计算机应用技术,E-mail:190037572@qq.com;陈庆章(1955-),男,博士,教授,主要研究方向为计算机应用技术、网络与多媒体技术。

理技术来研究网络入侵信号检测成为网络安全领域研究的重点。传统方法中，主要采用了基于时频分析的入侵信号检测算法和基于非线性时间序列分析的入侵信号检测算法，其中，文献[2]采用了一种基于博弈论的网络入侵系统病毒信号安全性扩展检测算法，该算法对攻击者的行动策略进行博弈机制伴随紊乱跟踪处理，实现对入侵信号的特征分解和检测，但算法的平均失效时间较短，不适用于对大规模潜质入侵病毒的检测。文献[3]中，提出采用干扰攻击定位方法来优化入侵容忍系统的状态转移特征，对病毒的入侵路径进行量化分析，实现了对潜质入侵信号的结构层次性特征分解，然而该算法没能有效避免网络防御措施之间相互的影响，导致对低信噪比的入侵信号检测效果不好，系统安全性受到限制。其中，文献[4]提出一种基于流数据分类和分形维分析的 DoS 入侵信号检测算法，用以改进病毒与干扰杂波信号的分类属性，提高数据聚类能力，实现病毒免疫抵御攻击行为。算法在实现过程中采用训练和检测两个阶段，每个阶段都需要读入入侵病毒的通信流信息特征，算法复杂度较高，实时性差，事实上实现困难。文献[5]中，樊爱宛、时合生等人提出一种基于特征选择和 SVM 参数同步优化的网络入侵检测算法，该算法将网络入侵检测正确率作为约束目标函数进行同步最优特征子集求解，在提高网络入侵信号检测正确率方面具有一定的收益，但是没能自适应求解特征选择和 SVM 参数之间的关联特征，导致在对网络入侵特征迭代检测中产生数据冗余，增大了计算开销，降低了检测精度。文献[6]中采用一种基于入侵容忍系统的病毒免疫安全属性分析方法抵御病毒入侵行为，通过设计系统状态转移模型，在入侵信号自我演化过程中实现入侵特征量化平衡，提高入侵容忍系统的安全属性，从而达到对网络入侵信号准确检测的目的，然而该算法设计中没有对强杂波进行过滤，抗干扰能力不强。文献[7]中提出一种采用余弦调制滤波组合的多径无线网络潜质入侵信号子带合成方法，该算法把网络潜质入侵信息在信号子带上进行数据聚类合成，然后采用粒子滤波算法实现对潜质入侵信号的检测，算法在抗干扰能力上具有一定的增益，但是无法有效检测具有双向延拓特性的低信噪比潜质入侵信号。另外，文献[8]中葛海慧、肖达等人提出一种基于动态关联分析的网络入侵检测算法，它对连续发生的关联性攻击行为检测性能较好。文献[9]中，张宗飞提出一种基于量子进化算法的网络入侵检测特征选择算法，保证了入侵检测的分类性能，增强了对入侵信号的寻优性能；由于近年来发现的网络潜质入侵信号具有频率突变非线性双向延拓特性，与强信混比条件下的暂态电磁干扰信号类似，因此，引入电磁信号检测领域中的 Hilbert-Huang 变换(HHT)检测算法，对提高这类潜质入侵信号检测性能大有裨益，对此，文献[10]提出一种基于经验模态分解和经典希尔伯特变换的网络入侵信号检测算法，然而，该算法在求解入侵信号的瞬时频率特征时，因包络线失真引起的边界控制误差，会造成频谱泄漏，从而导致检测性能较差。

针对上述问题，本文对传统的基于 HHT 的网络潜质入侵信号检测算法进行改进，引入偏移递阶控制算法，提出一种改进的网络入侵信号 HHT 检测算法。首先构建网络潜质入侵数学演化模型和信号模型，然后对改进算法思想和框架进行描述，对检测算法进行设计和实现，最后用仿真实验验证了算法的优越性能。

2 网络潜质入侵数学演化模型和信号模型

2.1 网络潜质入侵数学演化模型

本文研究和设计基于 HHT 的改进网络入侵信号检测算法，首先给出强干扰低信噪比背景的网络潜质入侵数学演化模型，并进行安全属性分析，为构建网络入侵信号模型奠定基础[11]。

网络潜质入侵数学演化模型可以根据状态入侵信号状态特征采用固有模态函数进行时频特征分析，因此研究入侵信号检测模型需首先进行信号特征的时频状态转移建模[12]，设潜质入侵信号的状态空间固有模态函数为：

$$y(t)=\frac{1}{\pi}P\int\frac{x(\tau)}{t-\tau}\mathrm{d}\tau=x(t)*\frac{1}{\pi t} \tag{1}$$

式中，P 为线性平稳柯西主频特征，$x(t)$为原始入侵信号，τ 为信号的特征时间尺度，任意原始信号 $x(t)$作为网络潜质入侵信号的频谱特征由两部分组成，即经验模态分解和 Hilbert 谱分析，分别描述为：

$$\begin{cases} c_i(t)=\| X_s-\sum_{i=1}^{n}\omega_i X_i \|_2^2, s=1,\cdots,n \\ h_i(t)=\dfrac{\dfrac{1}{\dfrac{\upsilon_s}{\sum_{j=1}^{n}\upsilon_j}+\lambda}}{\sum_{j=1}^{n}\dfrac{\upsilon_s}{\sum_{j=1}^{n}\upsilon_j}+\lambda}, s=1,\cdots,n \end{cases} \tag{2}$$

式中，υ_s 表示具体网络潜质入侵行为下各状态保持时间 X_s 与 ω_i 的偏差，网络系统在遭受潜质入侵状态下被屏蔽的状态节点个数越多，表示 υ_s 的值越大；网络入侵模型在数学演化过程中入侵初始时间 λ 设定为 $a(t)$，由此，把复杂的入侵信号分解成 IMF 单频信号，计算稳态概率得到：

$$WD_x(t,f)=\int x(t+\frac{\tau}{2})x^*(t-\frac{\tau}{2})\mathrm{e}^{-j2\pi ft}\mathrm{d}\tau \tag{3}$$

式中，f 表示信号的瞬时频率，x^* 表示对原始信号取卷积，上式表示了网络潜质入侵数学演化模型的能量模型在时频平面上的分布特性，通过上式构建网络潜质入侵数学演化模型，可以得到入侵检测系统的状态转移方程：

$$WT_f(a,\tau)=\frac{1}{\sqrt{a}}\int x(t)\psi^*(\frac{t-\tau}{a})\mathrm{d}t \tag{4}$$

式中，$x(t)$是潜质入侵信号平方可积函数，$\psi(t)$是基波函数。通过潜质入侵数学演化变换可见，入侵信号与两个参数 a 和 τ 有关，式中 $a(a>0)$被称为尺度因子，以此为基础可以构建入侵信号模型，为检测系统设计提供原始信号源。

2.2 潜质入侵信号模型及问题描述

在上述构建的网络潜质入侵数学演化模型的基础上，对式(4)的入侵检测系统状态转移方程进行 Hilbert 变换，使入侵信号离散数据解析化，构建入侵信号解析模型：

$$z(t)=x(t)+iy(t)=a(t)\mathrm{e}^{i\theta(t)} \tag{5}$$

式中，$z(t)$表示入侵信号，$x(t)$表示信号解析模型的实部，$y(t)$表示入侵信号的固有模态函数，$a(t)$表示潜质入侵数据序列的极大值和极小值进行 3 次样条插值后得到的上下包络线，$\theta(t)$表示高频分量，通过 EMD 分解将原始信号分解为多个窄带信号 IMF 分量，得到入侵信号的包络特征为：

$$a(t)=\sqrt{x^2(t)+y^2(t)},\theta(t)=\arctan\frac{y(t)}{x(t)} \tag{6}$$

式中，$a(t)$和 $\theta(t)$分别是潜质入侵信号的解析形式的包络和

相位，其中 $a(t)$ 和 $\theta(t)$ 都是时间的函数，由于极值点时间间隔小，因此对解析信号 $z(t)$ 实行 $x(t)$ 与 $1/t$ 的经验模态分解卷积，从而有效保留了原始入侵信号 $x(t)$ 的局部时间特性。从上式可见，网络潜质入侵信号具有双向延拓特性，针对低频域产生的干扰，对相位求导即为瞬时频率实现干扰滤波，最后得到信号瞬时频率特征表达式为：

$$f(t)=\frac{1}{2\pi}\times\frac{\mathrm{d}\theta(t)}{\mathrm{d}t} \tag{7}$$

从瞬时频率的定义可以发现，按照 Hilbert 相位求每层分解的误差会逐渐累加，采用传统的傅氏变换和 Hilbert-Huang 变换时，因包络线失真引起的边界控制误差会造成频谱泄漏，因此本文需要对传统的基于 HHT 变换的入侵信号检测算法进行改进。

3 入侵检测算法改进与关键技术实现

3.1 改进思想描述与 HHT 时频谱分析

在上述构建的网络潜质入侵数学演化模型和信号模型以及入侵信号预处理的基础上，针对传统的 HHT 入侵检测出现频谱泄漏、检测性能不好的问题，本文引入递阶控制策略，针对潜质入侵信号双向延拓特性，以入侵信号端点或者极值点为对称中心进行延拓，采用一种改进型 HHT 方法进行入侵信号检测。本文提出的改进型 HHT 方法思想描述如下：对强杂波背景干扰下的潜质入侵信号 $x(t)$ 进行 EMD 分解，得到多个窄带信号 IMF 分量，表示为：

$$x_{\min,j}=\max\{x_{\min,j},x_{g,j}-\rho(x_{\max,j}-x_{\min,j})\} \tag{8}$$

$$x_{\max,j}=\min\{x_{\max,j},x_{g,j}+\rho(x_{\max,j}-x_{\min,j})\} \tag{9}$$

式中，区间 $[x_{\min,j},x_{\max,j}]$ 构成多个窄带信号 IMF 分量的滑动时间窗口 SW。ρ 为网络入侵类别特征调整系数，定义为：

$$\rho=\frac{\sum\limits_{o\in N_{k-dist}(p)}\frac{lrd_k(o)}{lrd_k(p)}}{|N_{k-dist}(p)|} \tag{10}$$

由上节分析可知，在合法信号掩盖下的网络入侵背景噪声表现为若干个高频 IMF 分量，表示为：

$$Y_k=[y_{k1},y_{k2},\cdots,y_{kj},\cdots,y_{kJ}](k=1,2,\cdots,N) \tag{11}$$

本文采用经验模态分解方法对高频分量进行滤波处理，去除虚假分量，在对网络入侵特征的 IMF 分量进行前置处理后，使用时变 ARMA 对余下低频分量进行 HHT 建模，此时将会产生 HHT 频谱偏移量，为：

$$f_i(n)=\|\ln[\lambda_i(n)]\|/2\pi\Delta t \tag{12}$$

式中，Δt 表示信号采样时间间隔。基于上述分析，本文引入递阶控制策略对偏移量频谱进行自适应修正，算法实现流程如图 1 所示。

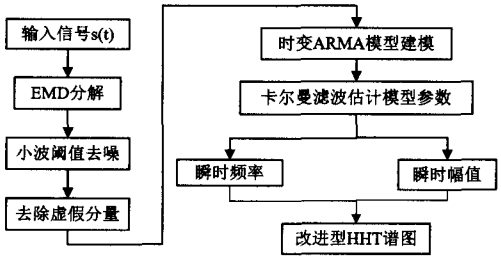


图 1 改进型 HHT 网络潜质入侵信号检测流程

从图 1 可见，整个信号检测过程中，基于对信号的模型参数估计实现 HHT 分析是检测算法实现的关键，改进型的 HHT 谱分析算法描述如下。

对每个入侵信号经验模态分解后的解析模型 IMF 分量用 Hilbert 变换进行谱分析，网络入侵信号的所有 IMF 分量的包络线的均值拟合值为 $c_i(t)$，根据经验模态分解的原理可知所得 $c_i(t)$ 可视为单分量信号，当满足固有模态函数条件的分量时，利用瞬时频率的概念将原信号 $x(t)$ 表示为：

$$x(t)=\mathrm{Re}[\sum_{i=1}^{n}a_i(t)\mathrm{e}^{j\omega_i(t)}]=\mathrm{Re}[\sum_{i=1}^{n}a_i(t)\mathrm{e}^{j\int\omega_i(t)\mathrm{d}t}] \tag{13}$$

式(13)反映了信号的幅值、时间和频率之间的关系，网络入侵信号的幅值可以表示为时间 t 和瞬时频率 ω 的函数 $H(\omega,t)$，得到具有时间-频率联合分布特征的 HHT 谱：

$$H(\omega,t)=\mathrm{Re}\sum_{i=1}^{n}a_i(t)\mathrm{e}^{j\int\omega_i(t)\mathrm{d}t} \tag{14}$$

为保证入侵信号的 HHT 谱分解后的 IMF 分量的频率调制和幅度调制偏移量减少，采用 Hough 变换对 $H(\omega,t)$ 的瞬时频率和时间进行积分，从而得到入侵信号的瞬时频率 Hilbert 边际谱：

$$h(\omega)=\int_0^T H(\omega,t)\mathrm{d}t \tag{15}$$

边际谱表达了每个频率在全局上的幅度(或能量)，代表了在统计意义上的全部累加幅度，反映了信号的幅值在整个频率段上随频率的变化情况。综上分析，得到 HHT 时频谱分析，得到信号检测模型，最后引入偏移量递阶控制律对频谱偏移进行修正，提高了检测性能。

3.2 偏移量递阶控制与检测实现

传统的 HHT 时频谱分析因包络线失真引起的边界控制误差，会造成频谱泄漏，导致检测性能较差。本文对频谱偏移采用递阶控制方法进行修正，令 H 为 Hilbert 空间，定义 $D=(d_\gamma)_{\gamma\in\Gamma}$ 为 H 中的网络入侵数据向量组成的基函数集，且 $\|d_\gamma\|=1$，其中下标 γ 表示某一基函数的递阶控制影响因子。令 V 是基函数集 D 中的向量的递阶尺度张成空间，经过“筛分”过程，采用 EMD 方法对入侵信号进行有限线性分解，信号分解过程如图 2 所示。

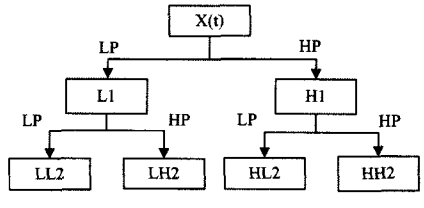


图 2 基于经验模态的信号 HHT 分解树

当且仅当 $V=H$ 时，信号 HHT 分解树集 D 是完备的，在某一个固定频率段内假设 $H=L^2(R)$，选择一定的基函数与入侵信号进行匹配，信号 f 和基 d_{γ_0} 之间的匹配程度为：

$$\lambda^n(d_{\gamma_0})=\int_{-\infty}^{+\infty}f(t)\mathrm{d}_{\gamma_0}^*(t)\mathrm{d}t \tag{16}$$

此时，采用递阶控制搜索出来的基函数即为一组极大线性无关组，$\{d_\gamma\}$ 的有限线性展开在 $L^2(R)$ 是稠密的，因此这种基函数集是完备的。采用匹配投影法寻求次优解，满足：

$$|\langle f,d_{\gamma_0}\rangle|\geqslant a\sup_{\gamma\in\Gamma}|\langle f,d_\gamma\rangle| \tag{17}$$

由 HHT 信号检测框架理论可知，如果这组完备的向量集构成 $L^2(R)$ 的一个框架，那么入侵信号就可以由若干个向量基函数的线性组合来表示，定义基函数的递阶控制指标集为：

$$\Lambda_0=\{\beta\in\Gamma:|\langle f,d_{\gamma_0}\rangle|\geqslant a\sup_{\gamma\in\Gamma}|\langle f,d_\gamma\rangle|\} \tag{18}$$

通过递阶控制调整 HHT 频谱偏移，使检测的入侵信号

特征与 f 的组成成分最佳匹配，这种展开是通过将 f 在 D 的元素上进行正交投影实现的。令 $d_{\gamma_0}\in D$，则信号 f 可被分解成：

$$f=\langle f,d_{\gamma_0}\rangle d_{\gamma_0}+R_f \tag{19}$$

式中，$\langle f,d_{\gamma_0}\rangle d_{\gamma_0}$ 是网络入侵信号 f 在 d_{γ_0} 方向上的投影，R_f 是投影后的残差信号，将残差信号投影在 D 中与 Hilbert 边际谱进行匹配，实现对 R_s 的分解，令残差初始值 $R_s^{(0)}=s$，通过 k 次分解后，对干扰进行有效过滤，且通过递阶控制实现对 HHT 谱的偏移修正，得到检测到的入侵信号：

$$R_s^{(0)}=\sum_{n=0}^{k}\langle R_s^{(n)},d_m\rangle d_m+R_s^{(k+1)} \tag{20}$$

综上分析，得到基于偏移量递阶控制的 HHT 匹配检测方法原理图，如图 3 所示。

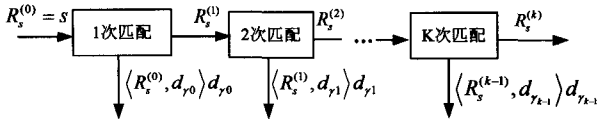


图 3　递阶控制 HHT 匹配检测原理

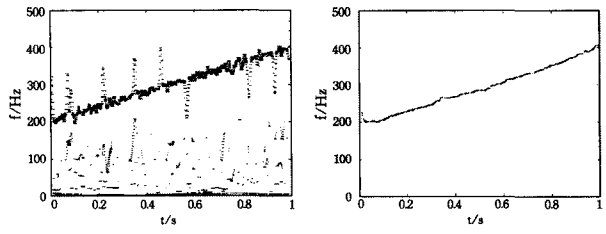
通过上述算法改进，有效抑制了包络线失真引起的边界控制误差，避免了频谱泄漏，从而提高了对入侵信号的检测性能。

4　仿真实验与结果分析

为了验证本文提出的引入 HHT 谱偏移量递阶控制的网络入侵信号检测算法的性能，基于 Matlab 仿真实验平台，对网络入侵信号进行检测实验。仿真实验样本数据来自于 MIT 林肯实验室的 DAPRPA 入侵检测数据集，分别在 ipsweep 和 smurf 等两种入侵行为下进行两组实验，来测试算法对低信噪比环境下的入侵信号的检测能力。实验样本参数选择中，设定合法网络信息样本数为 1024，访问次数为 10256 次，入侵信号样本数为 238，采用本文改进算法和传统的 HHT 检测算法，在相同条件下对入侵信号进行检测仿真和性能对比。首先对入侵信号进行色噪声滤波，通过滤波能有效避免显性干扰成分，滤波器设置为：

$$H(z)=\frac{z^{-2}}{1-a_1z^{-1}+a_2z^{-2}} \tag{21}$$

式中，$a_1=2\mu\cos(2\pi f_0/f_s)$，$a_2=\mu^2$，$\mu=0.87$。基于 Hilbert 变换，使入侵信号离散数据解析化，构建入侵信号解析模型，得到输入的入侵信号，以 ipsweep 入侵信号类型为例分析入侵检测性能，入侵信号的中心频率测试为 $f_0=1000$Hz，离散采样率为 $f_s=10*f_0$Hz$=10$kHz，带宽 $B=1000$Hz，采样点 $N=201$，其中 $T=N/f_s$，调频率 $k=B/T$，首先选取信噪比为 3dB，分别使用原始 HHT 方法和本文提出的改进型 HHT 方法，画出两种方法下得到的入侵信号的时频分布谱，如图 4 所示。

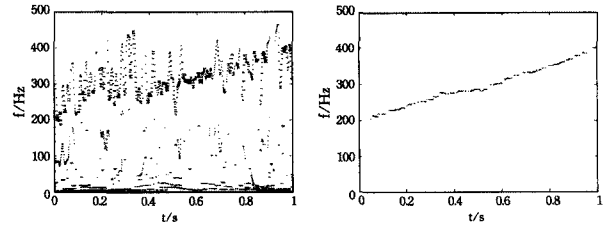


(a)原始 HHT 方法谱图　　(b)改进型 HHT 方法谱图

图 4　ipsweep 入侵信号 HHT 谱检测结果对比(SNR=3dB)

从图 4 结果分析可见，相比于原始 HHT 方法，改进型 HHT 方法提高了时频分布谱在噪声中的分辨率，并显著提高了抗噪声影响的能力，网络入侵信号频率随时间变化的特性较为清晰。可以看出无论是原始 HHT 方法或改进型 HHT 方法在求得 ipsweep 信号的初始频率和截止频率时因噪声存在产生了一定程度误差，原始 HHT 方法在起始频率得到了小于 200Hz 的估计值，而在截止频率处却获得了大于 40Hz 的估计值；相比于原始 HHT 方法，改进型 HHT 方法在起始频率和截止频率处只产生了相对较小的误差，也说明改进型 HHT 方法比原始 HHT 方法能更为有效地检测 ipsweep 入侵信号的参数。

对合法网络信息信号进行合理调节设置，在信噪比为 −3dB 下做检测实验，比较原始 HHT 方法和改进型 HHT 方法效果，得到 SNR=−3dB 条件下 HHT 谱检测结果对比，如图 5 所示。



(a)原始 HHT 方法谱图　　(b)改进型 HHT 方法谱图

图 5　ipsweep 入侵信号 HHT 谱检测结果对比(SNR=−3dB)

分析图 5 结果可见，由于信噪比降低，传统 HHT 方法的性能下降较为严重，原本在正信噪比 3dB 时较为集中的谱图在负信噪比下已经发生严重分散，难以分辨其频率随时间变化的特性，而且存在着低频部分的干扰；在改进型 HHT 方法中，谱图的分辨率依然较好，相比于原始 HHT 方法，改进型方法能较为清晰地展示出入侵信号的时频特性，检测性能较好。

以上都是单次实验的结果，下面通过 1000 次 Monte Carlo 实验，分别使用原始 HHT 方法和改进型 HHT 方法进行检测性能曲线绘制，得到检测性能曲线，如图 6 所示。分析得到改进型 HHT 方法在 −3dB 时检测概率在 50% 以上，而原始 HHT 方法仅为 15%；在 0dB 时改进型方法检测概率为 80%，而原始方法仅为 30%，证明本文算法在强干扰的信噪比下的网络入侵检测性能具有优越性。同理，对 smurf 入侵信号的检测也有类似结论。分析原因，在于本文方法采用 HHT 谱偏移量递阶控制策略，抑制了包络线失真引起的边界控制误差，避免了频谱泄漏，从而提高了检测性能。

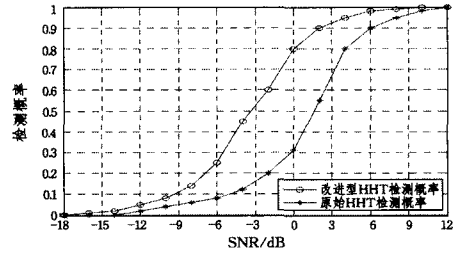


图 6　检测性能曲线对比

结束语　本文研究了强干扰背景低信噪比下对网络潜质入侵信号的准确检测问题，针对传统的 HHT 检测算法在求解入侵信号的瞬时频率特征时出现频谱泄漏，本文提出一种基于 HHT 谱偏移量递阶控制的网络入侵信号检测算法。首

先构建网络潜质入侵数学演化模型，采用经验模态分解方法对高频分量进行滤波处理，去除虚假分量，通过递阶控制调整HHT频谱偏移，使检测的入侵信号特征的组成成分形成最佳匹配，采用HHT谱偏移量递阶控制策略，抑制了包络线失真引起的边界控制误差，抑制了频谱泄漏，提高了检测性能。研究结果表明，改进的HHT检测算法能有效检测出信噪比极低背景下的信号特征，对诸如ipsweep和smurf等干扰性极强的潜在入侵信号具有较好的检测效果，检测性能较传统方法提高显著。研究成果在网络安全防御和对抗等领域具有较好的应用价值。

参 考 文 献

[1] 孙言强，王晓东，周兴铭. 无线网络中的干扰攻击[J]. 软件学报，2012，23(5)：1207-1221

[2] 周华，周海军，马建锋. 基于博弈论的入侵容忍系统安全性分析模型[J]. 电子与信息学报，2013，35(8)：1933-1939

[3] 梁力. 一种网络多次变异信息入侵检测算法[J]. 科技通报，2012，10(28)：55-57

[4] Bimal K M，Gholam M A. Differential epidemic model of virus and worms in computer network [J]. International Journal of Network Security，2012，14(3)：149-155

[5] 樊爱宛，时合生. 基于特征选择和SVM参数同步优化的网络入侵检测[J]. 北京交通大学学报，2013，37(5)：58-61

[6] Li Hong，Qian Chang-ji，Sun Li-zhen，et al. Simulation of a flexible polymer tethered to a flat adsorbing surface [J]. Journal of Applied Polymer Science，2012，124：282-287

[7] 罗柏文，沈彩耀，于宏毅. 采用余弦调制滤波器组的多径衰落信号子带合成[J]. 信号处理，2013，29(5)：537-543

[8] 葛海慧，肖达，陈天平，等. 基于动态关联分析的网络安全风险评估方法[J]. 电子与信息学报，2013，35(11)：2630-2636

[9] 张宗飞. 基于量子进化算法的网络入侵检测特征选择[J]. 计算机应用，2013，33(5)：1357-1361

[10] Zhu Q Y，Yang X F，Yang L X，et al. Optimal control of computer virus under a delayed model [J]. Applied Mathematics and Computation，2012，218(23)：11613-11619

[11] 张辉. 自体集网络入侵检测中的高效寻优算法仿真[J]. 计算机仿真，2013，30(8)：297-300

[12] 林冬茂，薛德黔. 一种基于无监督免疫优化分层的网络入侵检测算法[J]. 计算机科学，2013，40(3)：180-182

[13] 叶竞，石锐，何庆华. 基于HHT和改进CSP算法的运动想象BCI系统[J]. 重庆理工大学学报：自然科学版，2012，26(5)：70-73

(上接第106页)

结束语 本文提出了一种基于无证书公钥密码体制的非交互密钥交换协议，给出了这类协议的定义并刻画了协议的安全模型，然后给出了一种利用双线性对的无证书非交互密钥交换协议的构造方案，而且还在随机预言模型下基于BDH困难问题给出了该方案的安全性证明。该方案解决了基于身份的非交互密钥交换协议中的密钥托管问题。另外，该协议可以抵抗无证书公钥密码体制中的两类敌手的攻击，允许部分秘密信息泄露，因此其比现有的非交互密钥交换协议具有更高的安全性。

参 考 文 献

[1] Dodis Y，Katz J，Smith A，et al. Composability and on-line deniability of authentication[M]// Theory of Cryptography. Berlin，Springer Berlin Heidelberg，2009：146-162

[2] Boyd C，Mao W，Paterson K G. Key agreement using statically keyed authenticators[C]// Second International Conference，ACNS 2004，Yellow Mountain，China，2004：248-262

[3] Jakobsson M，Sako K，Impagliazzo R. Designated verifier proofs and their applications [C] // International Conference on the Theory and Application of Cryptographic Techniques. Saragossa，1996：143-154

[4] Diffie W，Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory，1976，22(6)：644-654

[5] Bernstein D J. Curve25519：new Diffie-Hellman speed records [C]// 9th International Conference on Theory and Practice in Public-Key Cryptography. New York，2006：207-228

[6] Cash D，Kiltz E，Shoup V. The twin Diffie-Hellman problem and applications[M]// Advances in cryptology-EUROCRYPT 2008. Berlin，Springer Berlin Heidelberg，2008：127-145

[7] Freire E S V，Hofheinz D，Kiltz E，et al. Non-interactive key exchange [M] // Public-Key Cryptography-PKC 2013. Berlin，Springer Berlin Heidelberg，2013：254-271

[8] Boneh D，Zhandry M. Multiparty key exchange，efficient traitor tracing，and more from indistinguishability obfuscation [R]. Cryptology ePrint Archive，Report 2013/642，2013

[9] Maurer U M，Yacobi Y. Non-interactive public-key cryptography[M]// Advances in Cryptology-EUROCRYPT'91. Berlin，Springer Berlin Heidelberg，1991：498-507

[10] Lim C H，Lee P J. Modified Maurer-Yacobi's scheme and its applications[M]// Advances in Cryptology-AUSCRYPT'92. Berlin，Springer Berlin Heidelberg，1993：308-323

[11] Maurer U M，Yacobi Y. A non-interactive public-key distribution system[J]. Designs，Codes and Cryptography，1996，9(3)：305-316

[12] Maurer M，Kügler D. A note on the weakness of the Maurer-Yacobi squaring method [R]. Technical report，TI 15/99，TU Darmstadt，1999

[13] Sakai R，Ohgishi K，Kasahara M. Cryptosystems based on pairings[C]// The 2000 Symposium on Cryptography and Information Security. Okinawa，2000：26-28

[14] Dupont R，Enge A. Provably secure non-interactive key distribution based on pairings[J]. Discrete Applied Mathematics，2006，154(2)：270-276

[15] Paterson K G，Srinivasan S. On the relations between non-interactive key distribution，identity-based encryption and trapdoor discrete log groups[J]. Designs，Codes and Cryptography，2009，52(2)：219-241

[16] Freire E S V，Hofheinz D，Paterson K G，et al. Programmable Hash Functions in the Multilinear Setting? [M]// Advances in Cryptology-CRYPTO 2013. Berlin，Springer Berlin Heidelberg，2013：513-530

[17] Steinwandt R，Corona A S. Identity-based non-interactive key distribution with forward security[J]. Designs，Codes and Cryptography，2012，64(1/2)：195-208

[18] Lin X J，Ren Ran，Wei Z G，et al. Comment on "Identity-based non-interactive key distribution with forward security"[J]. Designs，Codes and Cryptography，2013：1-7

[19] Wu T S，Lin H Y. Non-Interactive Authenticated Key Agreement over the Mobile Communication Network[J]. Mobile Networks and Applications，2013，18：594-599