文章编号：2095-2163(2019)02-0155-05 中图分类号：TP393 文献标志码：A

基于码元包络幅值提取的网络入侵检测算法

张创基
(广州华立科技职业学院，广州 511325)

摘 要：为了提高无线网络对移动终端高级持续性入侵检测的准确性，提出基于码元包络幅值提取的无线传感网络移动终端高级持续性入侵数据检测算法。构建无线传感网络的码元传输信道分布模型，提取无线传感网络传输流量序列的码元包络幅值特征量，根据码元包络幅值特征提取结果进行融合聚类处理，采用大数据信息融合和关联规则挖掘方法进行无线传感网络移动终端高级持续性入侵检测。仿真结果表明，采用该方法进行无线传感网络移动终端高级持续性入侵检测的准确性较高，抗干扰性较好，提高了网络的安全性。

关键词：码元；包络幅值；特征提取；网络入侵；检测

Network intrusion detection algorithm for extracting envelope amplitude of primitive symbols

ZHANG Chuangji
(Guangzhou Huali Science and Technology Vocational College, Guangzhou 511325, China)

【Abstract】 In order to improve the accuracy of wireless network for mobile terminal advanced persistent intrusion detection, a network intrusion detection algorithm based on symbol envelope amplitude extraction is proposed. An advanced persistent intrusion detection algorithm for mobile terminals in wireless sensor networks based on symbol envelope amplitude extraction is proposed. The symbol transmission channel distribution model of wireless sensor network is constructed, the symbol envelope amplitude characteristic quantity of wireless sensor network transmission symbol is extracted, and the fusion clustering processing is carried out according to the result of symbol envelope amplitude feature extraction. Big data information fusion and association rule mining methods are used to detect advanced persistent intrusion of wireless sensor network mobile terminal. The simulation results show that the proposed method has high accuracy and good anti-interference, and improves the security of the wireless sensor network.

【Key words】 symbol; envelope amplitude; feature extraction; network intrusion; detection

0 引 言

随着无线传感网络通信技术的发展，无线传感网络的安全性受到人们的极大关注，无线传感网络作为物联网和无线通信的主要通信方式，承载了大量的用户信息，通过无线传感网络进行大数据信息采样和传输，能提高对信息的自适应收发控制和网络组网能力[1]。在采用无线传感组网进行码元通信过程中，受到网络入侵和病毒植入的影响，在移动终端出现码元输出失真，需要进行无线网络的移动终端高级持续性入侵检测设计，提高网络的安全性[2]。

针对无线传感网络容易遭到移动终端高级持续性入侵的问题，进行无线传感网络移动终端高级持续性入侵检测算法的优化设计，提高网络安全性，提出基于码元包络幅值提取的无线传感网络移动终端高级持续性入侵数据检测算法[3]。首先构建无线传感网络的码元传输信道分布模型，然后进行入侵码元的大数据挖掘和包络幅值特征提取，实现入侵检测，最后进行仿真测试分析，得出有效性结论。

1 入侵码元模型构建与码元传输信道分布

1.1 移动终端高级持续性入侵码元模型构建

为了实现对无线传感器网络的移动终端高级持续性入侵码元的检测，首先需要进行网络攻击节点分布式传感组网设计和网络入侵的码元信道传输模型设计，结合入侵的干扰节点部署和入侵码元的幅值特征提取方法，进行包络滤波和特征提取，提高对网络入侵码元的检测和识别能力[4-6]。采用多传感信号跟踪识别和大数据关联规则挖掘方法，实现移动终端高级持续性入侵码元的模型构建[7]，根据上述分析，得到本文设计的无线网络移动终端入侵节点分布模型如图 1 所示。

在图 1 所示的无线网络移动终端入侵节点分布模型中，采用一个无向图模型 $G=(V,E)$ 表示入侵码元传输链路模型，其中节点 v 为移动终端的输出

作者简介：张创基(1983-)，男，硕士，讲师、网络工程师，主要研究方向：信息与网络安全、计算机控制、数据挖掘。

收稿日期：2018-12-20

链路层中任一节点、即 $v \in V$；入侵码元在移动终端分布节点的 Sink 链路集为 e，网络中任一连边、即 $e \in E$，假设分布式拓扑环境下无线传感网络传输链路的数据集 $X = \{x_1, x_2, \cdots, x_n\}$，构建移动终端高级持续性入侵环境下无线传感网络数据的采集模型[8]，设网络码元传输的有向图模型 $G(A)$、$G(B)$ 中，移动终端高级持续性入侵环境下无线传感网络数据分布特征点 $< x, y >$ 为 A、B 的一对锚点，无线传感网络数据分布的有向图的边 $(u, v) \in E$，构建无线传感网络移动终端高级持续性入侵大数据采样信道模型为：

$$X_1(k) = FFT\,[x_1(k), x_1(k+1), \cdots x_1(k+N-1)]^{\mathrm{T}}, \quad (1)$$

$$X_2(k) = FFT\,[x_2(k), x_2(k+1), \cdots, x_2(k+N-1)]^{\mathrm{T}}, \quad (2)$$

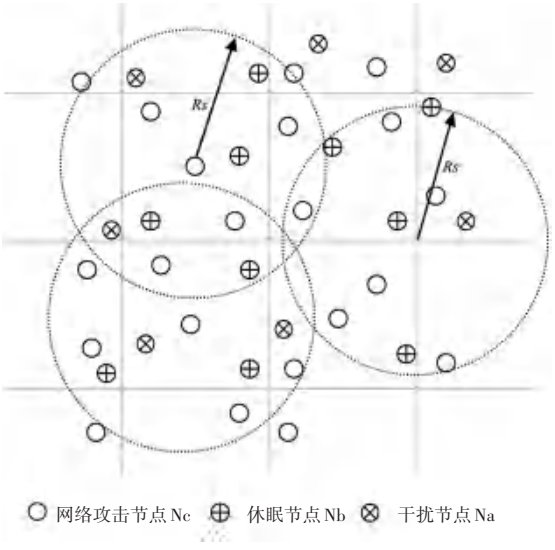

图 1 无线网络移动终端入侵节点分布模型

Fig. 1 Wireless network mobile terminal intrusion node distribution model

其中，$\tilde{X}_1(k)$，$\tilde{X}_2(k)$ 分别是 $X_1(k)$，$X_2(k)$ 前 $N/2+1$ 项组成的移动终端高级持续性入侵特征分布序列，由此提取无线传感网络传输码元的关联规则集[9]，用 N 维矢量 $\boldsymbol{x}(t)$ 表示无线传感网络移动终端高级持续性入侵数据的矢量，则：

$$\boldsymbol{x}(t) = \boldsymbol{A}\boldsymbol{s}(t) + \boldsymbol{n}(t), \quad (3)$$

其中，

$$\boldsymbol{x}(t) = [x_{-P+1}(t), x_{-P+2}(t), \cdots, x_P(t)]^{\mathrm{T}}_{N\times 1}; \quad (4)$$

$$\boldsymbol{s}(t) = [s_1(t), s_2(t), \cdots, s_I(t)]^{\mathrm{T}}_{I\times 1}; \quad (5)$$

$$\boldsymbol{n}(t) = [n_{-P+1}(t), n_{-P+2}(t), \cdots, n_P(t)]^{\mathrm{T}}_{N\times 1}; \quad (6)$$

$$\boldsymbol{A} = [a(\theta_1, r_1), a(\theta_2, r_2), \cdots, a(\theta_I, r_I)]_{N\times I}. \quad (7)$$

根据上述分析，构建无线传感网络的码元传输信道分布模型，提取无线传感网络传输流量序列的码元包络幅值特征量，结合关联规则挖掘方法进行网络入侵检测设计[10]。

1.2 网络入侵特征提取

在无线传感网络的传输信道中进行网络流量采集，构建网络入侵的传输信道模型，结合异常特征提取方法实现网络入侵检测[11]，采用高阶统计量描述无线传感网络的链路层中持续性攻击的入侵特征信息：

$$C_1(m,n) = \sum_{i=1}^{L} c_{4s_i} e^{\mathrm{j}2\phi_i(m-n)}, \quad (8)$$

其中，$c_{4s_i} = cum\{|s_i(t)|^4\}$ 表示无线传感网络中移动终端高级持续性入侵数据在节点 s_i 处的能量谱密度。用 C_{4S} 表示汇聚链路层中移动终端高级持续性入侵数据的强度：

$$\boldsymbol{C}_{4S} = diag[c_{4s_1}, c_{4s_2}, \cdots, c_{4s_L}], \quad (9)$$

已知 $a(t) \geqslant |s(t)|$，表示 $a(t)$ 在最小均方误差原则下的入侵包络幅值，最大包络幅值为 $|s(t)|$，选取曲率为 $a(t)$ 的曲线，构造如下的 $4P \times 4P$ 矩阵表示高级持续性入侵码元包络幅值特征量：

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_1 & \boldsymbol{C}_2 & \boldsymbol{C}_5 & \boldsymbol{C}_4 \\ \boldsymbol{C}_2^{\mathrm{H}} & \boldsymbol{C}_1 & \boldsymbol{C}_6 & \boldsymbol{C}_7 \\ \boldsymbol{C}_5^{\mathrm{H}} & \boldsymbol{C}_6^{\mathrm{H}} & \boldsymbol{C}_1 & \boldsymbol{C}_3^{\mathrm{H}} \\ \boldsymbol{C}_4^{\mathrm{H}} & \boldsymbol{C}_7^{\mathrm{H}} & \boldsymbol{C}_3 & \boldsymbol{C}_1 \end{bmatrix} = \bar{\boldsymbol{A}}\boldsymbol{C}_{4s}\bar{\boldsymbol{A}}^{\mathrm{H}}, \quad (10)$$

其中，$\bar{\boldsymbol{A}} = [\boldsymbol{A}^{\mathrm{H}}, (\boldsymbol{A}\Lambda)^{\mathrm{H}}, (\boldsymbol{A}\Omega)^{\mathrm{H}}, (\boldsymbol{A}\Phi)^{\mathrm{H}}]^{\mathrm{H}}$，表示无线传感网络移动终端高级持续性入侵数据的残余统计量[12]，由此得到网络移动终端高级持续性入侵数据的特征分解模型：

$$\boldsymbol{C} = \boldsymbol{E}\sum\boldsymbol{E}^{\mathrm{H}}, \quad (11)$$

其中，$\boldsymbol{E} = [e_1, e_2, \cdots, e_{4P}]$ 为无线传感网络移动终端高级持续性入侵码元传输链路 (a, b_m) 上的酉矩阵；$\sum = diag[\sigma_1, \sigma_2, \cdots, \sigma_{4P}]$ 为无线传感网络移动终端高级持续性入侵数据的异常码元包络幅值特征值组成的对角矩阵，且满足：

$$\sigma_1 > \cdots \sigma_L > \sigma_{L+1} = \cdots \sigma_{4P} = 0, \quad (12)$$

由此得到无线传感网络移动终端高级持续性入侵大数据的异常码元包络幅值特征提取为：

$$f_{s,\tau}(t) = [U(1/s, \tau)f(t)] = \sqrt{|s|}f(s(t-\tau)). \quad (13)$$

在整个时频平面内进行变量代换 $a = 1/s$，$b = \tau$，以此作为模板去拟合码元包络上升沿，实现对网络入侵的特征提取。

2 入侵检测算法优化设计

2.1 码元包络幅值检测

在构建无线传感网络的码元传输信道分布模型

和进行特征提取的基础上，进行网络入侵检测算法改进设计，本文提出一种基于码元包络幅值提取的无线传感网络移动终端高级持续性入侵数据检测算法[13]。在分布式的组网环境下，采用向量量化分解方法进行移动终端高级持续性入侵码元的融合性特征分析，令码元检测的自适应权值 $\hat{w}(0)=0$，对持续性入侵检测的滤波迭代公式为：

$$\theta_1(k+1)=\theta_1(k)-\mu\mathrm{Re}[y(k)\varphi^*(k)], \quad (14)$$

其中，μ 是不同码元包络的上升区域的时间线性控制参数，称为步长；$\varphi(k)$ 是入侵码元的输出期望响应，对不同的辐射源的入侵码元进行包络幅值检测，对输入的持续性攻击入侵特征 $u(k)$ 按最小均方误差准则进行线性变换处理[14]，表示为：

$$H_B(z)=\frac{(1+\sin\theta_2)}{\cos\theta_2}\cdot\frac{\cos\theta_1(k)\cos\theta_2 z^{-1}}{1+\sin\theta_1(k)(1+\sin\theta_2)z^{-1}+\sin\theta_2 z^{-2}}G(z), \quad (15)$$

其中，

$$G(z)=\frac{1-\sin\theta_2}{2}\cdot\frac{1-z^{-2}}{1+\sin\theta_1(k)(1+\sin\theta_2)z^{-1}+\sin\theta_2 z^{-2}}, \quad (16)$$

输入的移动终端高级持续性入侵码元的信号 $u(k)$ 经过自适应 IIR 处理，使得输出信号与期望响应之间的误差最小，令 $d(k)$ 代表高级持续性入侵检测的特征分量，得到码元包络幅值检测的误差分量为：

$$\varepsilon(k)=d(k)-y(k)=d(k)-\sum_{i=1}^{M}W_i x(k-i). \quad (17)$$

对式(17)两边取数学期望，采用码元包络幅值提取算法进行无线传感网络移动终端高级持续性入侵检测，实现对网络入侵的码元融合和抗干扰滤波处理，提高了入侵检测的抗干扰能力[15]。

2.2　无线传感网络移动终端高级持续性入侵检测

计算出移动终端高级持续性入侵码元的矩形包络，得到双线性变换后的移动终端高级持续性入侵码元形式为：

$$s(t)=\sum_{k=1}^{N}p_k\sin(\omega_k n+\Phi_k)+\zeta(n), \quad (18)$$

其中，Φ_k 为窄带高斯噪声；$\zeta(n)$ 为单个矩形脉冲；p_k 为尺度参数，对不同辐射源的信号包络特征进行关联规则挖掘，得到特征估计式为：

$$\frac{1}{2\pi m}\sum_{k=-q/2}^{q/2}b_k\phi(n+c_k m)=\hat{f}_{i_q}(n), \quad (19)$$

其中，b_k 为绝对相位，ϕ 为相位角；m 为期望的响应；c_k 为码元包络信息的互信息量。如果 $x_1(t)$ 和 $x_2(t)$ 表示无线传感网络中两组移动终端高级持续性入侵检测的特征分量，则有：

$$x_1(t)=-\sum_{k=1}^{p_1}a_{1k}x_1(t-k)+\varepsilon_1(t), \quad (20)$$

$$x_2(t)=-\sum_{k=1}^{p_2}a_{2k}x_2(t-k)+\varepsilon_2(t), \quad (21)$$

其中，$\varepsilon_1(t)$ 表示方差为 ${\sigma_1}^2$ 的高斯白噪声，得到输出网络入侵包络形式为：

$$u(t)=\frac{1}{\sqrt{T}}rect(\frac{t}{T})\exp\{-\mathrm{j}[2\pi K\ln(1-\frac{t}{t_0})]\}. \quad (22)$$

其中，$rect(t)=1$，$|t|\leqslant 1/2$。对无线传感网络移动终端高级持续性入侵进行包络特征检测，提高入侵检测的频域聚焦能力[16]，移动终端高级持续性入侵码元的时移不变特征量表达式为：

$$\begin{cases}y(t)=x(t-t_0)\Rightarrow W_y(t,v)=W_x(t-t_0,v),\\ y(t)=x(t)e^{\mathrm{j}2\pi v_0 t}\Rightarrow W_y(t,v)=W_x(t,v-v_0).\end{cases} \quad (23)$$

用时间平移关系描述网络入侵检测的特征变换，描述为：

$$W_u u(a,b)=e^{\mathrm{j}2\pi K\ln a}\times\frac{K}{\sqrt{a}}\left\{\left[ae^{\frac{\mathrm{j}2\pi f_{\min}}{a}(b-b_a)}-\frac{e^{\mathrm{j}2\pi f_{\max}(b-b_a)}}{f_{\min}}\right]+\mathrm{j}2\pi(b-b_a)\left[Ei(\mathrm{j}2\pi f_{\max}(b-b_a))-Ei\left(\frac{\mathrm{j}2\pi f_{\min}}{a}(b-b_a)\right)\right]\right\}, \quad (24)$$

其中，$b_a=(1-a)(\frac{1}{af_{\max}}-\frac{T}{2})$，$Ei(\cdot)$ 表示码元包络幅值提取的尺度平移，对于尺度为 a 的网络入侵信号进行包络特征提取，以 t/a 代替 t 根据码元包络幅值特征提取结果进行融合聚类处理，采用大数据信息融合和关联规则挖掘方法进行无线传感网络移动终端高级持续性入侵检测，入侵检测输出为：

$$\begin{cases}H_0:\tilde{x}(t)=\tilde{w}(t),\\ H_1:\tilde{x}(t)=\sqrt{E_t}\tilde{f}(t-\lambda)\tilde{b}_D(t-\frac{\lambda}{2})+\tilde{w}(t).\end{cases} \quad 0\leqslant t\leqslant T \quad (25)$$

其中，$\tilde{w}(t)$ 为每个信源的参数自动配对参数，综上分析，实现对移动终端高级持续性入侵检测。

3　仿真试验测试

为了测试文本方法在实现无线传感网络移动终

端高级持续性入侵数据检测中的应用性能,进行仿真实验,实验中算法设计采用 Matlab 设计,网络移动终端高级持续性入侵数据类型为 DoS、Probe 和 ipsweep 三种类型,每类网络移动终端高级持续性入侵数据的特征样本数包括 2 000 组测试样本,数据的长度为 1 024,对入侵码元的离散采样率为 f_s = 10 * f_0 Hz = 10 KHz,码元包络幅值检测的自适应步长参数 μ = 0.000 2,干扰为 $n(k) = n_r(k) + jn_i(k)$,信噪比为-12 dB,在上述仿真环境和参数设定情况下,进行无线传感网络移动终端高级持续性入侵检测,得到入侵数据样本和检测输出如图 2 所示。

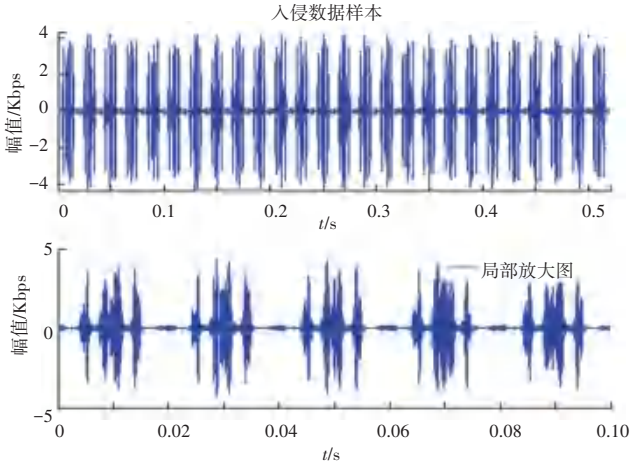

图 2 无线传感网络的持续性入侵检测输出

Fig. 2 Persistent intrusion detection output for wireless sensor network

分析图 2 得知,采用本文方法进行无线传感网络移动终端高级持续性入侵检测,能准确定位入侵码元的频域点,入侵检测的准确性较高。对网络入侵的码元包络幅值检测结果如图 3 所示。

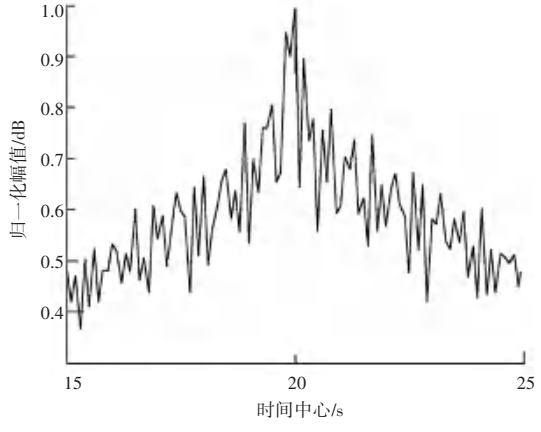

图 3 码元包络幅值提取结果

Fig. 3 Symbol envelope amplitude extraction result

分析图 3 得知,本文方法能准确检测无线传感网络移动终端高级持续性入侵信息的码元包络信息,测试不同方法进行网络入侵检测的准确性,采用 1 000 次Monte Carlo 实验,得到对比结果如图 4 所示,分析图 4 得知,本文方法进行入侵检测的准确性较高。

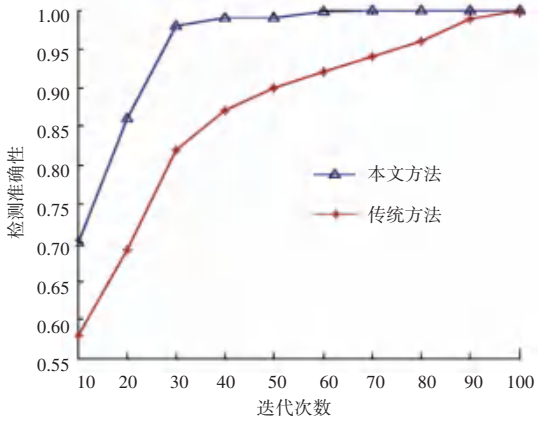

图 4 入侵检测性能对比

Fig. 4 Intrusion detection performance comparison

4 结束语

在采用无线传感器组网进行码元通信过程中,受到网络入侵和病毒植入的影响,需要进行无线网络的移动终端高级持续性入侵检测设计,本文提出基于码元包络幅值提取的无线传感网络移动终端高级持续性入侵检测算法。采用高阶统计量描述无线传感网络的链路层中持续性攻击的入侵特征,采用向量量化分解方法进行移动终端高级持续性入侵码元的融合性特征分析,对不同的辐射源的入侵码元进行包络幅值检测,实现入侵检测算法优化设计,并通过仿真实验实现性能分析,本文方法进行入侵检测的码元包络幅值定位性能较好,在网络入侵检测和网络安全设计中具有很好的应用前景。

参考文献

[1] 陈虹,万广雪,肖振久. 基于优化数据处理的深度信念网络模型的入侵检测方法[J]. 计算机应用,2017,37(6):1636-1643,1656.

[2] 胡彬,王春东,胡思琦,等. 基于机器学习的移动终端高级持续性威胁检测技术研究[J]. 计算机工程, 2017, 43(1): 241-246.

[3] 高妮,贺毅岳,高岭. 海量数据环境下用于入侵检测的深度学习方法[J]. 计算机应用研究,2018,35(4):1197-1200.

[4] 谷琼, 袁磊, 宁彬, 等. 一种基于混合重取样策略的非均衡数据集分类算法[J]. 计算机工程与科学, 2012, 34(10):128-134.

[5] 陈西宏,胡茂凯,孙际哲,等. 多径衰落信道下多音干扰 OFDM 系统性能分析[J]. 北京理工大学学报,2014,34(1):83-87.

[6] 任维武,张波辰,底晓强,等. 基于人工蜂群优化的密度聚类异常入侵检测算法[J]. 吉林大学学报(理学版),2018,56(1):95-100.

(下转第 161 页)