# 基于安全态势监测模型的泛在终端种类攻击自动识别研究

韩世海[1] 徐 鑫[2] 朱 珠[1]

[1](国网重庆市电力公司电力科学研究院 重庆 401123)

[2](重庆大学 重庆 400044)

**摘 要** 以提升泛在终端种类攻击自动识别精度为目的,研究基于安全态势监测模型的泛在终端种类攻击自动识别方法。对初始数据序列实施等时距处理,依照累加数列所表现出的反"S"形摆动特征,通过灰色 Verhulst 模型确定泛在终端风险值。将支持向量机的参数与分类精度分别作为改进粒子群算法的粒子和目标函数,通过全局搜索过程确定支持向量机的最优参数,构建多分类识别模型,将泛在终端风险值作为输入,利用识别模型自动识别泛在终端攻击类型。实验分析结果显示该方法攻击类型查准率为 97.81%,DCP 值最高达到 0.006 3%。

**关键词** 安全态势 泛在终端 种类攻击 自动识别 等时距处理

**中图分类号** TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.04.048

# AUTOMATIC IDENTIFICATION OF UBIQUITOUS TERMINAL TYPE ATTACKS BASED ON SECURITY SITUATION MONITORING MODEL

Han Shihai[1] Xu Xin[2] Zhu Zhu[1]

[1](*Electric Power Research Institute, State Grid Chongqing Electric Power Company, Chongqing 401123, China*)

[2](*Chongqing University, Chongqing 400044, China*)

**Abstract** In order to improve the accuracy of automatic identification of ubiquitous terminal type attack, the automatic identification method of ubiquitous terminal type attack based on security situation monitoring model is studied. The initial data sequence was treated with equal time interval. According to the anti-s-shaped swing characteristics of the cumulative sequence, the risk value of the ubiquitous terminal was determined by the grey Verhulst model. The parameters and classification accuracy of support vector machine were regarded as the particle and objective functions of the improved particle swarm optimization respectively. The optimal parameters of support vector machine were determined through the global search process, and the multi-classification recognition model was constructed. The ubiquitous terminal risk value was taken as the input, and the identification model was used to automatically identify the attack types of ubiquitous terminal. The experimental results show that the precision of attack type is 97.81%, and the highest DCP value is 0.006 3%.

**Keywords** Security situation Ubiquitous terminal Type attack Automatic recognition Equal time interval processing

## 0 引 言

当前大量实际案例显示,针对信息基础设施的攻击中有大部分是由现场终端作为初始点,通过逐渐渗透实现最终破坏的[1]。由于泛在终端的种类攻击较为复杂,同时由于泛在终端的防护措施受外在环境与自身条件限制无法做到完美防护[2],因此对泛在终端层面的行为感知与安全检测尤为重要,而泛在终端种类攻击自动识别则是泛在终端安全防护的基础[3]。

收稿日期:2020-11-16。国网重庆市电力公司科技项目(2020 渝电科技 11#)。**韩世海**,工程师,主研领域:网络安全技术,漏洞挖掘,攻防技术。**徐鑫**,高工。**朱珠**,工程师。

普遍使用的泛在终端种类攻击自动识别方法为基于生物免疫学的方法和基于知识图谱的方法[4-5]，但前者在识别过程中的能耗较大，而后者的识别精度受样本数据影响显著。为改善此类问题，研究基于安全态势监测模型的泛在终端种类攻击自动识别方法，提升泛在终端种类攻击识别精度。

# 1 方法设计

## 1.1 安全态势监测模型构建

### 1.1.1 非等时距数列的等时距处理方法

用 $L^{(0)}=\{l^{(0)}(t_k),k=1,2,\cdots,n\}$ 表示泛在终端的初始数据序列，其中 $t_k$ 表示时序，且 $t_{k+1}-t_k>0$。因 $t_k$ 具有非等间距特性[6]，用 $D$ 表示 $t_{k+1}-t_k$ 的最小值。此时，可通过最小二乘法获取泛在终端初始数据的等时序 $t'_k$，其表达式如下：

$$t'_k=h_0+h_1\cdot k \tag{1}$$

基于式(1)构建方程组：

$$\boldsymbol{T}'=\boldsymbol{AH} \tag{2}$$

式中：$\boldsymbol{A}^{\mathrm{T}}=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & 2 & \cdots & n\end{bmatrix}$，$\boldsymbol{H}=\begin{bmatrix}h_0\\ h_1\end{bmatrix}$。设定 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{AH}-\boldsymbol{A}^{\mathrm{T}}\boldsymbol{T}=0$，由此能够反推出：

$$\boldsymbol{H}=(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{T} \tag{3}$$

根据式(3)，利用式(1)能够确定 $\boldsymbol{T}'$，结合 Langrange 插值法获取等时距数列 $L^{(0)}(\boldsymbol{T}')$。

### 1.1.2 构建非等时距 Verhulst 模型

利用上述过程处理泛在终端初始数据序列后即可获取其等时距数列，在此基础上选取 Verhulst 模型构建泛在终端安全态势监测模型。用 $L^{(0)}=\{l^{(0)}(t)\mid t=1,2,\cdots,n\}$ 表示等时距处理后的初始序列，对其进行一次累加处理，获取数列 $L^{(1)}=\{l^{(1)}(t)\mid t=1,2,\cdots,n\}$，其中 $l^{(1)}(t)=\sum_{i=1}^{k}l^{(0)}(i),t=1,2,\cdots,n$。设定 $l^{(1)}(1)=l^{(0)}(1)$，由此，可通过 Verhulst 一阶白化非线性微分方程拟合 $L^{(1)}(t)$：

$$\frac{\mathrm{d}L^{(1)}(t)}{D}=rL^{(1)}(t)-b(L^{(1)}(t))^2 \tag{4}$$

式中：$r$ 和 $b$ 分别表示以大小与符号描述 $L^{(0)}$ 与 $L^{(1)}$ 发展态势的发展系数和表示系统作用量的系统输入值。其中 $b$ 值包含灰信息覆盖的作用量，无法通过直接观测获取[7]。选取最小二乘法确定 $r$、$b$ 值，公式描述如下：

$$[r,b]^{\mathrm{T}}=[B^{\mathrm{T}}B]^{-1}B^{\mathrm{T}}Y \tag{5}$$

$$\boldsymbol{B}=\begin{bmatrix}-\frac{1}{2}(l^{(1)}(1)+l^{(1)}(2)) & -\frac{1}{4}(l^{(1)}(1)+l^{(1)}(2))^2\\ -\frac{1}{2}(l^{(1)}(2)+l^{(1)}(3)) & -\frac{1}{4}(l^{(1)}(2)+l^{(1)}(3))^2\\ \vdots & \vdots\\ -\frac{1}{2}(l^{(1)}(n-1)+l^{(1)}(n)) & -\frac{1}{4}(l^{(1)}(n-1)+l^{(1)}(n))^2\end{bmatrix} \tag{6}$$

$$Y_N=[l^{(0)}(2),l^{(0)}(3),\cdots,l^{(0)}(n)]^{\mathrm{T}} \tag{7}$$

式(5)内，$\boldsymbol{B}$ 和 $Y$ 分别表示灰信息覆盖矩阵和约束条件。

在式(4)内代入计算获取的 $r$、$b$ 值，确定一阶白化非线性微分方程解[8]，由此确定 Verhulst 模型的时间响应表达式如下：

$$\hat{L}^{(1)}(t)=\frac{\frac{r}{b}}{1+\left[\frac{r}{b}\cdot\frac{1}{L^{(0)}(1)}-1\right]\mathrm{e}^{-a(t-1)}} \tag{8}$$

利用式(8)还原等时距处理后的初始序列的 Verhulst 模型检测值，得到：

$$\hat{L}^{(0)}(t)=\hat{L}^{(1)}(t)-\hat{L}^{(1)}(t-1) \tag{9}$$

### 1.1.3 非等时距 Verhulst 的反函数模型

泛在终端安全态势实测风险与时间曲线普遍表现为反“S”形[9]，同 Verhulst 模型曲线近似互为泛函数。该曲线在整体可分为曲线斜率线性提升、缓慢提升和位移量快速提升并趋于上限值三个主要阶段[10]。基于此由量化信息的角度出发，选取非等时距灰色 Verhulst 的泛函数模型表现其与拟合安全态势曲线反“S”形波动特性。

基于式(8)的反函数实施变量互换，即可获取式(10)所示的灰色 Verhulst 反函数模型：

$$\hat{L}^{(1)}(t)=\frac{1}{r}\ln\frac{(r-bt_0)t}{rt_0-bt_0t}+\hat{L}^{(0)}(t) \tag{10}$$

通过式(10)即可还原确定泛在终端初始序列的预测值。

## 1.2 泛在终端种类攻击自动识别

泛在终端是用户行为的直接感知者，且随着终端设备技术的飞速发展，尤其是智能终端和嵌入式操作系统的发展和普及，终端设备能够更好地感知用户的行为和习惯，例如用户活动的地理位置信息、设备使用习惯、个人兴趣偏好、消费倾向等。

将泛在终端初始序列的预测值输入训练好的支持向量机分类模型内，利用支持向量机即可完成泛在终端种类攻击自动识别。在支持向量机自动识别过程中

考虑泛在终端通信协议数据的高维特性和攻击种类的多样性[11],可采用粒子群算法优化支持向量机分类模型。

### 1.2.1　支持向量机分类模型参数优化

采用粒子群算法优化支持向量机分类模型就是通过模拟动物觅食过程,在优化问题的解空间内,随机初始化粒子群算法内各粒子的初始位置[12],令其具备初始速度;确定各粒子的适应度函数值,基于各代适应度值判断粒子个体最优位置与全局最优位置,此后经由跟踪两个最优位置持续优化粒子自身速度与位置[13]。优化算法公式描述如下:

$$v_{i,j}^{i+1} = qv_{i,j}^{t} + s_1 rand_1(w_{bi,j}^{t} - w_{i,j}^{t}) + s_2 rand_2(u_b^{tt} - w_{i,j}^{t}) \tag{11}$$

$$w_{i,j}^{t+1} = w_{i,j}^{t} + v_{i,j}^{i+1} \tag{12}$$

式中:$v_{i,j}^{i+1}$和 $w_{i,j}^{t+1}$分别表示优化后的粒子自身速度与位置;$w_b$和 $u_b$分别表示粒子个体最优位置与全局最优位置;$q$ 和 $rand(\,)$分别表示惯性权重和随机函数;$s_1$、$s_2$表示加速因子。由此能够说明粒子当前速度、个体最优与全局最优是影响粒子速度更新的主要因素[14]。

为提升全局搜索能力,可对粒子群的惯性权重 $q$ 实施优化,其随迭代次数的提升而线性提升,在迭代次数满足某一阈值的条件下,重置惯性权重初始值,可避免算法陷入局部极值的问题,由此确定最优解。惯性权重 $q$ 优化过程公式描述如下:

$$\begin{cases} q \quad c \leqslant c_{\max} \\ q = \dfrac{c \leqslant c_{\max}}{c_{\text{sum}} \leqslant c_{\max}}(q_{\max} - q_{\min}) + q_{\min} \quad c \geqslant c_{\max} \end{cases} \tag{13}$$

式中:$c$ 表示迭代次数;$c_{\max}$和 $c_{\text{sum}}$分别表示迭代次数阈值和优化次数总值;$q_{\max}$和 $q_{\min}$分别表示惯性权重的上限值和下限值。

### 1.2.2　优化后的分类模型构建

普遍使用的支持向量机模型多为二值分类,但考虑泛在终端攻击类型具有多样性特征,因此需以支持向量机模型为基础,采用间接法组合多个二分类器构建多分类器[15]。考虑一对多法对单一的二分类器的标准较为繁琐,因此选用一对一法处理二分类器,由此需构建$\dfrac{n(n-1)}{2}$个支持向量机模型,单一支持向量机训练过程中选用对应的两类样本。举例说明:将安全态势监测模型得到的预测值作为输入,在第 $i$ 类与第 $j$ 类间寻找最优超平面的条件下,利用式(14)表示相应的训练集。

$$(l_{ij,t}, y_{ij,t}), t = 1,2,\cdots,n_{ij,t}, l_{ij,t} \in R^d, y_{ij,t} \in \{i,j\} \tag{14}$$

$$\min_{q_{ij},e_{ij}} \quad \frac{1}{2}\|q_{ij}\|^2 + C\sum_{i=1}^{m_{ij}} \theta_{ij,t} \tag{15}$$

$$\text{s.t.} \begin{cases} (q_{ij})^{\mathrm{T}}\varphi(l_{ij,t}) + b_{ij} \geqslant 1 - \theta_{ij,t} \quad y_{ij,t} = i \\ (q_{ij})^{\mathrm{T}}\varphi(l_{ij,t}) + b_{ij} \geqslant -1 + \theta_{ij,t} \quad y_{ij,t} = j \\ \theta_{ij,t} \geqslant 0 \end{cases} \tag{16}$$

式(15)、式(16)内,$C$ 和 $\theta_{ij,t}$分别表示误差惩罚系数和经验风险,$\varphi$ 表示非线性变换。

在构建$\dfrac{n(n-1)}{2}$个支持向量机模型后,选取最大赢投票法划分检测样本集类型,即利用二分类支持向量机模型对比 $n$ 个类的训练样本中任意两个类,删除较差类别,保留优势类别,循环此过程至最优优胜分类机输出类别,该类别为输入样本的最终类别。

## 2　实验分析

为验证本文所研究的基于安全态势监测模型的泛在终端种类攻击自动识别方法在实际应用中的效果,搭建了一个实验网络,其网络拓扑结构如图 1 所示。网络中包括防火墙、交换机、入侵检测系统、Web 服务器、文件服务器、工作站以及一台攻击主机。其中:IDS 安装 SNORT 入侵检测系统,Web 服务器和工作站均安装 Windows 操作系统,文件服务器安装 Linux 操作系统。在数据采集上选用网络运行中 IDS、防火墙产生的报警数据,以及各主机的安全审计日志。

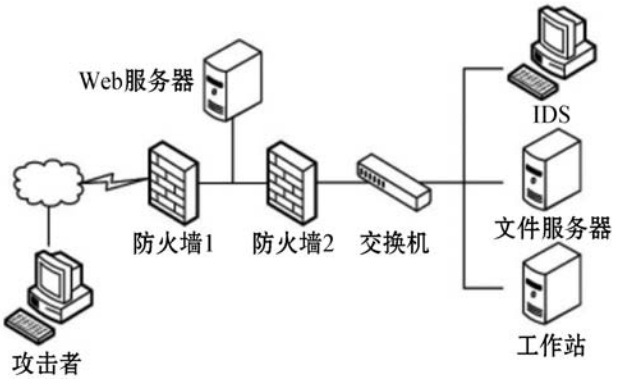


图 1　实验网络拓扑结构

### 2.1　研究对象安全态势监测

在图 1 实验网络拓扑结构的基础上,采用本文方法收集 NSL-KDD 数据集中 2020 年 8 月份的攻击数据作为测试数据,利用本文方法对研究对象在该月内的安全态势实施分析。对所采集的测试数据进行处理后,即可得到表 1 内所示的非等时距初始数据系列。

**表 1 非等时距初始数据系列**

| 时序 | 日期 | 风险值 |
|---|---|---|
| 1 | 8 月 7 日 | 18.4 |
| 2 | 8 月 9 日 | 4.9 |
| 3 | 8 月 12 日 | 3.6 |
| 4 | 8 月 17 日 | 8.1 |
| 5 | 8 月 21 日 | 16.3 |
| 6 | 8 月 24 日 | 11.9 |
| 7 | 8 月 26 日 | 6.5 |
| 8 | 8 月 29 日 | 12.0 |

分析表 1 得到，$L^{(0)}(t_i)=\{18.4,4.9,3.6,8.1,16.3,11.9,6.5,12.0\}(i=1,2,\cdots,8)$，$T=\{0,2,5,10,13,17,19,23\}$。

采用本文对表 1 内的数据进行等时距处理后能够得到 $H=\begin{bmatrix}h_0\\h_1\end{bmatrix}=\begin{bmatrix}-3\\4\end{bmatrix}$，$t_i'=h_0+h_1\cdot i(i=1,2,\cdots,8)$。由此能够确定等时距的时间序列。选取插值法，以基础数据 $L^{(0)}(T)$ 与 $T$ 为基础，可确定等时距处理后的数列为 $L^{(0)}(T')=\{17.8,3.6,7.4,14.5,11.9,8.2,4.3,11.7\}$。

采用本文方法对 $L^{(0)}(T')$ 实施一次累加处理，即可得到 $L^{(1)}(T')=\{17.8,21.5,29.0,43.6,55.6,63.9,68.3,80.1\}$。由于 $L^{(1)}(T')$ 在Ⅱ段曲线斜率快速上升，因此基于表 2 内的相关数据，采用 Verhulst 模型进行建模。

**表 2 安全态势感知数据**

| 时序 | 日期 | 观测值 $L^{(0)}$ | 一次累加处理值 $L^{(1)}$ | 预测值 $\hat{L}^{(1)}$ |
|---|---|---|---|---|
| 1 | 8 月 7 日 | 17.8 | 17.8 | 17.790 |
| 2 | 8 月 9 日 | 3.6 | 21.5 | 24.909 |
| 3 | 8 月 12 日 | 7.4 | 29.0 | 33.668 |
| 4 | 8 月 17 日 | 14.5 | 43.6 | 43.707 |
| 5 | 8 月 21 日 | 11.9 | 55.6 | 54.269 |
| 6 | 8 月 24 日 | 8.2 | 63.9 | 64.436 |
| 7 | 8 月 26 日 | 4.3 | 68.3 | 73.420 |
| 8 | 8 月 29 日 | 11.7 | 80.1 | 80.777 |

根据表 2 中的相关数据，采用 Verhulst 模型，构建安全态势监测模型，对研究对象 2020 年 9 月 1 日至 8 日的安全态势进行预测，所得结果与研究对象实际安全态势值间的拟合曲线如图 2 所示。

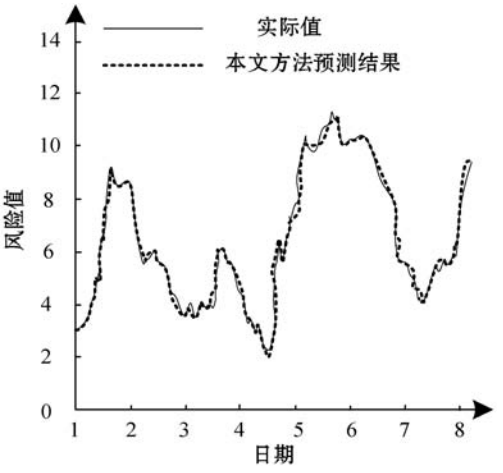


图 2 研究对象安全态势演化图

分析图 2 得到，本文方法的预测结果与实际值之间集拟合度较高，同时本文方法对于中长期安全态势的预测精度下降幅度较低，说明本文方法对研究对象的安全态势预测精度较高，利用本文方法得到的安全态势数据作为研究对象种类攻击识别的基础，能够提升识别精度。

## 2.2 支持向量机训练

利用本文方法对研究对象安全态势预测结果构建样本集，将其中 40% 的数据作为训练样本，剩余 60% 的数据作为测试样本，利用本文改进粒子群算法进行确定支持向量机模型参数的最优值，设定粒子群为 20，支持向量机模型参数寻优结果如图 3 所示。

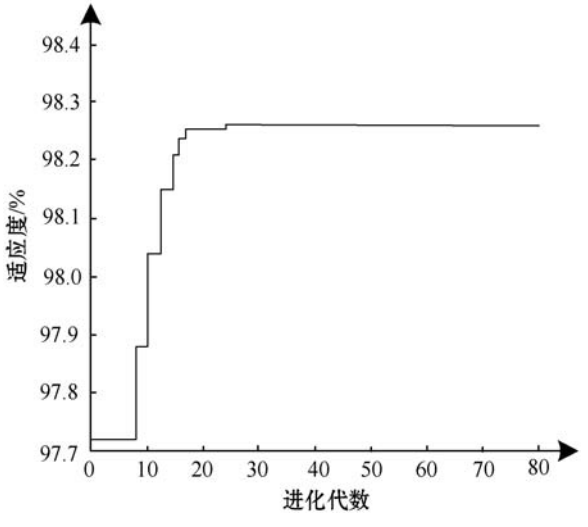


图 3 支持向量机参数优化结果

分析图 3 得到，在本文方法中改进粒子群算法进化代数达到 26 时，分类准确率达到上限值 98.27%，并稳定在 98.27%。

本文所使用的改进粒子群算法、粒子群算法和遗传算法对本文方法中支持向量机模型参数优化结果的对比情况如表 3 所示。

**表 3　优化结果对比**

| 性能 | 改进粒子群算法 | 粒子群算法 | 遗传算法 |
|---|---|---|---|
| 训练时间/s | 62.34 | 43.85 | 168.24 |
| 收敛代数 | 22 | 18 | 41 |
| 准确率/% | 99.24 | 95.9 | 95.34 |

由表 3 可知,利用改进粒子群算法对支持向量机模型参数进行优化后,模型的性能训练时间与收敛导数虽然略高于粒子群算法优化结果,但与遗传算法相比具有明显优势,同时训练准确率显著优于粒子群算法和遗传算法,综合之下可知本文所使用的改进粒子群算法对支持向量机模型参数进行优化后可提升模型性能。

## 2.3　识别结果

为验证本文方法对研究对象攻击类型识别的效果,对研究对象不同攻击类型进行标记,并详细描述不同攻击的具体内容,结果如表 4 所示。

**表 4　攻击描述**

| 标记号 | 攻击名称 | 攻击描述 |
|---|---|---|
| a | DOS | 拒绝服务攻击 |
| b | Reconnaissance | 侦察攻击 |
| c | CMRI | 复杂的恶意响应注入攻击 |
| d | NMRI | 简单的恶意响应注入攻击 |
| e | MPCI | 恶意参数命令注入攻击 |
| f | MSCI | 恶意状态命令注入攻击 |

采用本文方法识别研究对象攻击类型,结果如图 4 所示。

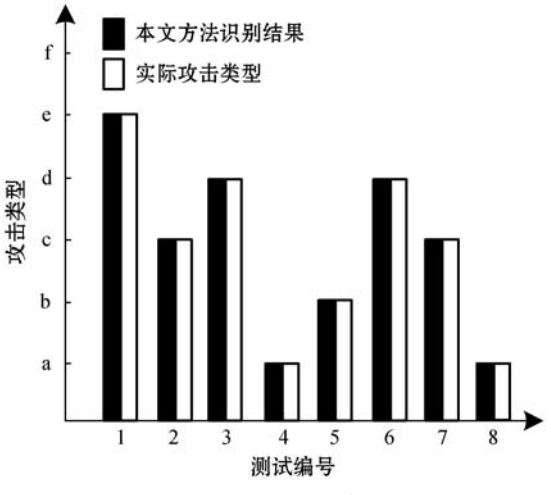


图 4　本文方法识别结果

本文方法通过支持向量机算法优化分类模型参数,在此基础上通过二分类支持向量机模型对比任意两个攻击类型,删除较差攻击类型,保留优势攻击类型,循环此过程至最优优胜攻击类型机输出攻击类型,该攻击类型为输入样本的最终攻击类型,提高了识别的准确度。分析图 4 可知,本文方法对研究对象攻击类型识别结果与实际攻击类型完全一致,进一步验证了本文方法的可应用性。

为验证本文方法在攻击类型识别领域的优势,以文献[4]内的方法和文献[5]内的方法为对比方法,对比本文方法对对比方法在识别攻击类型过程中的查准率、漏报率和误报率,结果如表 5 所示。

**表 5　不同方法识别性能对比(%)**

| 对比项 | 本文方法 | 文献[4]方法 | 文献[5]方法 |
|---|---|---|---|
| 查准率 | 97.81 | 91.12 | 90.11 |
| 漏报率 | 0.35 | 6.81 | 8.61 |
| 误报率 | 0.03 | 3.36 | 2.11 |

分析表 5 可知,相较于本文方法,文献[4]方法在误报率方面提升 3.33 百分点,文献[5]方法在漏报率方面提升 8.26 百分点。两种对比方法的查准率与本文方法查准率 97.81 百分点,相比分别降低 6.69 百分点和 7.70 百分点。由此说明本文方法具有较好的差别效果。

DCP 值所描述的是数据中心中输入能耗与关键设备置于用于数据处理、传输与存储等过程的能耗比值。DCP 值计算公式如下:

$$D_{\mathrm{CP}} = \frac{Y}{X} \times 100\% \tag{17}$$

式中:$X$ 表示数据中心输入总能耗;$Y$ 表示数据中心内关键设备直接用于数据信息计算、处理、存储、传输、交换的能源能耗。计算得出的 DCP 值越高说明攻击类型识别过程所使用的能耗越高。表 6 所示为本文方法与对比方法在识别攻击类型过程中的 DCP 值对比情况。

**表 6　不同方法 DCP 值对比**

| 样本数量 | 本文方法 DCP 值/% | 文献[4]方法 DCP 值/% | 文献[5]方法 DCP 值/% |
|---|---|---|---|
| 100 | 0.004 6 | 0.004 9 | 0.004 7 |
| 200 | 0.004 8 | 0.005 2 | 0.004 8 |
| 300 | 0.005 1 | 0.005 5 | 0.005 0 |
| 400 | 0.005 2 | 0.005 9 | 0.005 2 |
| 500 | 0.005 2 | 0.006 1 | 0.005 3 |
| 600 | 0.005 5 | 0.006 3 | 0.005 6 |
| 700 | 0.005 6 | 0.006 6 | 0.006 0 |
| 800 | 0.005 8 | 0.006 9 | 0.006 6 |
| 900 | 0.006 0 | 0.007 1 | 0.007 3 |
| 1 000 | 0.006 3 | 0.007 4 | 0.008 0 |

分析表6得到,随着样本数量的提升,不同方法在识别研究对象攻击类型过程中的 DCP 值均有所提升。其中本文方法在的 DCP 值最高达到 0.006 3%,与两种对比方法相比明显下降,由此说明本文方法在实际应用过程中具有较低的能耗。本文方法能耗较低的原因是在对攻击类型识别之前,构建了安全态势监测模型,充分利用该模型的优势,即通过数据融合技术实现态势感知分析,数据融合将来自多个信息源的数据收集起来,进行过滤、归并、关联,提升数据的有效性和精确度,减少数据中心内关键设备直接用于数据信息计算、处理、存储、传输、交换的能源能耗。

## 3 结 语

本文研究基于安全态势监测模型的泛在终端种类攻击自动识别方法,基于泛在终端安全态势监测结果,利用支持向量机模型识别泛在终端攻击种类,测试结果显示本文方法具有较高的识别精度与能耗。

## 参 考 文 献


[1] Cherpakov A V, Shlyakhova E A, Egorochkina I O, et al. Identification of concrete properties in beam-type structures with defects based on dynamic methods[J]. Materials Ence forum, 2018, 931(1):373 - 378.

[2] 王兴涛,赵训威,付海旋,等. 基于嵌入式系统的电力无线专网远程通信终端研制[J]. 电子技术应用,2020,46(1):108 - 112.

[3] 戚湧,郭诗炜,李千目. 电网融合泛在网信息平台设计及安全威胁分析[J]. 计算机科学,2017,44(3):150 - 152.

[4] 曲朝阳,董运昌,刘帅,等. 基于生物免疫学方法的泛在电力物联网安全技术[J]. 电力系统自动化,2020,44(2):1 - 12.

[5] 余洋,朱少敏,卞超轶. 基于知识图谱的泛在电力物联网安全可视化技术[J]. 电信科学,2019,35(11):132 - 139.

[6] Yang L, Liu J, Zhang Y. An intelligent security defensive model of SCADA based on multi-agent in oil and gas fields [J]. International Journal of Pattern Recognition and Artificial Intelligence, 2020, 34(1):1 - 13.

[7] 钱斌,蔡梓文,肖勇,等. 基于模糊推理的计量自动化系统网络安全态势感知[J]. 南方电网技术,2019,13(2):51 - 58.

[8] 韩晓露,刘云,张振江,等. 基于 IFS-NARX 模型的网络安全态势预测[J]. 吉林大学学报(工学版),2019,49(2):592 - 598.

[9] 丁华东,许华虎,段然,等. 基于贝叶斯方法的网络安全态势感知模型[J]. 计算机工程,2020,514(6):136 - 141.

[10] Kotenko I, Doynikova E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics[J]. Journal of Defense Modeling and Simulation, 2018, 15(2):181 - 204.

[11] 冯英伟,王庆福,吕国,等. 基于改进证据理论的物联网安全态势评估[J]. 西安理工大学学报,2018,34(4):121 - 127.

[12] 何金栋,王宇,赵志超,等. 智能变电站嵌入式终端的网络攻击类型研究及验证[J]. 中国电力,2020,53(1):81 - 91.

[13] 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.

[14] 刘远龙,潘筠,王玮,等. 用于泛在电力物联网的配电变压器智能感知终端技术研究[J]. 电力系统保护与控制,2020,48(16):140 - 146.

[15] 姚琳元,董平,张宏科. 基于对象特征的软件定义网络分布式拒绝服务攻击检测方法[J]. 电子与信息学报,2017,39(2):381 - 388.


(上接第 326 页)


[9] Alkadri N A, Bansarkhani R E, Buchmann J. BLAZE: Practical lattice-based blind signatures for privacy-preserving applications [C]//International Conference on Financial Cryptography and Data Security,2020:484 - 502.

[10] Bouaziz-Ermann S, Canard S, Eberhart G, et al. Lattice-based (partially) blind signature without restart [EB/OL]. [2020 - 12 - 07]. https://eprint.iacr.org/2020/260.

[11] Alkim E, Barreto P, Bindel N, et al. The lattice-based digital signature scheme qTESLA[C]//International Conference on Applied Cryptography and Network Security,2020:441 - 460.

[12] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology,2000,13(3):361 - 396.

[13] Ducas L, Durmus A. Ring-LWE in polynomial rings[C]// International Workshop on Public Key Cryptography,2012:34-51.

[14] Lyubashevsky V. Lattice signatures without trapdoors[C]// 31st Annual International Conference on Theory and Applications of Cryptographic Techniques,2011:738 - 755.

[15] Boneh D, Freeman D M. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures [C]//14th International Conference on Practice and Theory in Public Key Cryptography,2011:1 - 16.

[16] Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma[C]//13th ACM Conference on Computer and Communications Security,2006:390 - 399.