基于卷积神经网络的电力通信网络攻击源定位方法

严彬元,王皓然,周泽元
(贵州电网有限责任公司信息中心,贵州 贵阳,550002)

摘 要:为了提高电力通信网络攻击源定位准确性和方法收敛速度,本文提出基于卷积神经网络的电力通信网络攻击源定位方法。方法采用一阶空间回归模型分析电力通信网络目标设备的空间结构特征,采用振动波模型确定攻击源大尺度时空变化趋势,采用一阶自回归模型确定小尺度时空变化趋势,并以此为基础,利用 Stirling 插值公式导出电力通信网络攻击源模型状态方程,对电力通信网络攻击源聚合处理。采用双人攻防博弈模型计算网络攻击和网络防御策略效用,判断攻击和防御效用大小,评估电力通信网络安全性;确定电力通信网络熵变率阈值,计算网络熵变率、相对熵值和网络数据包基线概率分布,设计电力通信网络攻击检测步骤,检测网络攻击;根据卷积神经网络结构,选择网络激活函数,通过网络正向和反向传播,划分网络数据类别,确定电力通信网络拓扑结构,选择网络攻击者和被攻击节点,定位攻击源定位。实验结果表明:方法可有效提升攻击源的定位精度。

关键词:卷积神经网络;电力通信;通信网络;网络攻击;源定位;定位方法
文章编号:2096-4633(2022)3-0026-08 **中图分类号**:TP393 **文献标志码**:A
DOI:10.19317/j.cnki.1008-083x.2022.03.004

区域经济发展中的各个企业对于电力稳定、可靠、经济等性能的要求极高,亟需电力企业将通信、计算机、电子技术、网络等技术进行有机结合,实现电力智能化和自动化[1]。互联网时代,由于电力通信数据的不断增加,且传输过程中受到网络中多种病毒等的袭击[2],导致电力通信系统通信不佳,影响电力通信网络可靠性、CPS 的安全性[3]。

基于此,国内外相关学者十分重视电力通信网络安全,已经研究出众多网络安全检测、攻击追踪、攻击定位、攻击标记、安全评估、攻击防御等电力通信网络安全保护技术[4]。这些技术虽然在一定程度上保护了电力通信网络,却难以定位网络攻击源,从源头解决网络攻击[5]。其中,文献[6]将深空探测器信标信号作为研究对象,根据探测器信标的信号频率,定位探测器信标信号源。文献[7]在乌鸦搜索算法基础上,将其改进为自适应乌鸦搜索算法,全局搜索信息源头,实现信息源定位。上述网络攻击源定位方法中,定位电力通信网络攻击源时,存在攻击源定位准确性低的问题。

为此,本文提出基于卷积神经网络的电力通信网络攻击源定位方法。

1 电力通信网络攻击源分析

1.1 电力通信网络信道攻击源空间状态分析

电力通信网络在运行过程中,由于通信信道受到外界环境影响,存在一定的脆弱性。针对这一问题,本文提出了一种基于单一包标号的方法来改进传统的随机分组标记(PPM)的最弱链路和较差收敛的问题。在单次包标记算法中,用 p 表示攻击路径 AP 上的电力通信网络路由器 $R_i(i=1,2,\cdots\cdots,d)$ 对每个经过的数据包进行标记的概率,用 $\alpha_i(p)$ 表示一个数据包被传输路径上第 i 个路由器 R_i 最后标记到达电力通信网络设备的概率,则 $\alpha_i(p)=p(1-p)^{d-i}(i=1,2,\cdots\cdots,d)$。

因为 p 是单次包标记,那么 $\alpha_1(p)=p$,$\alpha_2(p)=p[1-\alpha_1(p)]=p(1-p)$,$\alpha_3(p)=p[1-\alpha_1(p)-\alpha_2(p)]=p(1-p)^2$,依次递推,$\alpha_1(p)=p(1-p)^{i-1}(i=1,2,\cdots\cdots,d)$,当 $p=1/25$,可以得出结论 $\alpha_1(p)\leqslant\alpha_2(p)\leqslant\alpha_3(p)\leqslant\cdots\cdots\leqslant\alpha_d(p)$。则电力通信网络设备受到攻击的时间计算公式为:

$$E(N)=\int_0^{\infty}\left[1-\prod_{i=1}^{d}(1-e^{-al})\right]dt \tag{1}$$

其中:q_i 表示电力通信网络设备收到由路由器 R_i 标记的数据包的概率,q 和 q^i 分别表示初始和 i 时刻电网通信网络设备接收到一个携带路由器 R_1 标记(最弱链)的包的概率,N 和 N^i 分别表示初始和 i 时刻电力通信网络设备获得最弱链标记所需的数据包质量。

假设电力通信网络中存在 S 个传感器节点,任

意传感器节点（$s=1,2,\cdots\cdots,S$）在 t_k 时隙采集关于目标攻击信息 $y_k(s)$ 的感知数据，即为 $ob_k(s)$。那么集合$\{ab_k(s),s=1,2,\cdots\cdots,s\}$可以表示为$\{y_k(s)\}$与加性噪声 $\eta_{ab}(s)$ 之和的形式：

$$ab_k(s)=y_k(s)+\eta_{ab}(s) \tag{2}$$

其中：$\{ab_k(s)\}$为一组独立同分布的随机变量集合，而 $\eta_{ab}(s)$ 为服从 $N(0,\sigma_{ab}^2(s))$ 分布的加性高斯白噪声。

根据贝叶斯空时建模方法，电力通信网络目标函数$\{y_k(s)\}$可以表示四个相互独立分量之和的形式，记为：

$$y_k(s)=\mu(s)+M(s,t_k)+\Omega_k(s)+\eta_y(s) \tag{3}$$

其中：$\mu(s)$ 表示电力通信网络攻击源相关函数，$M(s,t_k)$ 表示电力通信网络攻击源长期时变过程，$\Omega_k(s)$ 表示电力通信网络攻击源的短期时变过程，主要用于电力通信网络攻击链变化情况的体现。

对于 $\mu(s)$，采用一阶空间回归模型来描述电力通信网络目标设备的空间结构特征，其模型可以表示为：

$$\mu(s)=\mu_1+\mu_2 I(s) \tag{4}$$

其中：$I(s)$ 表示攻击源节点 s 的空间位置，μ_1 表示电力通信网络目标设备的整体均值，μ_2 表示空间位置对 $\mu(s)$ 的修正。

对于 $M(s,t_k)$，采用振动波模型来表示电力通信网络攻击源大尺度时空变化趋势，该模型可以表示为一个直流分量和两个谐波分量之和，记为：

$$M(s,t)=ht+f(s)\cos(\omega t)+g(s)\sin(\omega t) \tag{5}$$

其中：ht 代表电力通信网络特征随着时间线性变化的因子，ω 表示电力通信网络周期性变化因子的变化频率，$f(s)$ 和 $g(s)$ 表示随空间变化的周期性因子的振幅，记为：

$$f(s)=f_1+f_2 long(s)+f_3 lat(s) \tag{6}$$

$$g(s)=g_1+g_2 long(s)+g_3 lat(s) \tag{7}$$

其中：$long(s)$ 和 $lat(s)$ 分别表示攻击源节点 s 的经度和纬度；系数 f_1,f_2,f_3 以及 g_1,g_2,g_3 均为独立高斯随机变量。

对于 $\Omega_k(s)$，采用一阶自回归模型 AR(1) 描述电力通信网络攻击源短期的变化趋势为以下形式：

$$\Omega_k(s)=\phi(s)\Omega_{k-1}(s)+\eta_\Omega(s) \tag{8}$$

1.2　电力通信网络攻击源聚合分析

基于电力通信网络攻击源时空变化情况，通过自回归系数 ψ 确定电力通信网络随机变量并独立于攻击源节点所在位置。主要针对电力通信网络能力的限制和自组织的组网方式，典型传感器网络部署范围相对较小，假定电力通信网络中所有攻击源节点拥有近似相同的经度和纬度，那么上节中第一个分量 $\mu(s)$ 的取值趋向独立于位置函数 $l(s)$，即 μ_2 趋近于 0，而 $\mu(s)$ 可以近似为 μ_1。此外，电力通信网络的数据采样间隔从几秒至数天不等，因此上节中第二个分量 $M(s,t_k)$ 可以近似为：

$$M(s,t_k)=M(\ ,t_k)\approx M(\ ,t_k-1) \tag{9}$$

此外，假设电力通信网络每个分簇中平均有 b 个攻击源节点，令 z_k 表示攻击源节点关于 x_k 的观测值，那么聚合结果 x_k 可以表示为：

$$x_k=\frac{1}{b}\left(\sum_{s=s_1}^{s_b}\mu(s)+\sum_{s=s_1}^{s_b}M(s,t_k)+\sum_{s=s_1}^{s_b}\Omega_k(s)\right)\eta_{ob} \tag{10}$$

其中，η_{ob} 表示服从 $N\left(0,\frac{1}{b}\sum_{s=s_1}^{s_b}\sigma_{ob}^2(s)\right)$ 分布的加性高斯白噪声。功率通讯网中的一种近似形式的状态方程式：

$$x_{k+1}=F(x_k,w_k)\approx F(\bar{x}_k,w_k)\bar{D}_{\Delta k}F+\bar{D}_{\Delta k}^2F \tag{11}$$

其中：$\widetilde{D}_{\Delta k}$ 和 $\widetilde{D}_{\Delta k}^2$ 分别表示电力通信网络攻击源的特征量。令 $\widetilde{x}_k$ 和 $P_{x,k}$ 分别表示电力通信网络攻击状态 x_k 的均值和协方差。

为了简化聚合步骤，假定在受到攻击后，每个链路都具有同样的数据丢失和发送差错的可能性。

令 $\mu=E[ob_k(s)]$，$\sigma^2=\mathrm{var}[ob_k(s)]$，分别表示攻击源节点 t_k 时隙采集到感知数据的均值与方差。功率通信网络在此时隙中的攻击源的聚集结果可以用以下方式来表达：

$$x_k=\frac{1}{n-m-r}\left(\sum_{s=s_1}^{s_n}ob_k(s)-\sum_{j=j_1}^{j_n}ob_k(j)\right) \tag{12}$$

式中：$j_1,\cdots\cdots,j_{m+r}$ 表示攻击时电力通信网络发送数据包时，为了确保网络中的所有节点 ID 都能有效地传递失真和丢失的信息。

2　电力通信网络攻击源定位方法

电力通信网络中包含大量的电力系统运行数据，以此保障电力系统运行的安全、稳定、实时、可靠运行。因此，当电力通信网络受到攻击时，网络中的数据极易丢失，导致电力系统运行安全性和可靠性降低。基于此，采用评估电力通信网络安全的方式，

判断网络是否安全，若网络不安全，则需要检测网络攻击，并根据检测结果，采用卷积神经网络定位网络攻击源。

2.1 评估电力通信网络安全

此次将采用双人攻防博弈模型，评估电力通信网络安全。将网络的安全防御和攻击策略分别作为模型博弈两方，假设攻击策略从第 i 处网络 o_i，开始攻击电力通信网络，则攻击者攻击网络和防御者防御攻击的效用函数分别为：

$$\begin{aligned}\xi_1\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)&=\left[O_{o_j}^{(1)}-\zeta\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)\right]\times O_{o_j}^{(2)}\\ \xi_2\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)&=\zeta\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)\times O_{o_j}^{(2)}-G\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)\end{aligned}\tag{13}$$

式(13)中，$\xi_1\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$表示攻击策略攻击网络安全防御获得的效用；$O_j^{(1)}$ 表示第 j 处网络 o_j 安全防御漏洞；$\varsigma_{i,j}^{(1)}$表示攻击 o_j 的策略；$\varsigma_{i,k}^{(2)}$表示面对 o_i 处攻击，选择的第 k 个防御策略；$\zeta\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$表示网络受到$\xi_1\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$攻击时，$\varsigma_{i,j}^{(1)}$为电力通信网络带来的正面影响；$O_{o_j}^{(2)}$ 表示接入第 j 处网络 o_j 维度；$\xi_2\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$表示防御者防御攻击策略获得的效用；$G\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$表示面对 o_i 处攻击，选择的第 k 个防御策略，对电力通信网络造成负面的影响[8]。如(13)式所示的效用计算公式，攻击者与防御者博弈时，其为电力通信网络带来的正面与负面影响为：

$$\begin{aligned}\zeta\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)&=\left(a_j\wedge b_k\right)\times o_l\times L_{o_j}\\ G\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)&=o_j\times\sum_{i\in\gamma_k}A_{a_{2,j}}\end{aligned}\tag{14}$$

式(14)中，$a_j=[a_{1,j},a_{2,j}]$ 表示逻辑向量，其阈值为 $[0,1]$，其中，$a_{1,j}$表示对 o_j 发起攻击后网络信息完整性是否被破坏，$a_{2,j}$表示对 o_j 发起攻击后网络信息可用性是否被破坏，当 $a_{1,j}$和 $a_{2,j}$的值等于 1 时，网络信息的完整性和可用性被破坏，反之，则未破坏网络信息完整性和可用性；$b_k=[b_{1,k},b_{2,k}]$ 表示逻辑向量，其阈值为 $[0,1]$，其中，$b_{1,k}$表示$\varsigma_{i,k}^{(2)}$是否能加强信息的完整性；$b_{2,k}$表示$\varsigma_{i,k}^{(2)}$是否能加强信息的可用性，当 $b_{1,k}$和 $b_{2,k}$的值等于 1 时，则增强了网络信息完整性以及可用性，反之，则未增强；$\wedge$表示逻辑与操作符号；o_l 表示电力通信网络中 l 节点受损后，对网络造成的潜在影响；L_{o_j}表示 o_j 的利用难度；γ_k 表示受$\varsigma_{i,k}^{(2)}$影响的网络节点集合；$A_{a_{2,j}}$表示网络信息可用性受损对网络造成的影响[9]。

根据(13)式计算电力通信网络受到的攻击效用与防御效用，若$\xi_1\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)\le\xi_2\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$，则电力通信网络处于安全状态；若$\xi_1\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)>\xi_2\left(\varsigma_{i,j}^{(1)},\varsigma_{i,k}^{(2)}\right)$，则电力通信网络处于不安全的状态，需要检测网络攻击，来定位网络攻击源。

2.2 检测电力通信网络攻击

根据(13)式计算过程，得到的电力通信网络评估结果，通过电力通信网络熵变率检测网络攻击，所设计的网络攻击检测步骤如下。

1) 在电力通信网络中设置定时器，每间隔 t 时间采集一次网络数据包，并将保存采集到的数据包。

2) 统计数据包中熵变率链路数和网络中正在传输的数据包数量，则有：

$$|R|=\binom{|L|}{\mu}\times k!\tag{15}$$

式(15)中，R 表示网络状态空间；L 表示数据通信链路；μ 表示网络传输数据包数量；$k!$ 表示2^10=1024[10]。

3) 将(15)式得到的 L 值和 μ 值代入，求取网络熵变率$E\approx\frac{\partial u}{\partial H}\approx\ln 2\times\left[\left(\ln|L|-u\right)+\frac{2}{2u}\right]^{-1}$，其中，$\partial$表示求导符号；H 表示电力通信网络熵。

4) 确定网络熵变率阈值：

$$\begin{aligned}\overline{E}_t&=\frac{\sum_{I=t-n}^{t-1}E_i}{n}\\ \sigma_t&=\left(\frac{1}{n-1}\left[\sum_{I=t-n}^{t-1}\left(E_i-\overline{E}_t\right)^2\right]\right)^{\frac{1}{2}}\end{aligned}\tag{16}$$

式(16)中，$\overline{E}_t$ 表示单位时间 t 内的熵变率均值；I 表示第 I 个时间段；n 表示第 I 个时间段网络熵变率样本数量；E_i 表示第 I 个时间段网络熵变率值；σ_t 表示单位时间 t 内，n 个网络熵变率样本标准差[11-13]。

根据(16)式计算结果，依据正态分布理论，将 $3\sigma_t$ 作为网络熵变率阈值上下限，则设定的网络熵变率阈值为$[\overline{E}_t-3\sigma_t,\overline{E}_t+3\sigma_t]$。

判断步骤 3 得到的 E 值，是否属于设定的网络熵变率阈值区间，若$E\in[\overline{E}_t-3\sigma_t,\overline{E}_t+3\sigma_t]$，更新网络熵

变率阈值，返回步骤 1，反之，$E \notin [\overline{E}_t-3\sigma_t,\overline{E}_t+3\sigma_t]$，则进入步骤 5；

5) 计算数据包聚集类的概率分布。聚类网络中 n 各不相同的数据包，计算每个聚类集中样本 I 出现的概率 p_I：

$$p_I=\frac{x_I}{\sum_{I=1}^{n}x_I}(I=1,2,\cdots\cdots,n) \tag{17}$$

考虑到网络数据包在时间间隔 t 分段内，可以具有 m 个数据样本特征。因此，依据(17)式所示的样本出现概率，可以得到 m×n 的数据样本概率分布矩阵 P 为：

$$P=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{23} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m1} & p_{m2} & \cdots & p_{m3} \end{bmatrix}_{m\times n} \tag{18}$$

式(18)中，p_{IJ}表示第 I 个样本中，第 J 个聚集类出现的概率[14-16]。基于此，求取 P 每行均值，得到网络数据包基线概率分布：

$$P_0=\left\{\sum_{I=1}^{m}\frac{\rho_{I1}}{m},\sum_{I=1}^{m}\frac{\rho_{I2}}{m},\cdots\cdots,\sum_{I=1}^{m}\frac{\rho_{In}}{m}\right\} \tag{19}$$

6) 计算网络数据包相对熵值 $E(P_0\parallel P)=\sum_{I=1}^{n}\rho_I\ln\frac{P_0}{P}$，当 $P_0=P$ 时，$E(P_0\parallel P)=0$，则 P_0 与 P 之间存在的差异达到最小，反之，$E(P_0\parallel P)$ 的值越大，P_0 与 P 之间存在的差异越大[17-18]。

7) 判断步骤 6 得到的 $E(P_0\parallel P)$ 值是否在 $[\overline{E}_t-3\sigma_t,\overline{E}_t+3\sigma_t]$ 区间中，若在这一区间内，进入步骤 8，反之，进入步骤 9。

8) 将当前时段网络数据包分布放入 P_0 中，并对 P_0 的分布概率进行更新[19-21]。

9) 检测到电力通信网络攻击，完成网络通信攻击检测。依据上述 9 步，在电力通信网络中检测到网络攻击后，需要采用卷积神经网络，对攻击源进行定位。

2.3 基于卷积神经网络定位电力通信网络攻击源

面对电力通信网络中存在的网络攻击，根据卷积神经网络结构，进行定位网络攻击源。定位过程中，网络必须解决大量的非线性问题，需要选择能够增强网络非线性问题处理能力的激活函数[22]。为此，选择如(20)式所示的 ReLU 函数 $f(x)$ 作为卷积神经网络激活函数，则有：

$$f(x)=\max(0,x) \tag{20}$$

式(20)中，x 表示网络输入样本；max 表示取最大值[23-24]。将电力通信网络转化为通过高、深、宽表示的多维矩阵，在(20)式所示的激活函数作用下，网络的卷积层会根据输入网络的多维矩阵进行卷积运算，则有：

$$\begin{cases} H_{out}=\dfrac{H_{in}-H_0}{2}+1 \\ B_{out}=\dfrac{B_{in}-B_0}{2}+1 \end{cases} \tag{21}$$

式(21)中，B_{out}表示卷积层输出宽度；H_{out}表示卷积输出高度[25]；H_0 表示卷积核高度；B_0 表示卷积核宽度；H_{in}表示卷积层输入高度；B_{in}表示卷积层输入宽度。

经过式(21)卷积后的电力通信网络数据会被传入池化层，通过池化层的最大池化和平均池化作用，降低数据特征维数，并将其输入全连接层，划分网络数据类别，完成网络正向传播[26-28]。因此，需要重复上述计算过程，划分电力通信网络数据，且每一次划分网络数据后，都需要计算一次网络损失，判断其是否达到最小值，则网络损失函数 S 计算公式为：

$$S=\frac{1}{n}\sum_x[y\ln(c)(1-y)\ln(1-c)] \tag{22}$$

式(22)中，y 表示网络预测输出值；c 表示网络期望输出值[29]。考虑电力通信网络攻击源应为一处，所以将网络损失函数最小值设定为 1，即 $S_{\min}=1$。若 $S=S_{\min}$，则直接输出网络定位到的攻击源数据；若 $S\neq S_{\min}$，则需要进行反向传播[30]，对网络的偏差量 q 和连接权重 ω 求导，则有：

$$\begin{aligned} \frac{\partial S}{\partial q}&=-\frac{1}{N}\sum_x[f(x)-y]\,x \\ \frac{\partial S}{\partial \omega}&=-\frac{1}{N}\sum_x[f(x)-y] \end{aligned} \tag{23}$$

按照(23)式进行反向传播后，再次根据(22)式计算过程进行正向传播，判断 $S_{\min}$是否等于 1，若不等于 1，继续进行迭代计算，若等于 1，则停止网络迭代，通过输出电力通信网络攻击源定位结果，完成电力通信网络攻击源定位。

3 实例应用

选择电力通信系统中的 IEEE RBTS bus 2 部分

进行电力通信，并在通信过程中建立勒索病毒、DDoS 攻击、ATP 攻击 3 个攻击者，攻击 IEEE RBTS bus 2 中的通信节点，进行验证此次研究的基于卷积神经网络的电力通信网络攻击源定位方法。

3.1　电力通信网络

电力通信网络中的 IEEE RBTS bus 2 环形拓扑结构如图 1 所示。

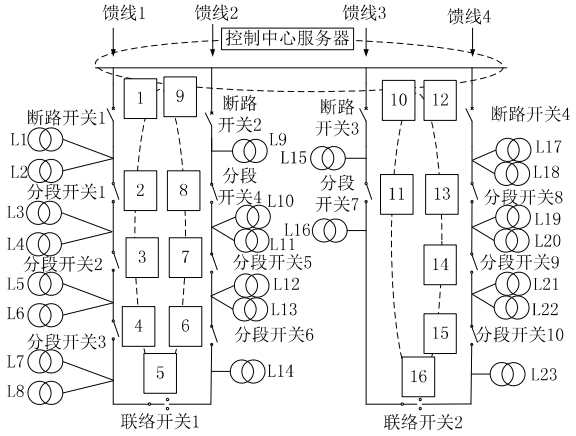


图 1　IEEE RBTS bus 2 通信网络拓扑图

Fig.1　IEEE RBTS bus 2 communication network topology

图 1 中，L 表示配电变压器，1～16 表示通信网络节点。如图 1 所示的 IEEE RBTS bus 2 通信网络拓扑图，通信属于环形通信网络，共包括 1 个控制中心服务器、4 条主馈线、23 个配电变压器、10 个分段开关、4 个断路开关和 2 个联络开关。面对图 1 所示的网络拓扑结构，网络攻击源在攻击 IEEE RBTS bus 2 网络时，只能攻击网络漏洞，即网络节点之间交换信息位置，如图 1 中虚线上的节点设备所示。

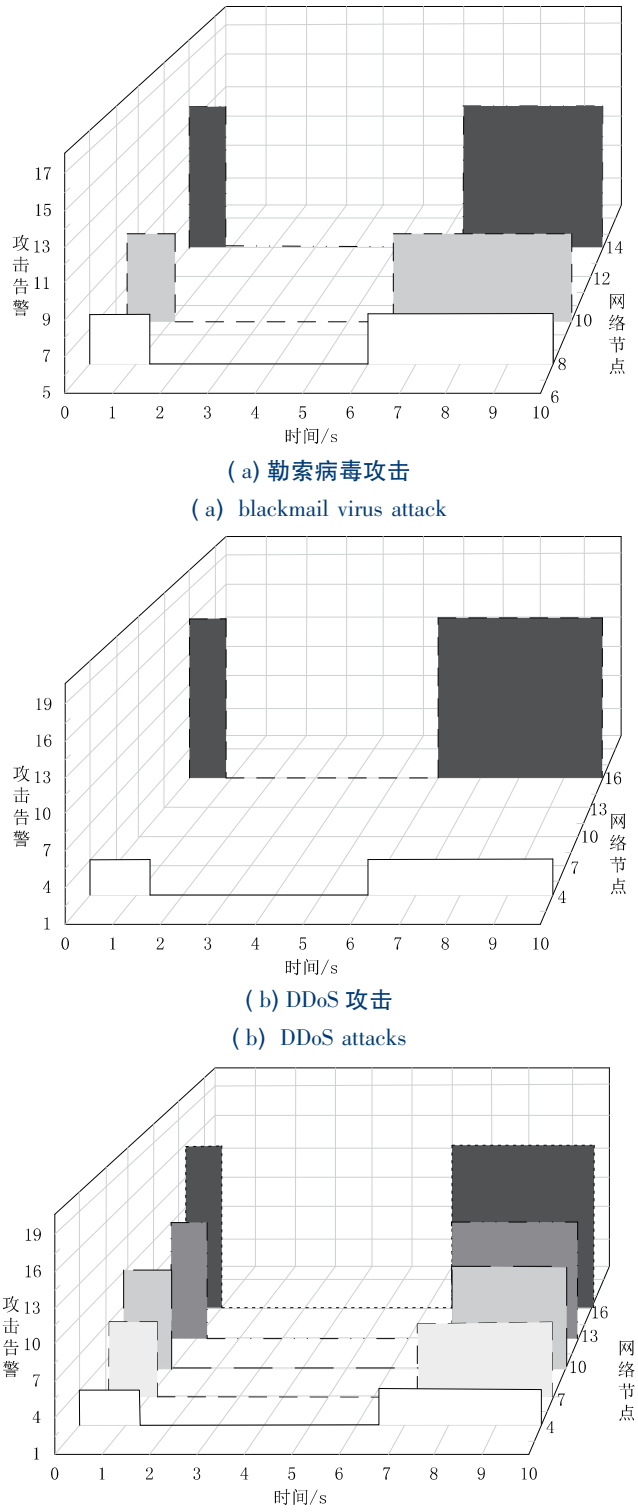
图 1 中虚线上的网络节点，均为攻击者攻击节点。根据图 1 所示的电力通信网络，此次实验在图 1 中的电力通信网络中，勒索病毒、DDoS 攻击、ATP 攻击 3 个攻击者，在同一攻击路径长度与数量下，只能攻击电力通信网络相邻节点中存在的漏洞。

3.2　分析结果

检测此次研究方法，定位 3 个攻击者攻击通信网络节点的攻击源位置准确性、收敛速度。

3.2.1　定位攻击源定位准确性

基于图 1 所示的 IEEE RBTS bus 2 通信网络，在 6s 时，采用实验选择的三个攻击者，分别攻击网络节点，其中，勒索病毒攻击者发生的攻击在 14、8、10 三个节点上；DDoS 攻击者发生的攻击在 16、4 两个节点上；ATP 攻击者发生的攻击在 16、4、13、7、10 五个节点上。根据上述三个攻击者攻击节点，研究方法定位网络攻击源得到的攻击源定位结果如图 2 所示。



(a) 勒索病毒攻击

(a)　blackmail virus attack

(b) DDoS 攻击

(b)　DDoS attacks

(c) ATP 攻击

(c)　ATP attack

图 2　攻击源定位结果图

Fig.2　Diagram of the result of the attack source location

从图 2 中可以看出,研究方法定位信号在 2s 内进入稳定状态,能够对勒索病毒、DDoS 攻击、ATP 攻击 3 个攻击者攻击的节点进行定位。当三个攻击者同时攻击网络时,攻击报警仅在攻击者攻击的节点处显示数值,得到的阶跃响应曲线出现明显波动,定位了三个攻击者攻击源,而其他未被攻击节点处曲线数值均为 0。由此可见,研究方法可以得到准确攻击源位置。

3.2.2　定位攻击源收敛速度

该方法的收敛性是本论文提出的基于该算法的攻击路径重建所需的最小报文数目,并且该算法所需的数据包数目也较小。

该方法定位攻击源收敛速度越快。在本组实验中,将 3 个攻击者的攻击路径长度设置为 1~30。在上一组实验基础上,检测研究方法在定位 3 个攻击者攻击通信网络节点的攻击源时,方法的收敛速度。其检测结果如图 3 所示。

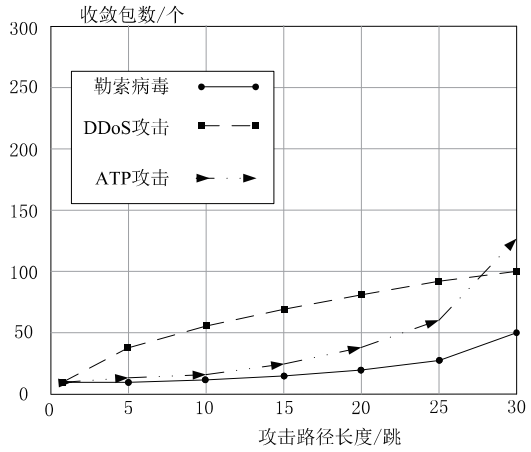


图 3　攻击源定位收敛速度

Fig.3　Convergence rate of attack source localization

从图 3 中可以看出,虽然研究方法面对不同的攻击者,其收敛速度存在一定的差异。但是,研究方法定位 3 个攻击者的攻击源时,所需要的收敛包数都十分少,具有较优的收敛性能。

4　结束语

此次研究采用评估电力通信网络安全的方式,来判断网络是否安全,避免定位方法重复检测网络攻击,提进行提高网络攻击源定位准确性和收敛速度。但此次研究的网络攻击源定位方法,在定位不同类型的网络攻击时,其收敛速度以及定位时间均存在一定的差异。在今后的研究中,还需进一步研究方法的适用范围,让研究方法面对不同类型的攻击源时,都可以快速、准确地定位到网络攻击源。

参考文献:

[1] 吴克河,程瑞,郑碧煌,等.电力物联网安全通信协议研究[J].信息网络安全,2021,21(09):8-15.
WU Kehe, CHENG Rui, ZHENG Bihuang, et al. Research on security communication protocol of power internet of things [J]. Netinfo Security,2021,21(09):8-15.

[2] 李沛哲,肖振锋,陈仲伟,等.电力终端通信接入网通信技术匹配[J].电力科学与技术学报,2021,36(03):125-134.
LI Peizhe, XIAO Zhenfeng, CHEN Zhongwei, et al. Analysis of communication matching technology of power terminal communication access network [J]. Journal of Electric Power Science and Technology,2021,36(03):125-134.

[3] 周楠,张平,郑征,等.基于机器学习的电力通信网带宽分配算法[J].电网与清洁能源,2021,37(05):67-73.
ZHOU Nan, ZHANG Ping, ZHENG Zheng, et al. Bandwidth allocation algorithm for power communication network based on machine learning [J]. Advances of Power System & Hydroelectric Engineering,2021,37(05):67-73.

[4] 佘金涛,姚文杰,王川丰,等. 基于多维融合的电力通信网节点风险评估[J].电子设计工程,2021,29(01):30-35+40.
SHE Jintao, YAO Wenjie, WANG Chuanfeng, et al. Node risk assessment of the power communication network based on multidimention [J]. Electronic Design Engineering,2021,29(01):30-35+40.

[5] BNILAM N,JOOSENS D,AERNOUTS M,et al.LoRay: AoA estimation system for long range communication network [J].IEEE Transactions on Wireless Communications,2020,20(03):2005-2018.

[6] YING W,ZHAN S,ZHONGMIAO K,et al.Research on importance evaluation method of power communication network node based on node damage resistance [J].Journal of Physics: Conference Series, 2019,1168(03):032138.

[7] 唐菁敏,郑锦文,曲文博.基于改进自适应乌鸦搜索算法的无源定位[J].重庆邮电大学学报(自然科学版),2021,33(03):372-377.
TANG Jingmin, ZHENG Jinwen, QU Wenbo. Improved adaptive crow search algorithm based on passive location [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition),2021,33(03):372-377.

[8] 张正,柳亚男,王雷,等.针对不规则网络的高精度和高效率的多跳定位算法[J].信息网络安全,2021,21(06):11-18.
ZHANG Zheng, LIU Yanan, WANG Lei, et al. An accuracy and efficiency multi-hop localization for irregular network [J]. Netinfo Security,2021,21(06):11-18.

[9] ZHANG F,LIU Q Y,LIU Y L,et al.Novel fault location method for power systems based on attention mechanism and double structure GRU neural network [J].IEEE Access,2020,8:75237-75248.

[10] Jiang J, Wang J, Kong B, et al. On the Survey of Network Attack Source Traceback [J]. Journal of Cyber Security, 2018, 54(07): 77-81.

[11] 高美凤,尹持俊.基于 UAV 的无线传感器网络加权质心定位算法[J].传感技术学报,2021,34(04):539-545.
GAO Meifeng, YIN Chijun. UAV-based weighted centroid localization algorithm for wireless sensor networks [J]. Chinese Journal of Sensors and Actuators, 2021, 34(04): 539-545.

[12] 王磊,刘利利,齐俊艳,等.基于高斯滤波的三维水声无线传感网络节点定位算法[J].河南理工大学学报(自然科学版),2021,40(04):147-153+161.
WANG Lei, LIU Lili, QI Junyan, et al. Node location algorithm for 3D underwater acoustic wireless sensor network based on Gaussian filter [J]. Journal of Henan Polytechnic University (Natural Science), 2021, 40(04): 147-153+161.

[13] 龚森,刘年,蒋健.一种电力巡检机器人控制系统设计与实现[J].信息技术,2020,44(03):159-162.
GONG Sen, LIU Nian, JIANG Jian. Design and implementation of electric power inspection robot control system [J]. Information Technology, 2020, 44(03): 159-162.

[14] 于然,于蒙,赵子兰,等.电力 SDH 通信网自愈模型实现网络安全分析[J].信息技术,2020,44(11):148-151+158.
YU Ran, YU Meng, ZHAO Zilan, et al. Analysis of self-healing model of electric power SDH communication network to realize network security [J]. Information Technology, 2020, 44(11): 148-151+158.

[15] 杨宇皓,张益辉,李井泉,等.基于增强现实技术的电力通信网络可视化研究[J].信息技术,2020,44(04):111-114+120.
YANG Yuhao, ZHANG Yihui, LI Jingquan, et al. Visualization of power communication network based on augmented reality [J]. Information Technology, 2020, 44(04): 111-114+120.

[16] 李荷婷,冯仁君,陈海雁,等.基于异卷积神经网络的入侵检测[J].计算机与现代化,2019,(10):121-124+130.
Li heting, Feng Renjun, Chen Haiyan, et al. Intrusion Detection Based on Heterogeneous Convolutional Neural Network [J]. Computer and Modernization, 2019, (10): 121-124+130.

[17] 李元诚,曾婧.基于改进卷积神经网络的电网假数据注入攻击检测方法[J].电力系统自动化,2019,43(20):97-104.
LI Yuancheng, ZENG Jing. Detection method of false data injection attack on power grid based on improved convolutional neural network [J]. Automation of Electric Power Systems, 2019, 43(20): 97-104.

[18] 向敏,饶华阳,张进进,等.基于图卷积神经网络的软件定义电力通信网络路由控制策略[J].电子与信息学报,2021,43(02):388-395.
XIANG Min, RAO Huayang, ZHANG Jinjin, et al. Software-defined power communication network routing control strategy basedon graph convolution network [J]. Journal of Electronics & Information Technology, 2021, 43(02): 388-395.

[19] 罗云,高艳宏,王志强. 基于大数据的电力通信网络风险辨识与评估方法研究[J].电力大数据,2019,22(11):64-69.
LUO Yun, GAO Yanhong, WANG Zhiqiang. Research on risk identification and assessment method of electric power communication network based on big data [J]. Power Systems and Big Data, 2019, 22(11): 64-69.

[20] 周孝信, 史东宇, 陈勇,等. 基于卷积神经网络的电力系统暂态稳定预防控制方法[J].电力系统保护与控制,2020,48(18):1-8.
ZHOU Xiaoxin, SHI Dongyu, CHEN Yong, et al. A preventive control method of power system transient stability based on a convolutional neural network [J]. Power System Protection and Control, 2020, 48(18): 1-8.

[21] 李洋麟,江全元,颜融,等.基于卷积神经网络的电力系统小干扰稳定评估[J].电力系统自动化,2019,648(02):50-57.
LI Yanglin, JIANG Quanyuan, YAN Rong, et al. Small-signal stability assessment of power system based on convolutional neural network [J]. Automation of Electric Power Systems, 2019, 648(02): 50-57.

[22] 苗春雨,李晖,葛凯强,等.基于一维卷积神经网络的 WSN 多攻击行为判别研究[J].网络空间安全,2020,125(07):109-116.
Miao Chunyu, Li Hui, Ge Kaiqiang et al. Research on WSN multi-attack behavior discrimination based on one-dimensional convolutional neural network [J]. Information Security and Technology, 2020, 125(07): 109-116.

[23] 滕志鹏,梁远升,曾德辉,等.基于卷积神经网络的高压输电线路故障定位时域法[J]. 广东电力,2021, 34(06):1-9.
TENG Zhipeng, LIANG Yuansheng, ZENG Dehui, et al. Time domain method for fault location of high voltage transmission line based on convolutional neural network [J]. Guangdong electric power, 2021, 34(06): 1-9.

[24] 曹阳,王金明,徐程骥,等.基于 PID 和深度卷积神经网络的辐射源识别方法[J].数据采集与处理, 2020,35(04):664-671.
CAO Yang, WANG Jinming, XU Chengji, et al. Emitter recognition method based on PID and deep convolution neural network [J]. Journal of Data Acquisition and Processing, 2020, 35(04): 664-671.

[25] 陆世豪,祝云,周振茂.基于多头注意力循环卷积神经网络的电力设备缺陷文本分类方法[J].广东电力,2021,34(06):30-38.
LU Shihao, ZHU Yun, ZHOU zhenmao. Text classification model of power equipment defects based on multi head attention RCNN [J]. Guangdong electric power, 2021, 34(06): 30-38.

[26] CHENG F, JIA G, YANG J, et al. Readback error classification of radiotelephony communication based on convolutional neural network [C]. Chinese Conference on Biometric Recognition. Springer, Cham, 2018, 36(07): 67-73.

[27] 孙子文,朱颖.工业无线传感器网络攻击源定位任务分配优化算法[J].信息与控制,2020,49(02):225-232.
SUN Ziwen, ZHU Ying. Industrial wireless sensor network attack source location task assignment optimization algorithm [J]. Information and Control, 2020, 49(02): 225-232.

[28] LAI Y, ZHANG J, LIU Z. Industrial anomaly detection and attack classification method based on convolutional neural network [J].

Security and Communication Networks,2019,2019(09) : 1-11.
[29] KHAN A S, CHATZIGEORGIOU I, ZHENG G, et al. Random linear network coding based physical layer security for relay-aided device-to-device communication[J]. IET Communications, 2020, 14(07) : 1155-1161.
[30] WANG X, WAQAS M, TU S, et al. Power maximization technique for generating secret keys by exploiting physical layer security in wireless communication[J]. IET Communications, 2020, 14(05) : 872-879.

收稿日期: 2022 年 1 月 22 日

作者简介:

严彬元 (1989) , 男, 本科, 工程师, 主要从事信息安全、信息安全防护体系工作。

(本文责任编辑: 施　玉)

Location Method of Attack Source in Power Communication Network Based on Convolutional Neural Network

YAN Binyuan, WANG Haoran, ZHOU Zeyuan

(Information Center of Guizhou Power Grid Co., Ltd., Guiyang 550002 , Guizhou, China)

Abstract: In order to improve the accuracy and convergence speed of attack source location in power communication network, an attack source location method based on convolutional neural network is proposed. The first-order spatial regression model is used to analyze the spatial structure characteristics of the target equipment of the power communication network, the vibration wave model is used to determine the large-scale spatio-temporal change trend of the attack source, and the first-order autoregressive model is used to determine the small-scale spatio-temporal change trend. On this basis, the state equation of the power communication network attack source model is derived by using stirling interpolation formula, and the power communication network attack sources are aggregated. The two player attack defense game model is used to calculate the utility of network attack and network defense strategy, judge the utility of attack and defense, and evaluate the security of power communication network; and determine the entropy change rate threshold of power communication network, calculate the network entropy change rate, relative entropy and network packet baseline probability distribution, and design the power communication network attack detection steps to detect network attacks. According to the convolution neural network structure, the network activation function is selected. Through the network forward and back propagation, the network data categories are divided, the power communication network topology is determined, the network attacker and the attacked node are selected, and the attack source is located. Experimental results show that the proposed method can effectively improve the location accuracy of attack sources.

Key words: convolutional neural network; power communication; communication network; network attack; source location; positioning method