Key Information Warning for Random Attacks on Vulnerable Surfaces in Cellular Fiber Optic Sensing Networks*

LIU Tao[1*], XIE Linxu[2], YE Jun[1]
(1.School of Information Technology, Guangxi Police College, Nanning Guangxi 530028, China;
2.Network Information Center, Nanning Normal University, Nanning Guangxi 530001, China)

Abstract: The characteristic of random attacks on fiber optic sensing networks is that the attack behavior and time are unpredictable. In cellular fiber optic sensing networks, random attacks cause sensors to output abnormal signals similar to normal environmental changes. The attack patterns are diverse and difficult to distinguish, reducing the accuracy of attack information recognition. Therefore, a method for warning critical information of random attacks on vulnerable surfaces of the network is proposed. Key nodes and links in the network are used as potential vulnerable surfaces, key information of random attacks on vulnerable surfaces is collected through identity authentication technology. Word vector deep learning models are used to identify random attack types on vulnerable surfaces of cellular fiber optic sensing networks. The generated word vectors are input into support vector regression (SVR) and grid based multi resolution clustering (STING) warning models to identify multi style attack patterns and achieve random attack warning for vulnerable surfaces. The simulation results show that the designed method has a false alarm rate of less than 0.5 in all five random attacks, and performs well in the recognition accuracy index.

Key words: fiber optic sensing network; random attack warning; word vector deep learning model; support vector regression
EEACC: 7230 **doi**: 10.3969/j.issn.1004-1699.2026.09.015

蜂窝形光纤传感网络脆弱面随机攻击关键信息预警*

刘 涛[1*], 谢林栩[2], 叶 俊[1]
(1.广西警察学院信息技术学院, 广西 南宁 530028; 2.南宁师范大学网络信息中心, 广西 南宁 530001)

摘 要: 光纤传感网随机攻击的特点为攻击行为和时间不可预测。在蜂窝形光纤传感网中, 随机攻击使传感器输出类似正常环境变化的异常信号, 攻击模式多样难区分, 降低攻击信息识别正确性, 因此提出网络脆弱面随机攻击关键信息预警方法。以网络中的关键节点和链路为潜在的脆弱面, 通过身份认证技术对脆弱面随机攻击的关键信息实施采集。利用词向量深度学习模型来辨识蜂窝形光纤传感网络脆弱面的随机攻击类型。将生成词向量输入至支持向量回归(Support Vector Regression, SVR)与基于网格的多分辨率聚类(STING)预警模型中, 识别多样式攻击模式, 实现脆弱面随机攻击预警。仿真结果表明, 设计方法在五种随机攻击中的虚警率均低于 0.5, 识别正确指数上均表现出色。

关键词: 光纤传感网络; 随机攻击预警; 词向量深度学习模型; 支持向量回归
中图分类号: TP39.08 **文献标识码**: A **文章编号**: 1004-1699(2026)09-2045-07

蜂窝形光纤传感网络是一种高度集成的传感系统, 其通过光纤将大量分布式传感器节点连接起来, 形成一个类似蜂窝结构的网络。这种网络在环境监测、安全监控、工业自动化等领域有着广泛的应用[1]。然而, 随着网络的复杂性和规模的增加, 也面临着越来越多的安全威胁, 尤其是随机攻击。随机攻击的特点是攻击行为和时间难以预测, 使得防御机制的设计变得非常困难[2-3]。在蜂窝形光纤传感网络中, 随机攻击会导致传感器输出异常信号, 这些信号与正常环境变化信号在形式上相似, 从而使得攻击模式多样化且难以区分, 导致攻击信息的识别正确性降低。因此, 深入研究网络脆弱性特征, 建立有效的随机攻击预警机制, 成为当前保障网络信息安全、提升系统鲁棒性的重要课题。

当前网络攻击预警的研究现状呈现出多维度、高复杂性的特点。其中, 文献[4]融合了统计解析、人工智能机器学习及深度数据挖掘等多重数据分析手段, 对网络入侵行为进行全方位、细致化剖析。由

项目来源: 2021 年中国高校产学研创新基金——新一代信息技术创新项目课题项目(2021ITA11006)
收稿日期: 2024-08-22 **修改日期**: 2024-09-29

于多重数据分析手段所需运行资源较多,导致该技术的即时反应能力较差。文献[5]聚焦于警报信息的整合优化处理层面,构建了基于攻击流程演变逻辑的预警机制。并在 Linux 操作系统平台上,通过 C 语言编程实现,将理论构想转化为实际运行的预警算法。该机制依赖于对攻击流程的深入理解,但现实中的网络攻击往往具有复杂性和不确定性,难以准确预测所有可能的攻击路径和演变逻辑。文献[6]提出了分布式网络日志管理与分析策略模型,给出了基于该模型的指示预警系统的模型和设计方法。然而,分布式网络日志的收集、存储和分析面临数据一致性、延迟和可扩展性等多方面的挑战。同时,不同系统间日志格式的差异导致信息整合困难,进而影响预警的准确性和时效性。文献[7]深入分析了分布式异构网络环境,提出一种创新的恶意攻击追踪与预警体系。利用 CVSS 评估体系量化网络威胁的严重程度,引入灰色系统理论中的关联分析法,构建灰色关联模型,对评估要素实施数值转换。搜集、整合日志、事件、警告及关键证据信息,构建全面的证据库。融合 TOP-K 优选策略,实现对分布式异构网络中恶意攻击的高效预警。虽然结合了 CVSS 评估体系和灰色系统理论,但在实际应用中面临评估要素量化不准确、灰色关联模型构建复杂度高以及证据库构建困难等问题。

针对光纤传感网随机攻击的不可预测性和在蜂窝形网络中攻击模式难区分的问题,以关键节点和链路为脆弱面,用身份认证技术采集攻击关键信息,借词向量深度学习模型辨识攻击类型,将词向量输入 SVR 与 STING 模型识别攻击模式。仿真显示,该方法在五种随机攻击中虚警率低、识别正确指数佳,为预警提供新思路。

1 蜂窝光纤传感网随机攻击预警方法设计

1.1 光纤传感网络随机攻击种类确定

蜂窝形光纤传感网络中的传感器节点分布广泛,形成一个密集的网络,这种分布式特性使得防御者难以确定关键节点。并且,随机攻击会产生异常信号,其与正常环境变化信号相似,从而增加了攻击种类确定的难度,难以实现攻击识别。为了提高攻击信息预警的准确性,需要分析随机攻击种类,构建更加全面的预警策略。

通过身份认证技术,实时监控和采集网络中的关键信息,以便及时发现异常行为。其中,关键节点和链路承载着重要的信息传输任务,是网络的核心组成部分。一旦这些节点或链路受到攻击,会导致整个网络的功能受损或信息传输中断。以网络中的关键节点和链路为潜在的脆弱面,通过模拟 Cookie 的运行机制,采集脆弱面随机攻击的关键信息流程如图 1 所示[8]。

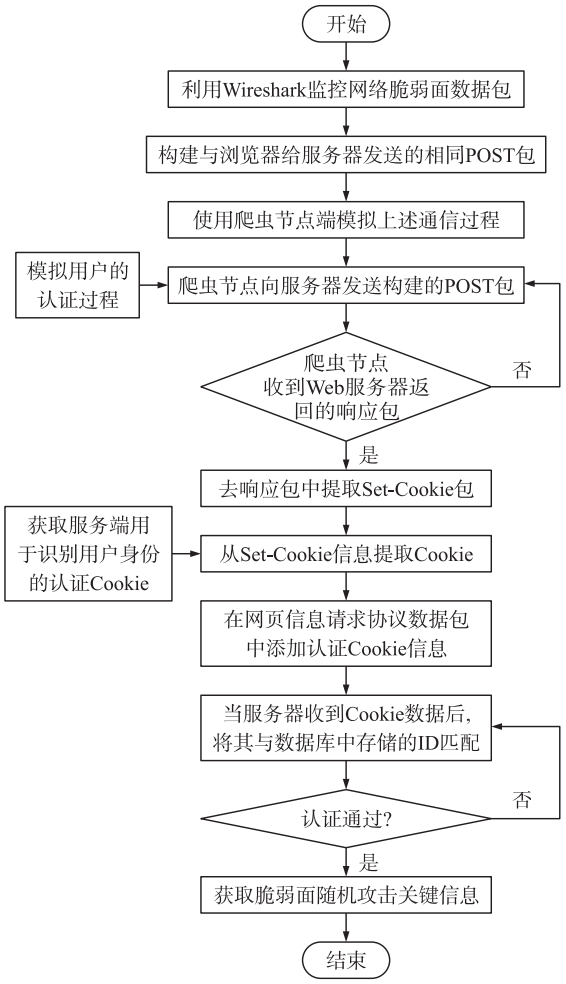

图 1 随机攻击关键信息采集流程图

步骤 1 使用 Wireshark 监控与分析网络流量。Wireshark 是一款功能强大的网络分析工具,利用它设置捕获过滤器,将焦点集中在目标服务器的 IP 地址和端口上,这样可以精准地捕获到用户通过浏览器与服务器之间的 HTTP/HTTPS 通信。

步骤 2 根据分析得到的 POST 请求信息,使用编程工具构造相同的 POST 请求。然后将构造好的 POST 请求发送给服务器,服务器会做出相应的响应。从服务器响应中的 POST 中的 Set-Cookie 字段提取 Cookie 值,并对提取的 Cookie 值进行解析。之后,将解析得到的 Cookie 值与数据库中存储的用户 ID 进行匹配,以此来验证认证是否成功。

步骤 3 在认证通过之后,利用爬虫访问服务器的脆弱面。爬虫可以按照预定的规则自动获取服务器上的数据,通过这种方式能够提取到关键信息。这些关键信息对于及时发现网络中的异常行为具有

重要意义,为后续的随机攻击预警提供了重要的数据支持。

通过上述流程,能够有效地采集到脆弱面随机攻击的关键信息,从而为构建全面的预警策略奠定基础,以应对蜂窝形光纤传感网络中的随机攻击问题。

依据采集的脆弱面随机攻击关键信息,采用混合词向量深度学习模型来辨识蜂窝形光纤传感网络脆弱面的随机攻击类型[9]。结合循环神经网络的序列处理能力与卷积神经网络的高效特征提取能力,将该模型构建为两个并行子网络的结构:一个处理字符级词向量,另一个则针对双字符组词向量。将采集的脆弱面随机攻击关键信息作为输入,并将其转换为字符和双字符组序列,通过词嵌入层生成词向量[10]。这些向量经卷积神经网络提取特征,最终在全连接层整合信息,输出攻击类别分类结果。

由于蜂窝形光纤传感网络中的关键信息包含复杂的模式和结构,单一粒度的特征提取无法全面捕捉这些信息。为深度解析随机攻击关键信息的文本结构,使用词嵌入层集成双轨并行的词向量处理路径,即一轨专注于字符级,另一轨则面向双字符组级,通过预处理采集的脆弱面随机攻击关键信息字符串,并将其转化为两个不同维度的序列表示一字符序列与双字符组序列,并调整至统一的最大长度。通过生成字符级和双字符组级的词向量 $\boldsymbol{\theta}_1$、$\boldsymbol{\theta}_2$,同时从细粒度和粗粒度两个层面提取特征。其中,$\boldsymbol{\theta}_1$ 表示基于单个光纤传感器节点采集到的原始数据(如光强、相位、频率等)经过初步处理得到的低层特征向量;$\boldsymbol{\theta}_2$ 表示更高层次的特征,用于捕捉更复杂的网络状态异常模式。生成两种粒度的词向量表达:

$$\boldsymbol{\theta}_1=\boldsymbol{L}_1^{\mathrm{T}}Y_{U_1} \tag{1}$$

$$\boldsymbol{\theta}_2=\boldsymbol{L}_2^{\mathrm{T}}Y_{U_2} \tag{2}$$

式中:Y_{U_1} 表示光纤传感网络中单个传感器的原始数据序列;Y_{U_2} 表示基于原始数据序列构建的更高级别的数据序列;$\boldsymbol{L}_1^{\mathrm{T}}$ 表示将单个传感器的数据映射到高维空间中的向量表示;$\boldsymbol{L}_2^{\mathrm{T}}$ 表示将两个相邻时间点的数据组合后得到的向量表示。

蜂窝形光纤传感网络中的数据具有局部相关性,针对随机攻击关键信息的词向量一维特征,选用一维卷积神经网络(One-Dimensional-Convolutional Neural Network,1D-CNN)挖掘出隐藏在随机攻击中的复杂模式[11],结合长短期记忆(Long Short-Term Memory,LSTM)网络解析这些特征中的时序依赖,并通过 Dropout 减轻过拟合,实现了网络的正则化[12]。

蜂窝形光纤传感网络面临多种不同类型的随机攻击,全连接层的灵活性允许模型适应不同的输入特征维度,使得预警系统能够适应不同的攻击模式,提高其泛化能力和适应性。全连接层可以连接所有输入与输出节点,整合全局与局部词向量特征,精准识别分类攻击。训练中,网络学习从 $\boldsymbol{\theta}_1$、$\boldsymbol{\theta}_2$ 两种粒度的词向量提取关键信息,映射至相应攻击类别,实现攻击种类的准确判定。

1.2　SVR 结合 STING 下蜂窝光纤安全预警

蜂窝形结构中的每个六边形单元都是一个独立的传感单元,网络具有高度的冗余性,即使部分单元受到攻击,其他单元仍能继续工作,从而增加了攻击者确定关键攻击点的难度。然而,根据 1.1 小节可知,随机攻击模式具有多样性的特点,单一的预警方法不足以覆盖所有的攻击节点和链路。而 SVR 与基于网格的 STING 预警模型具有独特的优势。

SVR 具有强大的非线性映射能力,能够处理复杂的数据关系。在应对随机攻击时,可以通过对历史攻击数据和正常运行数据的学习,构建一个能够区分正常与异常的模型。即使面对未知的攻击模式,由于其对数据内在关系的挖掘能力,能够在一定程度上对新出现的攻击模式进行识别。而基于网格的 STING 预警模型则擅长对数据进行聚类分析。在蜂窝形光纤传感网络中,可以根据传感器节点的数据特征进行聚类。对于随机攻击产生的异常数据,由于其与正常数据在特征上存在差异,STING 能够通过聚类分析将其与正常数据区分开来。而且,STING 的多分辨率特性使其能够在不同的细节层次上对数据进行分析,这有助于应对攻击模式的多样性。

通过将 SVR 和 STING 结合应用于蜂窝形光纤传感网络脆弱面随机攻击的预警中,可以提高预警模型对未知攻击模式的适应性和鲁棒性,从而更有效地预警随机攻击。通过五元组形式化描述蜂窝形光纤传感网络入侵事件:

$$Q=\{W,Y,U,I,O\} \tag{3}$$

式中:U 是指发起攻击的传感节点的标识符;I 是指随机攻击的目标传感节点标识符;O 是指攻击所针对的网络服务类型,如光纤传感数据采集、传输控制、信号处理等关键服务;W 是指随机攻击频率;Y 是指攻随机攻击的具体形式,如非法接入、信号劫持、中间人攻击、数据篡改等。

通过上式表示入侵事件后,采用 STING 技术实施聚类分析,该技术计算与查询操作相互独立,将其整合至预警模型中,可提升预警响应速度[13]。因此,通过生成的两种粒度词向量 $\boldsymbol{\theta}_1$、$\boldsymbol{\theta}_2$,可以识别出攻击行为中频繁出现的字符对或序列片段,进一步推断出攻击的频度。启动多维扫描流程,从一维逐

步深入至高维事件数据库,筛选满足最小频次阈值的事件集,代表网络中特定模式或异常。记录各维度符合标准的事件集数组标识,类似蜂窝网络信息编码传递。这些标识含关键信息,高效传播处理,确保快速响应潜在威胁。通过上述步骤获得的攻击频度序列,基于攻击频度序列,实现对网络脆弱面随机攻击的预警。引入 SVR 算法,在攻击频度序列的特征空间 H 上构建线性回归函数:

$$F(\boldsymbol{X})=\frac{Q\times[\boldsymbol{S}^t\psi(\boldsymbol{X})+c]}{\boldsymbol{\theta}_1+\boldsymbol{\theta}_2} \tag{4}$$

式中:$\boldsymbol{S}^t$ 是指光纤传感网络面临的各种潜在攻击模式的特征集合;$\psi(\boldsymbol{X})$ 是指输入向量 $\boldsymbol{X}$ 即攻击频度序列由原空间至 H 的攻击频度序列;c 用于调整攻击检测模型的灵敏度[14]。

通过求解上式实现攻击事件预警,在求解中需要寻找 $\boldsymbol{S}^t$ 与 c。在蜂窝形光纤传感网络中,每个蜂窝单元独立感知处理信息,汇聚至中心节点进行分析。SVR 采取的是一次性整体输入并成批计算的策略[15],而成批计算在面对大数据集时导致计算冗长,影响实时响应。针对 SVR 在处理大数据集时计算过程冗长的问题,引入松弛因子 σ_i,且其转置 $\sigma_i^*\geqslant 0$,通过引入松弛因子 σ_i 来调整模型的容错能力,实现对局部环境变化的适应性调整。实施攻击事件预警时,这种改进的 SVR 模型可以快速识别异常模式,并及时发出预警信号。求解下式的优化问题:

$$\begin{cases}\min\rho(\boldsymbol{S}^t,\sigma_i,\sigma_i^*)=\dfrac{1}{2}\boldsymbol{S}^{t2}+V(\sigma_i+\sigma_i^*)\\ \text{s,t}\begin{cases}\sigma_i,\sigma_i^*\geqslant 0,i=1,2,\cdots,m\\ \{\boldsymbol{S}^t\psi(\boldsymbol{X})+c\}-p_i\leqslant\kappa+\sigma_i^*\\ p_i-[\boldsymbol{S}^t\psi(\boldsymbol{X})+c]\leqslant\kappa+\sigma_i^*\end{cases}\end{cases} \tag{5}$$

式中:$\min\rho(\boldsymbol{S}^t,\sigma_i,\sigma_i^*)$ 表示光纤传感网络的安全性优化目标;V 表示针对导致网络瘫痪攻击的惩罚系数;p_i 表示不同的攻击类型、故障模式和正常状态的训练样本;κ 表示线性函数拟合的精度,m 表示随机攻击关键信息总量。

蜂窝形光纤传感网络的特点是每个蜂窝单元(即传感器节点)都能够独立地感知和处理局部信息,并将这些信息汇聚到中心节点进行综合分析。因此,利用核函数技术和拉格朗日乘子法对上式实施变形处理,获得回归函数,具体如下式所示:

$$F'(\boldsymbol{X})=(b_i-b_i^*)\times R(x_i,\boldsymbol{X})+c \tag{6}$$

式中:$R(x_i,\boldsymbol{X})$ 是指核函数;b_i、b_i^* 是指拉格朗日乘子。

在 SVR 的优化问题构建中,旨在最小化一个目标函数,同时受到一些约束条件的限制。设目标函数为 J,约束条件可分为不等式约束 $g_i(x)\leqslant 0$ 和等式约束 $h_j(x)=0$。KKT 条件包括以下几个方面:①原始可行性:约束条件 $g_i(x)\leqslant 0$ 和 $h_j(x)=0$ 必须满足。在 SVR 中,这意味着与拉格朗日乘子相关的约束条件必须成立。②对偶可行性:拉格朗日函数关于变量 x 的梯度为零,确保了在满足约束条件下目标函数的最优性。③互补松弛性:$b_ig_i(x)=0$,这一条件在 SVR 中确保了拉格朗日乘子与约束条件之间的平衡关系,使得在最优解处,只有起作用的约束对应的拉格朗日乘子不为零。

通过满足 KKT 条件,可以确保式(6)中的优化问题得到的解是全局最优的,并且满足所有的约束条件。基于这个满足 KKT 条件的全局最优解得到的回归函数,回归函数能够捕捉到随机攻击关键信息中的细微变化,并及时识别出潜在的攻击行为,从而在攻击发生之前发出预警。因此,以 KKT 条件为依据,设执行至第 l 步,用 $\mathbf{SV}_l$ 表示支持向量集合,得到如下式的回归函数:

$$F_l(\boldsymbol{X})=F'(\boldsymbol{X})\,|\mathbf{SV}_l|\,R(x_i,\boldsymbol{X})+c \tag{7}$$

针对蜂窝形光纤传感网络中的随机攻击,通过身份认证和实时监控采集关键节点与链路信息,利用混合词向量深度学习模型结合 1D-CNN 和 LSTM 网络提取复杂模式及时序依赖,实现对随机攻击种类的精准识别。利用 STING 高效聚类分析识别异常模式,同时引入 SVR 算法构建基于攻击频度序列的线性回归模型,利用核函数和拉格朗日乘子法优化 SVR 模型,确保全局最优解,实现对随机攻击的精准预警。

2 仿真分析

2.1 蜂窝形光纤传感网络搭建

为了验证蜂窝形光纤传感网络在面临随机攻击时其脆弱面的关键信息预警系统的有效性,采用 OPNET Modeler 仿真工具搭建蜂窝型多点光纤传感网络架构,如图 2 所示。

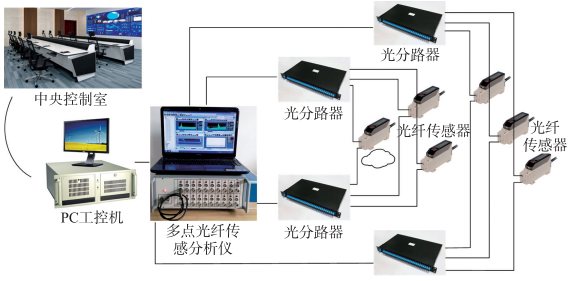

图 2 蜂窝形光纤传感网络架构图

在图 2 所示的蜂窝形光纤传感网络架构中,中央控制室作为指挥中心,通过 PC 工控机进行数据处理和系统控制;多点光纤传感分析仪负责接收和分析来自多个光纤传感器的数据,这些传感器分布在网络的各个节点,用于监测环境变化或异常信号。光分路器则扮演着数据分流的角色,将来自传感器的信号分发至分析仪进行处理。各个组件之间通过光纤连接,形成一个高效的信息传输和处理网络,确保了整个系统对环境变化的快速响应和准确分析。

该传感网络中的光纤传感器节点负责采集环境数据(如振动、温度等)。设定网络中部署了多个光纤传感器节点,均匀分布在蜂窝网络的各个小区内。每个节点平均间距为 500 m,以保证良好的覆盖和数据采集密度。根据网络覆盖区域大小,假设设置 7 个蜂窝基站,每个基站覆盖一个六边形小区,小区半径约为 1 km。每个基站具备处理每秒 10 GB 数据流量的能力。假设每个小区内平均有 50 个 D2D 用户设备。每个 D2D 设备能与周围最多 5 个其他 D2D 设备或基站直接通信,通信半径约为 100 m。D2D 通信速率可达 10 Mbps。

在网络中的关键节点和链路中,使用随机数生成器随机选择攻击目标。确保每次验证的攻击目标都是随机且不可预测的,以模拟真实场景中的随机攻击。

2.2　仿真参数设置

通过身份认证对脆弱面随机攻击的关键信息实施采集,采集的部分信息如表 1 所示。

利用设计的混合词向量深度学习模型来辨识蜂窝形光纤传感网络脆弱面的随机攻击类型。将部分采集数据作为训练数据,实施模型训练。将初始学习率设定为 0.001、字符级词嵌入维度为 128、最大序列长度为 46 双字符组。1D-CNN 层卷积核数量为 256、卷积核大小为 4、LSTM 单元数量为 256、Dropout 比例为 0.1。

表 1　采集的部分信息

序号	攻击时间	攻击目标节点 ID	攻击强度	采集信息类型
1	2023-04-01 12:00:00	Node001	低	振动变化
2	2023-04-01 12:15:00	Node037	高	温度异常
3	2023-04-01 12:30:00	Node074	突发	湿度数据丢失
4	2023-04-01 12:45:00	Link01-02	轻微	压力数据中继
5	2023-04-01 13:00:00	Node101	攻击强度	振动频率变化

利用设计的融合 SVR 与 STING 的预警模型实现仿真蜂窝形光纤传感网络的安全预警。STING 算法的最小频次阈值的总事件数为 1%、SVR 算法的线性函数拟合的精度为 0.5、偏置项为 0.1。

2.3　预警结果分析

不同的攻击种类对网络的影响和破坏程度不同。根据波段运行频率,确定具体的攻击种类,可以针对性地测试预警系统对各种攻击的响应能力和准确性,有助于发现预警系统在应对特定类型攻击时的弱点,从而进行针对性的改进和优化。采用所提方法确定随机攻击种类,结果如图 3 所示。

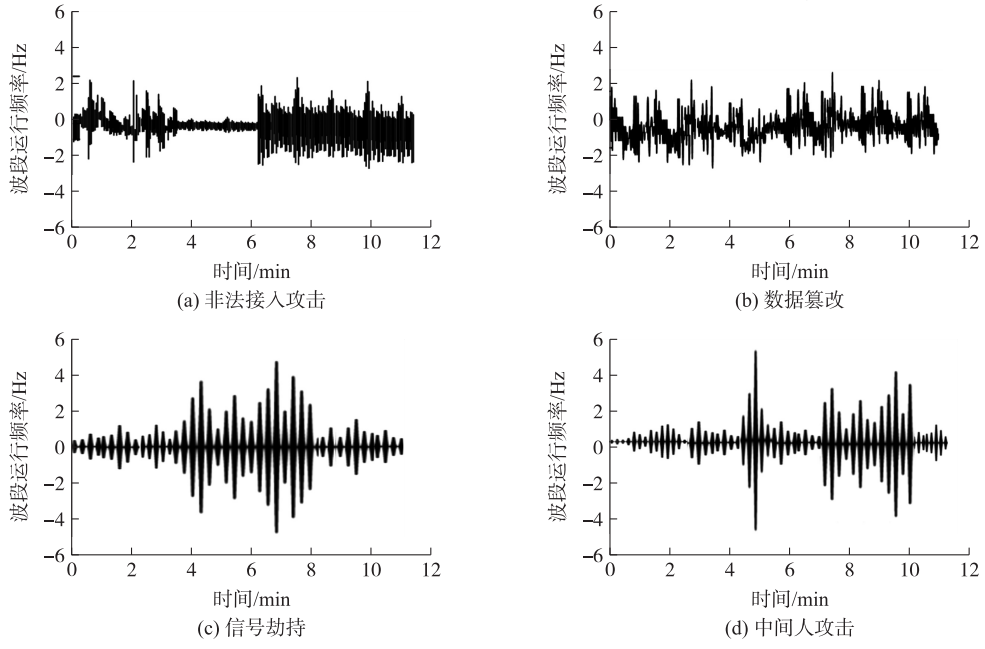

图 3　所提方法随机攻击种类确定

图 3 展示了不同攻击种类在蜂窝形光纤传感网络中的分布情况。从图中可以看出,信号劫持、中间人攻击的波动频率较高,反映了实际网络环境中攻击种类的多样性和复杂性。这是因为所提方法采用了身份认证技术,监控网络中的关键节点和链路,有效地采集到了脆弱面随机攻击的关键信息,从而揭示不同攻击种类在蜂窝形光纤传感网络中的分布情况。

以虚警率、识别正确指数作为预警性能的评价指标,将文献[6]提出的分布式网络日志管理方法、文献[7]提出的灰色系统理论方法作为对比方法。设计方法与两种对比方法的虚警率结果如图 4 所示。

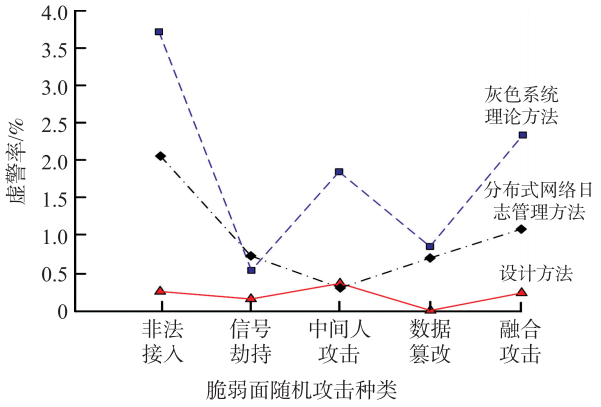

图 4 虚警率结果

设计方法在五种随机故障中的虚警率均低于 0.5%,这是由于设计方法通过身份认证对关键信息实施采集,确保了数据的真实性和可靠性。这为后续的模型训练和预测提供了坚实的基础,减少了数据质量问题导致的识别错误。同时利用设计的混合词向量深度学习模型实施随机攻击类型识别,能够获得准确的识别结果,并结合 SVR 与 STING 融合模型的预测能力,因此实现了较低的虚警率。总体得益于深度学习模型对复杂数据的高效处理能力以及 SVR 和 STING 在回归和聚类分析方面的优势结合。分布式网络日志管理方法在五种随机故障中的虚警率居中,其中在非法接入故障中的虚警率最高。灰色系统理论方法在五种随机故障中的虚警率最高,其中在非法接入故障与协议漏洞利用故障中的虚警率最高。

识别正确指数结果如表 2 所示。从表中可以看出,设计方法在五种随机故障的识别正确指数上均表现出色,显著高于分布式网络日志管理方法和灰色系统理论方法。这表明设计方法在辨识蜂窝形光纤传感网络脆弱面的随机攻击类型时具有更高的准确性。因为设计方法采用的深度学习模型可以通过多层次的非线性变换,捕捉到数据中的深层次特征,将词向量深度学习模型的输出作为 SVR 和 STING 模型的输入,能够从不同角度和层次上对故障进行识别,提高了整体的识别准确性。

表 2 识别正确指数结果

方法	识别正确指数/%				
	非法接入	信号劫持	中间人攻击	数据篡改	融合攻击
设计方法	97.0	96.5	95.8	95.8	97.5
分布式网络日志管理方法	92.0	90.0	88.5	88.5	92.5
灰色系统理论方法	93.5	91.5	90.0	90.0	93.0

为了进一步全面评估蜂窝形光纤传感网络在面临随机攻击时其脆弱面的关键信息预警的性能,引入了 PR-AUC 值作为关键评估指标。PR-AUC 值越高,表明其预警准确率越高。三种方法的 PR-AUC 曲线结果如图 5 所示。

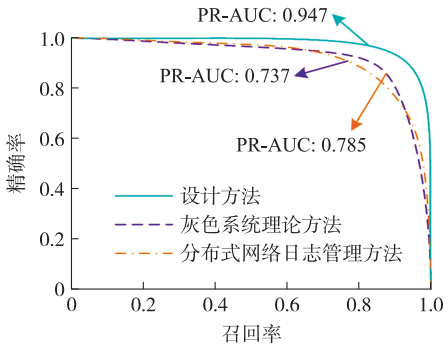

图 5 不同方法 PR-AUC 曲线对比

通过对比分析图 5 中的 PR 曲线结果可知,所提方法的 PR-AUC 值高达 0.947,显著优于其他两种对比方法。这一结果充分体现了所提方法在蜂窝形光纤传感网络脆弱面随机攻击关键信息预警方面的卓越性能。从曲线的走势来看,所提方法在整个召回率的取值范围内,都能保持较高的精确率,这意味着在不同的检测阈值下,该方法都能够较为准确地预警随机攻击。

3 结束语

本研究通过深入分析蜂窝形光纤传感网络的拓扑结构与信号传输特性,结合身份认证与多种深度学习技术,成功构建了针对网络脆弱面的随机攻击预警模型。这一技术创新不仅提升了预警的精准度与即时性,更为后续的网络防御策略制定提供了有力支持。

参考文献:

[1] 徐礼金,贺艳芳. 基于随机森林算法的无线传感网络

攻击流量阻断模型构建[J]. 计算机工程与科学,2022,44(5):819-825.
[2] 张迪,韩铮,王雪丽. 无线传感网络最佳候选节点空洞攻击抑制方法[J]. 传感技术学报,2023,36(6):984-989.
[3] 陈坤定,李隘优. 无线传感网络混合密钥安全分簇方法[J]. 传感技术学报,2023,36(9):1459-1466.
[4] 陈剑彪. 基于新一代防火墙的网络攻击预警分析设计与应用[J]. 信息与电脑,2023,35(15):224-227.
[5] 张常有,杨明华,王振海,等. 基于攻击过程的入侵预警技术研究[J]. 石家庄铁道大学学报(自然科学版),2006,19(3):66-69.
[6] Wen H,W C S,Ou H X. The Distributing Network Attack Indication Warning System Model Base on Analysis Policy of Log Files[J]. Natural Science Journal of Xiangtan University,2004,26(4):39-42.
[7] 高菲. 分布式异构网络恶意攻击取证及预警方法研究[J]. 计算技术与自动化,2021,40(1):184-188.
[8] 夏云舒,王勇,周林,等. 基于改进生成对抗网络的虚假数据注入攻击检测方法[J]. 电力建设,2022,43(3):58-65.
[9] 苏新,张桂福,行鸿彦,等. 基于平衡生成对抗网络的海洋气象传感网入侵检测研究[J]. 通信学报,2023,44(4):124-136.
[10] 刘丹丹,朱鸿飞,李德文,等. 基于科氏质量流量计的微米级煤尘和岩尘颗粒分类方法[J]. 中国粉体技术,2024,30(1):132-143.
[11] 陈锦晶,宋颜培,周荃,等. 冲击载荷对钢骨砼桥墩损伤容限的影响研究[J]. 兵器材料科学与工程,2024,47(1):69-75.
[12] 苗奎星,魏海峰,张懿,等. 基于龙伯格观测器的 PMSM 单相低分辨率位置传感器故障容错控制算法[J]. 江苏科技大学学报(自然科学版),2023,37(1):49-56.
[13] 吴钢,周金辉,李慧. 面向边缘增强分布式电力无线传感网的资源分配[J]. 中国电力,2023,56(8):77-85.
[14] 谭平,毛江峰,丁进,等. 面向接触网状态监测的无线传感网络循环冗余校验多项式性能研究[J]. 中国铁道科学,2023,44(1):177-185.
[15] 王晓丹,王子乔,金山海. 社交网络中用户签到行为位置泄露风险预警[J]. 计算机仿真,2023,40(9):401-405.

刘　涛(1978—),男,汉族,广西警察学院专任教师,高级工程师,中国计算机学会专业会员,中国国际互联网+大赛优秀创新创业导师,主要研究方向为计算机网络安全、高校信息化建设。近年来主持教育部课题《基于物联网的电子实验室教学管理系统建设》,主要参与国家语委课题《民族语言调查·云南屏边壮语》、广西教育厅重点教改课题《产教融合视域下广西职业教育精准服务面向东盟开放合作新高地路径的研究与实践》等科研项目,指导学生参加省级以上比赛获奖 8 项,取得软著 4 项,实用新型专利 9 项,liutao23232024@ 163.com。