恶意攻击下自组织网络安全态势感知算法

白 磊[1] 张 涛[2]
BAI Lei ZHANG Tao

摘 要 在恶意攻击下的网络安全状态数据类内和类间散度差异过大，导致数据降维效果差影响网络安全态势感知。为此，提出恶意攻击下自组织网络安全态势感知算法。采用线性判别分析方法，将原始的高维网络安全状态数据进行降维处理，把原始高维样本数据投影到最佳矢量空间中，找到新的投影方向，然后结合线性变换实现数据降维。考虑网络状态数据的动态发展属性特征，引入RBF神经网络展开态势感知，并利用最小二乘法对RBF神经网络的结构参数进行优化处理，实现对安全态势的精准判断。在测试结果中，设计网络安全态势感知算法对于不同恶意攻击下网络丢包率的感知误差较低，说明其可以准确识别不同类型的攻击，有利于提高网络运行的安全性。

关键词 恶意攻击；自组织网络；安全态势感知；线性判别分析；鉴别矢量空间；数据特征；空间维数

doi：10.3969/j.issn.1672-9528.2024.09.047

0 引言

自组织网络是一种无中央控制的分布式网络，具有高度鲁棒性和灵活性，适用于各种应用场景[1]。然而，随着自组织网络的广泛应用，其面临着日益复杂和多样化的安全威胁，包括恶意攻击、信息泄露和网络拒绝服务等。因此，研究自组织网络安全态势感知算法具有重要的意义[2]。这样的研究旨在通过监测、收集和分析网络中的安全数据和信息，以实时获取网络的安全状态和威胁情报，并利用这些信息来识别恶意活动、发现异常行为和预测潜在的攻击趋势，提高自组织网络的安全性和防御能力。通过有效的安全态势感知算法，可以及时发现并应对恶意攻击，保护自组织网络中的节点和数据安全，确保网络运行的可靠性和稳定性。

周莉等人[3]提出一种基于决策树算法的联级网络安全态势感知方法，通过划分攻击数据类型与切分数据流，构建决策树模型，运用该模型实现安全态势感知。该方法的不足之处是需要大量的标注数据和计算资源，实用性不佳。张红斌等人[4]提出一种基于威胁情报的网络安全态势感知方法，比较外源威胁情报与系统内部安全事件之间的相似度，根据相似度度量结果，结合博弈论感知网络安全态势。实验结果表明，该方法能够实时反映网络安全状态，但是不能对不同的攻击类型实现有效检测。贾一浩[5]提出一种基于FGCM的通信网络运行态势感知方法，采用FGCM算法评价网络运行数据，提取网络态势特征，根据特征提取结果构建态势感知模型。实验结果表明，该方法可以降低网络运行带宽，但是网络数据传输的丢包率较高。丁华东等人[6]提出一种基于贝叶斯方法的网络安全态势感知方法，离散化处理态势指标数据，建立指标分层模型，采用贝叶斯网络逐层融合态势层，获取态势感知结果。该方法的不足之处是恶意攻击的误报率较高。

为了提升网络安全态势感知效果，本文提出一种恶意攻击下自组织网络安全态势感知算法，并设置了对比测试环境，分析验证了设计网络安全态势感知算法的实际应用价值。

1 自组织网络安全态势感知算法设计

1.1 自组织网络状态数据降维

为了能够最大限度实现对恶意攻击下自组织网络安全状态的综合分析，本文首先将原始的高维网络安全状态数据进行降维处理，采用的具体方法为线性判别分析（linear discriminant analysis，LDA）。在具体的实施过程中，主要是通过把原始高维的恶意攻击下自组织网络安全状态特征样本数据投影到最佳的鉴别矢量空间中，最大化各类别之间的差异，最小化类别内部的差异，找到最能代表数据特征的新的投影方向，以此实现数据降维[7]。

原始的高维网络安全状态数据投影后，矢量空间内第 i 类样本的中心点和所有样本的中心点分别表示为：

$$o_i = \frac{1}{n_i}\sum z_i = \frac{1}{n_i}\sum W^T x_i = W^T \mu_i \quad (1)$$

1. 郑州工业应用技术学院信息工程学院 河南郑州 451150
2. 郑州理工职业学院信息工程学院 河南郑州 451100

$$o=\frac{1}{n}\sum z=\frac{1}{n}\sum W^T x=W^T\mu \tag{2}$$

式中 o_i 表示原始的高维网络安全状态数据投影后，矢量空间内第 i 类样本的中心点；o 表示投影后所有样本的中心点；z_i 表示待分类样本的特征向量；n_i 表示第 i 类样本总数；x 表示原始数据；x_i 表示第 i 类样本内部的离散程度；μ_i 表示第 i 类样本的均值；W^T 表示类别之间的离散度。

然后计算矢量空间中每个类别数据的均值向量：

$$\bar{x}=\frac{1}{n_i}\sum_{j=1}^{n} n_i\times x_{ij} \tag{3}$$

式中：x_{ij} 表示第 i 个类别中的第 j 个样本。

基于均值向量计算类内散度矩阵 S_w 和类间散度矩阵 S_b：

$$S_w=\sum_{i=1}^{c}\sum_{j=1}^{n_i}\left(x_{ij}-\bar{x}\right)\left(x_{ij}-\bar{x}\right)^T \tag{4}$$

$$S_b=\sum_{i=1}^{c} n_i\left(\bar{x}-\overline{X}\right)\left(\bar{x}-\overline{X}\right)^T \tag{5}$$

式中：c 表示类别的数量，$\overline{X}$ 表示所有样本的总体均值向量。通过类内散度矩阵和类间散度矩阵计算结果最大化各类别之间的差异，最小化类别内部的差异。

最后根据 S_w 和 S_b 计算新的投影方向：

$$O=\frac{f_v(\max)\times\left(\frac{S_b}{e_v}+\frac{S_w}{f_v}\right)}{o-o_i} \tag{6}$$

式中：e_v 表示特征值，f_v 表示特征向量，f_v(max) 表示特征向量最大值。

利用新的投影方向将原始数据进行线性变换，实现数据的降维，结果可以表示为：

$$y=\left(f_v\right)^O\times x \tag{7}$$

式中：$(f_v)^O$ 表示由选取的特征向量构成的投影矩阵，y 表示降维后的数据。

按照上述所示的方式，实现对自组织网络状态数据的降维处理，为后续的安全态势感知提供可靠的基础。

1.2 考虑动态属性的自组织网络安全态势感知方法设计

在对自组织网络安全态势进行感知的过程中，本文充分考虑了自组织网络状态与其安全态势之间的关系，意识到在恶意攻击下，自组织网络状态数据具有动态发展的属性特征。一般情况下，当自组织网络处于稳定运行状态下时，状态数据是相对稳定的，即在一定的阈值范围内波动[8-9]。但是，当自组织网络处于恶意攻击状态下时，状态数据会呈现出一定的线性发展规律，并且有超出安全阈值范围的趋势。因此，引入 RBF（radial basis function neural network）神经网络，结合状态数据的动态属性，展开网络安全态势感知，利用神经网络的非线性映射特性来处理网络状态数据的动态属性，能够更有效地预测动态属性的发展变化。然后利用最小二乘法对 RBF 神经网络的结构参数进行优化处理，有助于提高神经网络在描述和理解网络状态动态发展属性方面的准确性和适应性，更好地满足网络安全态势感知的需求。

根据 1.1 降维处理后的网络安全状态样本数据，设置 RBF 神经网络的输入层节点数量、输出层节点数量以及对应的最大隐含层节点数量。采用二进制编码配合实数编码的方式，对自组织网络安全状态数据进行编码处理，并将其作为初始种群[10-12]，具体的处理方式可以表示为：

$$p(o_i\to o)=\begin{cases}1\\ \exp\dfrac{f(x_i)-f(x_j)}{T}\end{cases} \tag{8}$$

式中：$p(o_i\to o)$ 表示原始的高维网络安全状态数据投影后，矢量空间内第 i 类样本中心点到所有样本中心点距离为基础的编码结果；$f(x_i)$ 和 $f(x_j)$ 均表示待编码的自组织网络安全状态数据的原始特征。

结合式（8），当原始的高维网络安全状态数据投影后，矢量空间内第 i 类样本中心点与所有样本中心点的距离＜第 i 类样本中心点的类内距离时，编码结果的取值为 1；当原始的高维网络安全状态数据投影后，矢量空间内第 i 类样本中心点与所有样本中心点的距离 ≥ 第 i 类样本中心点的类内距离时，编码结果的取值为 $\exp\frac{f(x_i)-f(x_j)}{T}$。按照这样的方式，实现对自组织网络安全状态数据的编码处理。

在此基础上，使用最小二乘法确定对 RBF 神经网络各层的权值参数进行差异化处理，同样以矢量空间内第 i 类样本中心点与所有样本中心点的距离作为设置基准。那么，对于自组织网络安全态势的感知问题而言，其就转化为了对 RBF 神经网络各层输出结果与允许安全阈值之间关系的判断问题，具体可以表示为：

$$G(t)=\frac{p(o_i\to o)-\lambda}{\sum nx_{ij}(t)} \tag{9}$$

式中：$G(t)$ 表示恶意攻击作用下 t 时刻自组织网络的安全态势；λ 表示网络允许安全阈值，$\sum nx_{ij}(t)$ 表示恶意攻击作用下；t 时刻 RBF 神经网络各层输出结果之和，也就是自组织网络状态数据的拟合结果。需要注意的是，自组织网络的安全态势需要结合攻击状态下的网络状态数据发展进行实时更新。

按照上述所示的方式，实现对自组织网络安全态势的精准感知。

2 实验分析

2.1 测试环境

在对本文设计的恶意攻击下自组织网络安全态势感知算法性能进行分析时，以某自组织网络环境为基础开展了具体的测试。在测试自组织网络环境中，对应的网络拓扑结构采用了 Ad Hoc 网络结构，节点之间通过无线链路直接通信，无需基础设施支持。网络由多个节点组成，每个节点都具有路由和数据传输功能。节点之间形成一个多跳网络，通过协作传输数据。节点是测试网络的基本单元，每个节点都具有相同的硬件和软件配置。表 1 为测试自组织网络的基础配置情况。

表 1 测试自组织网络基础配置情况

编号	配置	参数
1	节点数量	50 个
2	无线通信接口	802.11 g 标准，2.4 GHz 频段
3	通信距离	最大 100 m（视环境因素而定）
4	带宽	20 Mbit/s（单信道）
5	电源管理	节能模式和休眠模式
6	安全机制	AES 加密算法
7	节点连接	无线通信接口连接
8	节点功能	数据传输和路由功能

在上述配置的基础上，测试自组织网络环境中的每个节点都具有以下功能。

（1）数据传输：节点可以发送和接收数据，并能够将数据从一个节点传输到另一个节点。

（2）路由：节点能够根据网络拓扑结构和通信状况选择最佳路径，节点具有自组织能力，可以通过协作形成路由。

（3）能量管理：节点具有能量管理功能，可以监测节点的能量使用情况，并在需要时进行节能操作。

（4）自我修复：节点具有自我修复能力，可以在某些节点出现故障时，通过协作修复网络拓扑结构。

在网络协议配置方面，测试自组织网络采用基于 IP 的通信协议，包括 TCP/IP 和 UDP/IP 协议族。这些协议可以确保数据的可靠传输和正确接收。此外，网络还采用自组织路由协议——OLSR（optimized link state routing）协议，用于节点之间的路由选择和拓扑结构发现。

为了保障网络的安全性和隐私，测试自组织网络采用加密技术保护数据的机密性和完整性，使用 AES（advanced encryption standard）加密算法对数据进行加密。此外，网络还采用访问控制机制，限制未经授权的节点访问网络资源。隐私保护方面，网络采取匿名通信技术，使用 Tor（the onion router）网络来保护用户的隐私。

2.2 恶意攻击设置

在上述测试环境的基础上，设置网络恶意攻击类型，具体如表 2 所示。

表 2 网络攻击设置

攻击类型	攻击方式	作用影响
XSS 攻击	对网络实施跨站脚本攻击，对测试自组织网络设置漏洞，以漏洞为作用点向网络里注入特定代码，使得网络访客执行代码对应的指令信息	入侵账户、激活木马程序、修改网站内容
CSRF 攻击	借助跨站请求的方式，利用合法用户的身份对网络实施非法操作处理	转账交易、发表评论
SQL 注入	将恶意 SQL 命令注入到 HTTP 请求中	修改服务器指令
ARP 攻击	借助伪造的 IP 地址，或者伪造的 MAC 地址，在网络中产生大量的 ARP 通信量	发送伪造的 ARP 响应包来欺骗路由器的 ARP 表

在上述测试环境的基础上，将基于决策树算法的联级网络安全态势感知方法和基于贝叶斯方法的网络安全态势感知方法作为对比方法，与所提算法进行对比分析。

2.3 测试结果与分析

将丢包率作为评价指标，即在网络传输过程中丢失的数据包与总数据包数的比例越高，对应的安全态势越低，在网络传输过程中丢失的数据包与总数据包数的比例越低，对应的安全态势越高。通过与实际丢包率进行比较，分析不同算法的感知效果。具体的测试结果如图 1 所示。

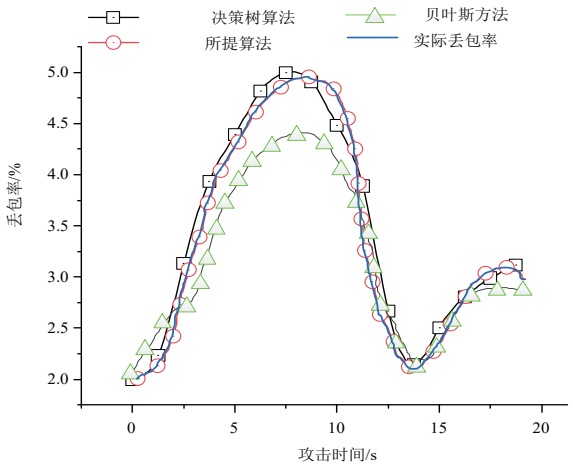

图 1 不同算法的丢包率测试结果对比图

结合图 1 所示的测试结果可以看出，在三种不同网络安

全态势感知算法下，对于测试自组织网络在不同恶意攻击下的丢包率感知结果与实际丢包率之间的关系表现出了较为明显的差异。其中，基于贝叶斯方法的安全态势感知算法，对应的丢包率感知结果与实际丢包率之间差距较大；基于决策树算法的安全态势感知算法下，丢包率感知结果与实际丢包率之间的差距得到了缩小。但是相比之下，还是在本文设计网络安全态势感知算法下，丢包率与实际丢包率更加接近，所提算法具有明显优势，说明所提方法能够精准感知网络安全态势，结果可信度更高。

接下来以误报率为评价指标，误报率是指算法错误地将正常行为识别为恶意行为的比例，较低的误报率可以减少系统管理人员的工作量和干扰。测试结果如图 2 所示。

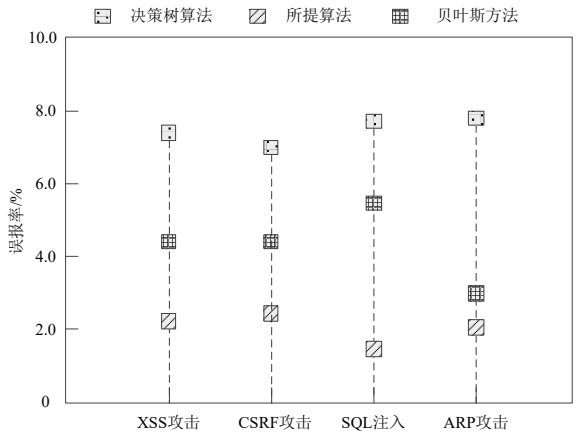

图 2 不同算法的误报率测试结果对比图

结合图 2 所示的测试结果可以看出，针对不同的攻击类型，所提算法的误报率均为最低，其误报率始终低于 3%，说明其能够实现对不同类型攻击的有效识别，提升网络安全感知效果。

综合上述测试结果可以得出，本文设计的恶意攻击下自组织网络安全态势感知算法可以实现对不同类型攻击作用下，网络安全态势情况的精准感知，对于实际的网络安全维护工作具有可靠的指导价值。

3 结语

恶意攻击对网络安全状态具有严重的影响，需要采取有效的措施进行防范和应对。网络安全态势感知在攻击状态下具有重要的实际意义，能够帮助管理员及时发现和处理威胁，提高网络的防御能力和安全性。为此，本文提出恶意攻击下自组织网络安全态势感知算法，通过线性判别分析方法降维处理网络状态数据，基于降维结果，采用 RBF 神经网络开展网络安全态势感知，并利用最小二乘法对 RBF 神经网络的结构参数进行优化处理，提升神经网络对网络状态动态发展属性的适应性。经实验验证可知，该算法实现了对不同状态下网络安全态势的准确分析。借助本文对于网络安全态势感知问题的研究与设计，希望能够为实际的网络安全管理提供有价值的参考。

参考文献：

[1] 张伟 , 纪巍 . 基于 Cyber-net 与无监督学习的电网调度网络安全态势感知方法 [J]. 微型电脑应用 ,2023,39(10):197-200.

[2] 徐植 , 陈俊 , 张智勇 , 等 . 新型电力系统中基于人工免疫和隐马尔可夫的网络安全态势评估 [J]. 华东师范大学学报 (自然科学版), 2023(5):182-192.

[3] 周莉 , 李静毅 . 基于决策树算法的联级网络安全态势感知模型 [J]. 计算机仿真 ,2021,38(5):264-268.

[4] 张红斌 , 尹彦 , 赵冬梅 , 等 . 基于威胁情报的网络安全态势感知模型 [J]. 通信学报 ,2021,42(6):182-194.

[5] 贾一浩 . 基于 FGCM 的通信网络运行态势感知模型研究 [J]. 现代电子技术 ,2023,46(12):159-162.

[6] 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 ,2020,46(6):130-135.

[7] 王莹莹 , 刘秀朵 . 基于自适应加权算法的通信网络安全态势感知数学模型研究 [J]. 长江信息通信 ,2023,36(7):60-62.

[8] 丁昊天 . 基于模糊 C 均值算法的多层次网络安全态势感知方法 [J]. 信息与电脑 (理论版),2023,35(12):76-78.

[9] 魏伟 . 基于改进 K-means 算法的校园网络环境安全态势感知方法 [J]. 信息与电脑 (理论版),2023,35(12):96-98.

[10] 姚征 . 基于时间序列输入结合 SIQNN 的网络安全态势感知研究 [J]. 微型电脑应用 ,2023,39(6):163-167.

[11] 任高科 , 莫秀良 . 基于 PRFGRFECV 特征优选的 GAGLight GBM 的网络安全态势评估 [J]. 计算机科学 , 2023, 50(S1):769-774.

[12] 常富红 , 李麒 , 张文丰 . 考虑数据特征聚类的电力系统网络运行安全态势感知 [J]. 无线互联科技 ,2023,20(11):159-161.

【作者简介】

白磊（1985—），男，河南新郑人，学士，讲师，研究方向：计算机技术、网络安全等。

张涛 (1991—)，男，河南新郑人，学士，助教，研究方向：软件工程。

（收稿日期：2023-12-26）