文章编号:1671-4598(2024)01-0099-06 DOI:10.16526/j.cnki.11-4762/tp.2024.01.015 中图分类号:TP393.083 文献标识码:A

基于 SOINN 结合 ADNDD 的网络安全动态控制技术研究

温浩杰，解韵坤，苏　彬
（中国人民解放军东部战区总医院，南京　210002）

摘要：医院网络安全动态控制技术对于保障医院网络的安全性和稳定性具有重要意义；传统的网络异常监测和网络安全动态控制无法解决大面积网络入侵的问题；为了解决这些问题，研究构建了基于 SOINN 结合 ADNDD 的医院安全动态控制模型；研究对算法进行优化，将 SOINN 与 ADNDD 进行融合构建网络安全动态控制模型，再利用数据集去验证模型的性能；结果表明，在数据集中训练后，模型在对浪涌攻击、偏差攻击和几何攻击数据集中的离群点识别率分别为 92.13%、90.04%和 89.07%；这说明模式算法经过数据集的应用能够在医院网络异常检测和动态防御控制中满足网络安全的要求；旨为提高医院网络的安全性和稳定性。

关键词：网络异常监测；医院；网络安全；动态控制

Research on Dynamic Control Technology of Network Security based on SOINN Combined with ADNDD

WEN Haojie, XIE Yunkun, SU Bin
(Eastern Theater Command General Hospital, Nanjing　210002, China)

Abstract: It is of great significance for hospital network security dynamic control technology to ensure the security and stability of hospital networks. The anomaly monitoring and security dynamic control of traditional networks cannot solve the problem of large area network intrusion. To solve these problems, a hospital security dynamic control model based on self-organizing incremental neural network (SOINN) combined with advanced digital network data design (ADNDD is constructed. The algorithm is optimized to fuse the SOINN with the ADNDD to construct the network security dynamic control model, and then the dataset is used to verify the performance of the model. The results show that after training in the dataset, the model identifies 92.13%, 90.04% and 89.07% of outliers in the datasets of surge attack, deviation attack and geometric attack, respectively. This indicates that the model algorithm can meet the requirements of network security in hospital network anomaly detection and dynamic defense control after the application of the dataset. The aim is to improve the security and stability of hospital network.

Keywords: network anomaly monitoring; hospital; network security; dynamic control

0　引言

随着信息技术的不断发展，医院网络安全问题日益凸显。医院作为医疗服务提供方，其网络系统也面临着越来越多的安全威胁。为了确保医院网络的安全，需要采取有效的安全动态控制技术。医院网络安全动态控制技术是指通过对医院网络流量和协议数据包等信息进行实时监测和分析，及时发现并处理潜在的安全威胁。该技术能够有效避免网络攻击，保障医院网络的安全性和稳定性。动态控制技术采用了多种手段，包括实时监控、异常行为检测等。此外，该技术还可以根据检测到的异常行为，动态调整医院网络配置和行为，以确保医院网络的安全性和稳定性[1-3]。探求一种更加安全的网络架构，从而解决日益严峻的医院网络安全问题是医院网络安全防御的热门领域。

近年来，国内外对于医院网络安全动态控制技术的研究日益受到重视。在国内，相关研究主要集中在如何建立有效的网络安全模型，以及如何实现网络安全动态控制。目前，国内已有一些高校和研究机构对医院网络安全动态控制技术进行了深入的研究和实践，提出了一些实用的技术方案，如基于流量特征、基于行为模式等[4]。此外，国内也有一些研究开始关注医院网络安全动态控制技术的应

收稿日期:2023-05-29；　**修回日期**:2023-07-12。
基金项目:东部战区总医院院管项目(YYQN2021081)。
作者简介:温浩杰(1978-),男,大学本科。
通讯作者:解韵坤(1987-),男,大学本科。
引用格式:温浩杰，解韵坤，苏　彬.基于 SOINN 结合 ADNDD 的网络安全动态控制技术研究[J].计算机测量与控制,2024,32(1):99-104,113.

用，如何在医院网络中实现实时的安全监控和预警等。国内学者李梦悦等人为了解决日益严峻的医院网络安全问题，构建了一种微分隔和细粒度的边界策略。通过对风险信息的收集、分析和漏洞的修复，有效地解决了医院现存的网络风险问题，可有效提升医院网络安全防护水平[5]。目前，国外一些研究机构已经开发出了一些实用的技术方案，如基于机器学习的动态控制技术、基于模型的动态控制技术等。这些技术可以根据网络安全模型，动态调整医院网络的配置和行为，从而保证医院网络的安全性[6]。而传统医院网络安全动态控制技术存在监测和控制难度大、误报和漏报较多等缺点[7-8]。与传统医院网络安全动态控制计算相比，这些技术具有更高的准确性和鲁棒性，可以更好地应对各种复杂情况。

同时，国外研究机构也对医院网络安全动态控制技术进行了相应的研究，研究发现有关医院网络安全的问题，如来自黑客的网络攻击、员工网络安全防护意识较差等问题。如何应对医院网络安全是保证医院正常运行的基础。因此，研究基于网络异常监测的医院网络安全动态控制技术，构建了医院安全动态控制模型，旨在提高医院网络的安全性和稳定性。

1 基于网络异常监测的医院网络安全动态控制模型构建

1.1 基于 ADNDD 的网络动态防御系统构建

为了实现网络动态的防御，研究基于数字信息处理的网络技术（ADNDD，advanced digital network data design）进行网络动态的防御优化，这是因为 ADNDD 能够使用数字信息来模拟网络流量，从而可以更加准确地监测网络流量，了解网络状况。当监测到有网络异常时会对异常情况进行分类，若是系统已知的攻击类型，则可以采取相应的攻击，从而避免攻击面扩大产生的额外运行开销；若监测到的网络异常是未知的攻击类型，则可以采取动态防御，以降低攻击的入侵，从而达到防御的效果[9-11]。首先，需要建立 ADNDD 的基本思路，将异常驱动与策略响应相结合，以确保网络能够抵御攻击。该状态应包括攻击者的攻击路径、攻击时间间隔，以及 ADNDD 中的网络资源消耗。然后，需要构建一个动态防御体系，以确保在受到攻击时，可以迅速对攻击进行识别和分类，并采取对应的措施。这个体系包括攻击者追踪、网络流量监测、资源保护等功能。最后，需要根据实际情况进行防御策略的优化，在受到严重攻击时，可以调整防御策略以提高网络的生存性。

异常驱动与策略响应相结合是一种将异常驱动技术和策略响应策略相结合的方法，这种方法可以提高网络的安全性和稳定性。异常驱动技术是指通过分析网络流量和协议数据包的模式来检测和识别异常行为。它可以帮助网络管理员快速识别和响应攻击，从而减少损失。策略响应策略则是指根据异常驱动技术检测到的异常行为，制定相应的响应策略[12-15]。例如，当网络遭到攻击时，策略响应策略可以包括恢复受损网络功能、阻止攻击行为等。此外，策略响应策略还可以对攻击者的身份、目的、攻击方式等进行分析和评估，并制定相应的响应措施。将异常驱动与策略响应相结合可以帮助管理员快速识别和应对潜在的安全问题，提高网络的安全性和稳定性。同时，这也有助于简化网络管理，减少资源浪费。

ADNDD 动态防御体系是一种将动态防御技术和网络设计技术相结合的方法，它可以帮助网络管理员在网络规划和建设过程中实现动态防御，ADNDD 动态防御流程图如图 1 所示。

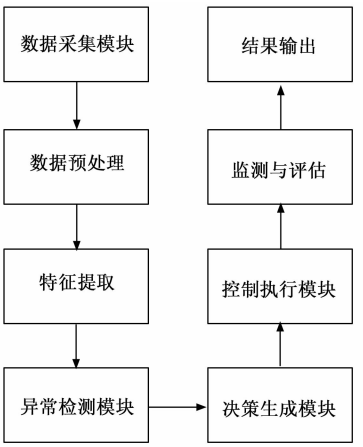


图 1 ADNDD 动态防御流程

结合图 1 分析可知，ADNDD 动态防御体系在医院网络安全动态控制模型中的各个模块具体作用如下。

1）数据采集模块：该模块负责从医院网络中收集实时的网络流量数据、日志数据和安全事件数据等信息。它可以通过网络监测设备、防火墙和入侵检测系统等来获取数据，并将这些数据传递给下一个模块。

2）数据预处理模块：该模块对采集到的原始数据进行处理和清洗，以去除噪声和异常值，并对数据进行标准化和规范化，以便后续模块对其进行处理和分析。

3）特征提取模块：该模块负责从预处理后的数据中提取有用的特征，例如网络流量的源 IP 地址、目的 IP 地址、协议类型、数据包大小等。这些特征可以用于后续模块的分析和决策。

4）异常检测模块：该模块使用机器学习和统计方法来检测医院网络中的异常行为，例如入侵攻击、恶意软件传播或未授权访问等。它可以利用预先训练的模型或实时学习的算法来识别异常模式，并生成相应的告警或警报。

5）决策生成模块：该模块基于异常检测模块的输出结果，生成相应的决策规则和策略。例如，当异常行为被检测到时，决策生成模块可以生成相应的防御措施，如封锁源 IP 地址、隔离受感染的设备或触发警报通知相关人员。

6）控制执行模块：该模块负责执行由决策生成模块生成的控制策略和防御措施。它可以通过网络设备配置、访问控制列表或防火墙规则等来实施这些措施，并确保网络安全的实时性和有效性。

7）监测与评估模块：该模块对医院网络安全控制系统的效果进行监测和评估。它可以收集执行过程中的日志数据和事件信息，并进行实时分析和评估，以便及时调整和优化系统的配置和策略。这些模块共同组成了医院网络安全动态控制模型中的 ADNDD 动态防御体系。通过这些模块的协同工作，可以实现对医院网络中的异常行为的实时监测、快速响应和动态控制，从而提高医院网络的安全性和可靠性。

由此可知该体系基于网络流量分析、动态防御策略、网络资源保护和网络安全评估等模块。其中，网络流量分析可以更加准确地监测网络流量，了解网络状况。动态防御策略可以确保在受到攻击时能够迅速调整防御策略。该策略可以包括异常驱动技术、策略响应策略等多种方法[16-17]。网络资源保护能够避免因攻击导致网络不可用的情况发生。网络安全评估可以确保网络在未来的发展中不会受到潜在的安全威胁。ADNDD 防御策略的优化是网络动态防御体系的重要组成部分，它可以帮助管理员应对日益复杂的网络威胁，提高网络的安全性和稳定性，对 ADNDD 防御策略的优化主要是更新防御策略，更新后的策略可以根据实际情况进行防御策略的优化。例如，在受到攻击时，可以调整防御策略以提高网络的可用性和安全性[18-20]。通过对 ADNDD 技术和动态防御体系进行综合优化，可以帮助管理员应对日益复杂的安全威胁，提高网络的安全性和稳定性。

1.2　基于 SOINN 结合 ADNDD 的医院安全动态控制模型构建

随着计算机网络和信息技术的发展，医院的网络安全问题日益突出[21-22]。为了保障医院的信息安全和正常运行，研究构建了一种动态控制模型，该模型基于自组织增量式神经网络算法（SOINN，self-organizing incremental neural network）和 ADNDD 两种技术，实现网络的动态防御和异常监测。SOINN 是一种用于解决神经网络训练过程中出现过拟合或欠拟合问题的算法。它通过不断调整网络参数来适应当前训练情况，从而避免了神经网络在训练过程中出现过拟合或欠拟合问题。自组织增量式神经网络算法的核心是将最近训练的神经网络参数与之前训练好的参数进行自组织合并，从而形成一个新的神经网络模型。自组织增量式神经网络算法可以应用于各种神经网络模型，如前馈神经网络、卷积神经网络、循环神经网络等。它可以解决各种神经网络训练中出现的问题，如过拟合、欠拟合、降维等，从而提高神经网络的训练精度和泛化能力。因此研究将 SOINN 结合 ADNDD 用于网络异常点检测，并在融合的基础上构建医院安全动态控制模型。

SOINN 能够对神经网络进行动态更新，并能在递增学习时自动保留已有的数据，避免重复学习，减少了训练所需的内存和运算量。在此基础上，将 SOINN 和有监督的分类方法有机地融合在一起，可以在保证模型运行的同时，有效地提高模型的性能。但若要将 SIONN 应用于异常检测，需要解决 SOINN 对采样顺序的敏感和 SOINN 通过距离计算样本之间的相似性等问题。如果对相同的采样顺序进行训练，得到的结果可能是完全不同的，从而影响到异常检测的精度。SOINN 通过距离来计算样本之间的相似性，实现了对高维、高量级数据的有效处理，并且存在着对高维、高量级数据的偏好，忽视了低维度对样本的判别力，进而降低了特征学习的精度。因此需要保证数据具有良好的特性，以保证能够满足递增学习的运输开销。首先需要初始化学习周期内的神经元集合，在神经元集合中加入新的输入样本。

SOINN 的输入是一组样本数据，输出是神经网络的权重和偏置。该算法的目标是通过学习样本数据，使神经网络能够对未知数据进行准确预测。网络参数的优化选取步骤如下。

1）通过初始化网络参数：初始权重和偏置可以通过随机初始化的方式进行。

2）计算神经网络的输出：使用当前的网络参数计算神经网络的输出。

3）计算损失函数：将计算得到的神经网络输出与样本数据的真实标签进行比较，计算损失函数的值。

4）更新网络参数：使用梯度下降法或其他优化算法来更新网络参数，使得损失函数的值减小。

5）重复步骤 2）～4），直到达到指定的停止条件（如达到最大迭代次数或损失函数收敛到一定阈值）。在网络参数的优化选取过程中，可以使用一些技术来提高算法的性能，如学习率衰减、正则化等。此外，还可以使用交叉验证等方法来选择合适的参数（如学习率、正则化参数等），以进一步提高算法的性能。再找到新的神经元和获胜神经元。神经元的计算公式可用公式（1）表示：

$$s_1 = \operatorname{argmin}\left\| \zeta - W_\tau \right\|, \tau \in \boldsymbol{N} \tag{1}$$

公式（1）中，ζ 表示新的输入样本；W_τ 表示神经元的权重；N 表示神经元集合；τ 表示神经元集合中的任意神经元。获胜神经元可用公式（2）计算：

$$s_2 = \operatorname{argmin}\left\| \zeta - W_\tau \right\|, \tau \in \boldsymbol{N}/\{s_1\} \tag{2}$$

公式（2）中，s_1 表示新的神经元值。计算得到的神经元和获胜神经元阈值，其中神经元对应的阈值可用公式（3）计算：

$$T_{s1} = \max\left\| W_\tau - W_j \right\|, j \in \boldsymbol{N}_\tau \tag{3}$$

公式（3）中，j 表示神经元集合中的权重。获胜神经元阈值可用公式（4）计算：

$$T_{s2} = \min\left\| W_\tau - W_j \right\|, j \in \boldsymbol{N}/\{\tau\} \tag{4}$$

公式（4）中，τ 表示神经元集合中的权重。为了提高算法的精度，还需要对神经元权重进行更新，更新的神经元权重可用公式（5）表示：

$$W_{s1} = W_{s1} + \varepsilon(t)(\zeta - W_{s1}) \tag{5}$$

公式（5）中，$\varepsilon(t)$ 表示新神经元的学习效率，t 表示神经元从开始训练到结束取得胜利的数量。获胜神经元的新权重值可用公式（6）表示：

$$W_{s2} = W_{s2} + \varepsilon'(t)(\zeta - W_{s2}) \quad (6)$$

公式（6）中，$\varepsilon'(t)$ 表示获胜神经元的学习效率。结合上述分析，基于 SOINN 结合 ADNDD 的医院安全动态控制流程如图 2 所示。

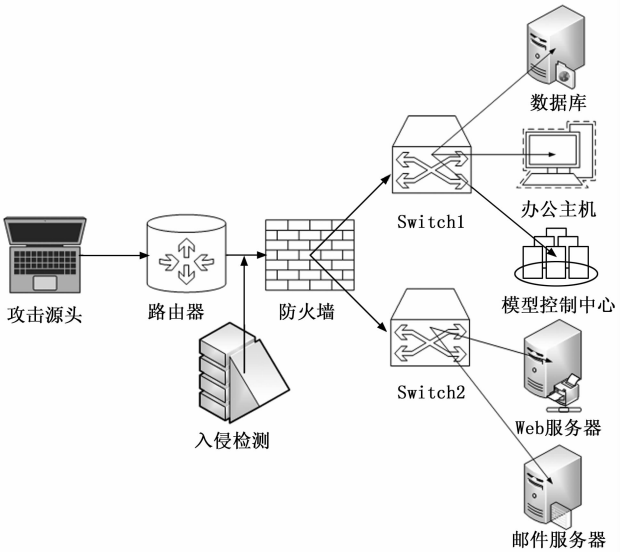


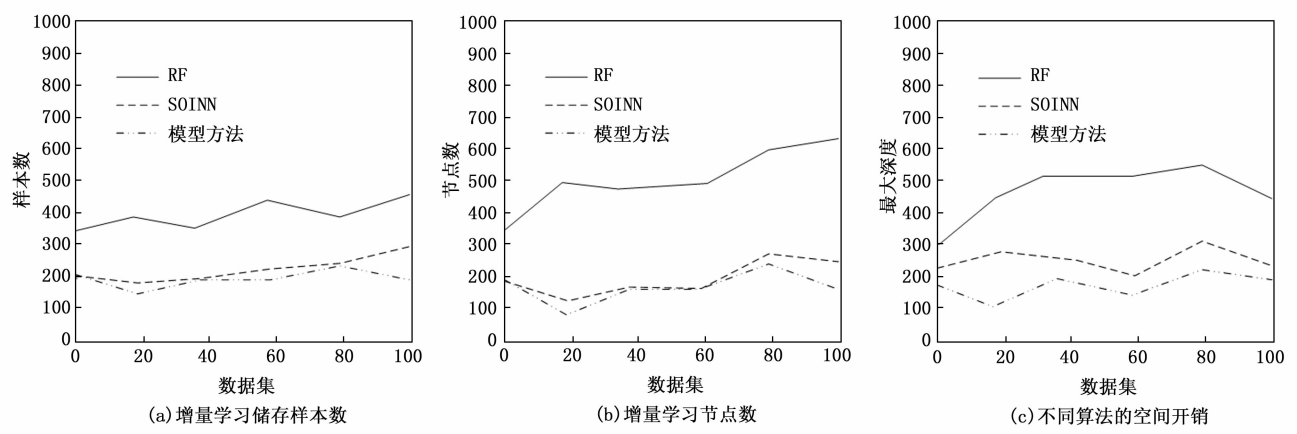
图 2 基于 SOINN 结合 ADNDD 的医院安全动态控制流程

结合图 2 分析，将 SOINN 与 ADNDD 结合并应用到医院安全动态控制模型构建中，可以采用以下步骤：第一步：数据收集收集医院安全方面的数据，包括诸如医生和护士的职称、患者的病情严重程度、医疗设备的使用情况、病房的拥挤程度等。第二步：特征提取从收集到的数据中提取特征，例如医生和护士的工作经验、患者的疾病类型、医疗设备的品牌和型号等，这些特征将用于构建 SOINN 和 ADNDD 模型。第三步：构建 SOINN 模型基于特征提取的数据，构建 SOINN 模型，可用于将数据聚类和分类。在医院安全动态控制模型中，可以使用 SOINN 模型对医生、护士、患者和医疗设备等进行聚类，以便更好地理解它们之间的关系。第四步：构建 ADNDD 模型基于特征提取的数据，构建 ADNDD 模型，可用于生成决策规则。在医院安全动态控制模型中，可以使用 ADNDD 模型根据实时数据生成决策规则，例如当病房拥挤程度超过某个阈值时，需要增派护士或调整患者的病房分配。第五步：模型融合与训练将 SOINN 和 ADNDD 模型进行融合，并使用历史数据对模型进行训练。通过模型融合，可以充分利用 SOINN 的聚类和分类能力以及 ADNDD 的决策能力，提高模型的综合性能。第六步：模型应用将训练好的 SOINN 与 ADNDD 模型应用于医院安全动态控制中。根据实时收集到的数据，使用 SOINN 模型对数据进行聚类和分类，然后使用 ADNDD 模型生成相应的决策规则。比如当 SOINN 模型将某个病房标记为高风险病房时，ADNDD 模型可以根据这个标记生成相应的决策规则，如调配更多的护士或提醒医生加强监护。根据收集到的数据和特征，可以构建包含若干节点和边的 SOINN 网络，并训练 ADNDD 模型生成相应的决策规则。

2 模型在网络异常监测的医院网络动态控制性能分析

为了验证模型在发生网络异常的医院网络动态控制中的性能，研究将医院的防火墙按照安全设定规则，分别设置了办公区域的电脑和隔离区域的电脑。同时为了保证数据的稳定性，在办公区域还配置了一台数据库，在隔离区域设置了网络服务器和邮件服务器，将攻击源设置为外部网络攻击。研究构建了 MVTEC 数据集；MVTEC 数据集是针对医院网络动态控制任务而创建的一个开放数据集。该数据集用于训练和测试网络异常监测算法，以检测医院网络中的异常行为。MVTEC 数据集包含了多种常见的医院网络异常行为，例如恶意软件入侵、网络攻击、数据泄露等。每个异常行为都有相应的高质量图像样本。这些图像样本被采集自真实医院网络环境中的网络流量数据，以保证数据的真实性和多样性。数据集的具体参数值包括：数据集规模：MVTEC 数据集包含了多个子数据集，每个子数据集由不同类型的异常行为组成。每个子数据集包含了数百到数千个图像样本。图像分辨率：MVTEC 数据集中的图像样本分辨率为 256×256 像素。标注信息：每个图像样本都有对应的异常标签，用于指示该样本是否属于正常行为还是异常行为。数据集划分：MVTEC 数据集通常采用训练集和测试集的划分方式。训练集用于训练网络异常监测算法，而测试集用于评估算法的性能。数据集来源：MVTEC 数据集的图像样本来自真实医院网络环境的网络流量数据，保证了数据的真实性和多样性。然后将 MVTEC 作为实验的数据集，该数据集中含有 15 000 个主机进程的动态行为特征，且每个样本有 100 个特征维度。最后随机取 1 000 个异常数据样本，1 000 个正常数据样本。通过数据集的仿真实验结果可知，在这个数据集中，模型算法的平均运行时间为 43.27 秒，而 SOINN 的平均运行时间为 48.92 秒，二者的平均运行时间相差了 5.65 秒。虽然差距不是很大，但这也说明模型算法在时间开销方面比 SOINN 更具有优势。此外，随着数据集的增加，两者的趋势也基本一致，这表明神经元操作是可行的。根据实验结果，可以得出结论，模型算法在处理数据集时的效率更高，因为它相对于 SOINN，平均运行时间更短。虽然差距只有 5.65 秒，但对于大规模数据集，这个差距可能会进一步扩大。此外，随着数据集的增加，模型算法和 SOINN 的运行时间都有所增加，且趋势基本一致。这表明无论是模型算法还是 SOINN，在处理更多数据时，都能够保持较为稳定的运行效率。为了验证模型方法在进行增量学习的空间开销情况，研究在同一数据集中进行实验，且以随机森林算法（RF，relevant feedback）、SOINN 和模型方法进行对比，对比结果如图 3 所示。

由图 3（a）可知，该图表示增量学习需要的储存样本数，在增量学习的过程中储存样本数的需求量越小说明其

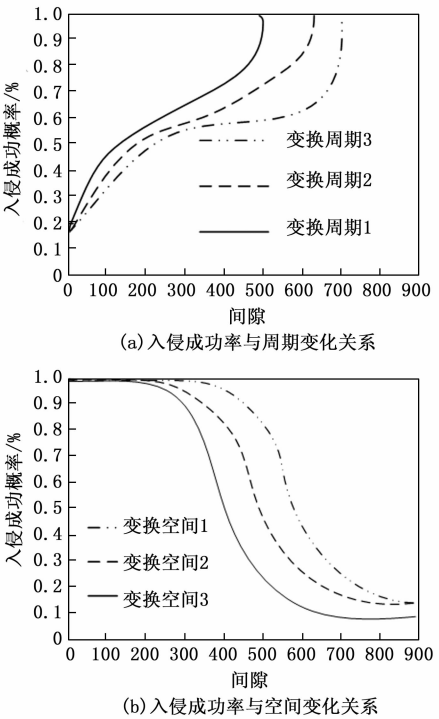


(a)增量学习储存样本数　(b)增量学习节点数　(c)不同算法的空间开销

图 3　不同算法在增量学习中的结果对比

占用的储存空间越少，这样能够增加现有存储只有的利用率。图中模型方法的需要储存样本数平均值为 196.53；SOINN 算法需要的储存样本平均值为 213.56；而 RF 算法需要的储存样本平均值最大，为 385.71。模型算法需要的储存样本数平均值比 SOINN 算法和 RF 算法需要的储存样本平均值低 17.03 和 189.18，这说明模式算法能够在占用更小空间的情况下完成监测。由图 3（b）可知，该图表示增量学习节点数，节点数的大小与模型检测异常所需的空间大小有关，在模型的增量学习过程中，节点数越小，说明模型检测时需要的储存空间越小。图中模型方法的节点数平均值为 180.89；SOINN 算法的节点数平均值为 226.51；同样 RF 算法的节点数平均值最大，为 509.35。模型算法的节点数平均值比 SOINN 算法和 RF 算法的节点数平均值低 45.62 和 328.46，这说明模式算法在检测时占用的空间更少，有利于资源的利用。由图 3（c）可知，该图表示不同算法在同一数据集中的空间开销对比情况，在同一数据集中最大深度值越小，模型方法检测时所占用的 CPU 空间越小，更有利于检测的进行。图中模型方法的最大深度平均值为 200.06；SOINN 算法的最大深度平均值为 246.13；RF 算法的最大深度平均值为 509.43。模型算法的最大深度平均值比 SOINN 算法和 RF 算法的最大深度平均值低 46.07 和 309.37，这说明模式算法在检测时具有更好的可行性。为了验证模型在网络入侵成功后的防御性能，研究在同一数据集中，利用动态变换周期和变换空间来探究模型网络动态防御的性能。图 5 表示基于单脆弱性变换的入侵成功率，图 4 中变换周期 1、2、3 和变换空间 1、2、3 分别表示单脆弱性的取值分别为 10、100 和 1000。

由图 4（a）可知，随着间隔的增加入侵成功率也在增加，其中脆弱性的取值越小，入侵成功率越低，变换周期 1 的成功入侵率达到 100%时，间隙为 449.17。变换周期 2 的成功入侵率达到 100%时，间隙为 631.06；变换周期 3 的成功率入侵达到 100%时，间隙为 713.56。这验证了变换周期越小越有利于模型网络动态的防御。由图 4（b）可知，随着间隙的增加，变换空间发生变化后入侵成功率明显下降，



(a)入侵成功率与周期变化关系

(b)入侵成功率与空间变化关系

图 4　脆弱性变换下的入侵成功率

变换空间 3 的入侵成功率最低，其次是变换空间 2 和变换空间 1，这说明变换空间能够增加模型的动态防御性能。为了进一步验证模型的动态防御性能，研究也在同一数据集中，利用最小周期和空间大小来探究模型网络动态防御的性能。图 5 表示基于多脆弱性情况下的入侵成功率对比图。

由图 5（a）可知，随着最小变换周期的变化，入侵成功率也在增加，最小变化周期 1 的入侵最快，其次是周期 2 和周期 3，这说明最小变化周期值影响动态防御的性能。由图 5（b）可知，随着总变换空间的减小，入侵成功率也明显的下降，这同样能够说明总变换空间值越大，模型对异常入侵的动态防御性能越强。为了验证研究提出的模型算法在医院网络异常检测和动态防御控制的实际应用效果。研究将网络入侵划分为浪涌攻击、偏差攻击和几何攻击 3

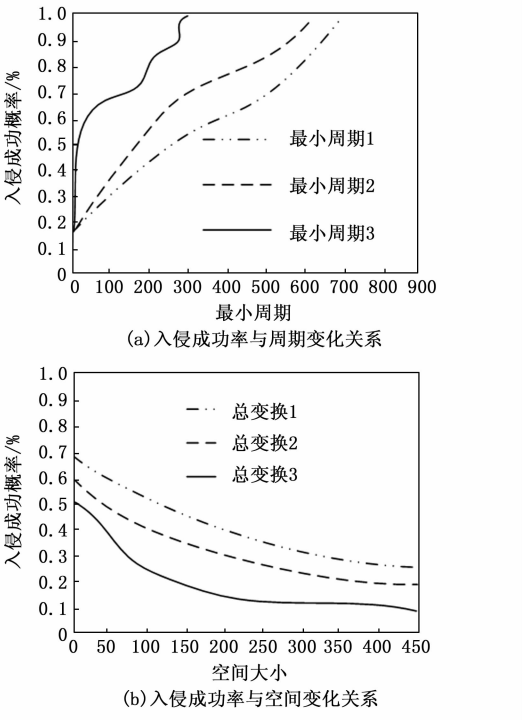


图 5 多脆弱性情况下的入侵成功率对比

种。且研究选取 3 种类型网络入侵的数据进行实验，每种攻击均选取 1 000 个经过预处理且带有离群点标记的样本进行实验。其中浪涌攻击的有 63 个离群点，偏差攻击的有 49 个离群点，几何攻击的有 41 个离群点。随后研究将 RF、SOINN 和模型方法应用于样本数据集中进行对比实验，并以识别率、误判率以及算法耗时作为对比指标。通过实验结果可知，模型算法在 3 种不同类型网络入侵数据集中的离群点识别率均显著高于 SOINN 算法和 RF 算法。且其在浪涌攻击、偏差攻击和几何攻击数据集中的离群点识别率分别为 92.13%、90.04%和 89.07%。这说明模式算法在模型算法在医院网络异常检测和动态防御控制的实际应用效果也优于对比算法。

3 结束语

随着计算机网络的发展，医院网络环境也遭受到更多的异常入侵，为了确保医院工作的正常开始和维护患者的隐私安全等，需要采取有效的网络安全动态控制技术。研究首先对医院网络安全动态控制构建模型，然后将 SOINN 算法与 ADNDD 进行融合，最后利用数据集进行仿真实验，以验证模型算法的具体性能。为了验证模型算法的可行性，将模型算法与 SOINN 进行了对比，模型算法的运行时间明显低于 SOINN，这说明其具有更高的可行性。将模型算法与 RF 和 SOINN 用于数据集仿真训练，结果表明模型算法需要的储存样本数平均值比 SOINN 算法和 RF 算法需要的储存样本平均值低 17.03 和 189.18；模型算法的节点数平均值比 SOINN 算法和 RF 算法的节点数平均值低 45.62 和 328.46；模型算法的最大深度平均值比 SOINN 算法和 RF 算法的最大深度平均值低 46.07 和 309.37。为了验证模型的实际防御效果，通过采用 3 种已知的异常入侵对模型进行测试，在浪涌攻击、偏差攻击和几何攻击数据集中的离群点识别率分别为 92.13%、90.04%和 89.07%。这说明模式算法在模型算法在医院网络异常检测和动态防御控制的实际应用具有很高的价值。同时这也表明模型算法在网络异常检测和动态防御过程中能够减少医院现有计算机的资源浪费，并帮助医院及时发现并处理潜在威胁，提高医院的网络安全。但研究中还存在不足之处，由于实验中采用的数据集均为同一数据集，数据中的数据来源较为单一，这使得结果存在一定的局限性，下一步可以增加数据集种类，以提高模式算法的适应性。

参考文献：

[1] 李 麟. 基于 Ad Hoc 网络的医院智能安防控制系统设计 [J]. 计算机测量与控制，2019，27 (4)：64 - 67.
[2] 李 铮，魏 星，佟明泽，等. 基于网络安全的医院信息安全设计改造与分析 [J]. 微型电脑应用，2021，37 (3)：10 - 12.
[3] 刘 阳，俞 准. 网络安全等级保护 2.0 时代医院管理的方法与对策 [J]. 海南医学，2022，33 (4)：535 - 537
[4] 刘建兰，覃仁超，何梦乙，等. 基于大数据技术的网络异常行为检测模型 [J]. 计算机测量与控制，2020，28 (3)：62 - 66.
[5] 李梦悦，陈 敏. 基于零信任架构的医院网络安全防护研究 [J]. 中国数字医学，2021，16 (9)：106 - 109.
[6] LIM S B，LOSASSO T，CHAN M，et al. Risk Management of Clinical Reference Dosimetry of a large hospital network using statistical process control [J]. International journal of medical physics，clinical engineering and radiation oncology，2021，10 (3)：119 - 113.
[7] 王华磊，李子涛，温 喆. 基于物联网技术的智慧医院健康监测平台研究 [J]. 现代科学仪器，2023，40 (1)：154 - 159.
[8] 周 彬，黄 磊，李 为，等. 基于 5G 技术构建医院网络系统的创新应用研究 [J]. 中国数字医学，2022，17 (5)：40 - 45.
[9] 药 炜，张 凯，原 军，等. 基于数字信号处理的电力光纤通信网络状态监测 [J]. 机械与电子，2021，39 (7)：24 - 27.
[10] 刘仲驰. 基于果蝇算法的网络图像边缘检测方法 [J]. 自动化应用，2022 (11)：81 - 83.
[11] 范美玉，傅昊阳. 数字化转型推动医院信息管理发展的机理与路径研究 [J]. 中国医院管理，2023，43 (2)：60 - 63.
[12] 孙晓虎，余阿祥，申栩林，等. 混合注意力机制的异常行为识别 [J]. 计算机工程与应用，2023，59 (5)：140 - 147.
[13] 胡巧婕，刘永辉. 基于 IPv6 技术的局域网入侵检测系统设计 [J]. 信息技术，2022，46 (9)：46 - 50.
[14] 雷江龙，余 娟，向明旭，等. 基于深度神经网络的数据驱动潮流计算异常误差改进策略 [J]. 电力系统自动化，2022，46 (1)：76 - 84.
[15] ARUNA SANTHI J，VIJAYA SARADHI T. Attack detection in medical Internet of things using optimized deep learning：Enhanced security in healthcare sector [J]. Data Technologies and Applications，2021，55 (5)：682 - 714.

(下转第 113 页)