摘 要

物联网（IoT）和其他新兴的通信网络技术在各个领域中有着极高的效率、便利性和连接性。然而，这些进展也带来了重大的安全风险，因为攻击的复杂性越来越高，有效的安全策略也缺乏。传统的安全方案，如基于签名的入侵检测系统，存在高误报率、低准确性、高纬度数据处理困难、缺乏实时性和难以适应新威胁。因此，基于网络安全态势感知的主动防御技术是必不可少的。网络安全态势感知旨在通过对过去以及现在的网络数据进行特征要素提取，从而有效表征某时刻的网络安全状况并准确预测未来的网络安全状况。真实网络环境中流量数据复杂、规模大、攻击行为无明显周期等问题导致现有网络安全态势感知模型无法有效提取网络安全态势要素、精准度低。针对上述问题，采用改进的多尺度残差网络从多尺度、多角度提取网络安全态势要素和适用于网络安全态势感知的注意力机制提高网络安全态势感知的精准度。具体工作如下：

(1) 针对现有网络安全态势评估方法准确率较低的问题，提出了一种基于改进的 ResNeXt 和 Transformer 的网络安全态势评估方法。为了解决由于真实网络环境中网络流量数据复杂、攻击数据周期混乱导致网络安全态势评估模型无法有效提取网络安全态势要素、评估网络安全状况的问题，首先对 ResNeXt 进行了改进，采用多尺度卷积交叉结构代替单一尺度的卷积结构，使得网络安全态势评估模型能够从多角度、多尺度全面的提取网络安全态势要素。通过使用通道注意力机制（SEnet）进一步提炼、表征改进的 ResNeXt 处理后的数据。最后使用 Transformer 的编码器对网络模型进行优化，提高网络安全态势评估的精准度。使用 KDDCUP99 数据集、UNSW-NB15 数据集、WSN-DS 数据集和 CICIDS2017 数据集进行仿真实验，实验表明提出的基于改进的 ResNeXt 和 Transformer 的网络安全态势评估模型获得了更高的精准度。

(2) 针对现有的网络安全态势预测方法只能捕捉长周期或者短周期数据特征，导致态势预测精准度低的问题，本文提出了一种基于注意力机制的长短周期网络安全态势预测（ALSNAP）方法，使用分支注意力机制融合了多头自注意力机制改进的双向长

短周期记忆神经网络、向量自回归和多尺度卷积神经网络，分别从长数据周期、短数据周期等多个角度提取网络安全态势要素。同时提出了一种适用于网络安全态势感知的注意力机制来优化预测模型网络结构、提高预测模型精准度。本文在包括三个典型的物联网数据集在内的四个公共网络数据集上评估了 ALSNAP 的性能，并与其他最先进的方法进行了比较。结果表明，ALSNAP 的预测准确性高于其他方法。

关键词：网络安全态势评估，网络安全态势预测，注意力机制，残差网络，长短期记忆神经网络

目录

1 绪论

1.1 研究背景及意义

通信和网络技术，尤其是无线网络，在近年来得到了快速的发展。从 2G 时代的无线数字语声传输到 5G 时代的物联网、智能家居系统、工业控制系统和远程医疗等各种应用，网络已经成为生活中不可或缺的一部分。然而，网络也越来越容易受到不断增加的网络安全风险的威胁，对我们的隐私和安全构成重大威胁[1][2]。一些常见的网络安全威胁包括数据拦截、破解、传输干扰[3]、配置问题、蠕虫攻击和拒绝服务攻击[4]。

传统上，入侵检测系统（IDS）用于检测攻击，通过识别未经授权的使用、误用或滥用计算机系统来提供安全保障[5]。然而，新兴的无线网络，如物联网（IoT），面临着比传统网络更多的安全问题和威胁。这是因为它们缺乏标准化，由于资源有限而存在设备漏洞，并且往往由不重视安全的制造商生产[6]。这导致了越来越多且越来越复杂的攻击，使得 IDS 难以及时检测到它们。节点的移动性和灵活性也给事件处理人员或网络管理员做出适当和及时决策带来了越来越大的困难。这种矛盾在各种新的网络技术的快速发展和应用以及网络安全人员短缺的情况下变得更加严重。此外，一旦被检测到攻击才采取行动已经太晚了，而损害可能是难以修复的[7]。最后，由于大多数 IDS 的误报[8]，入侵保护系统（IPS）无法合理迅速地分配策略和应对威胁。因此，当前的安全方案面对真实网络环境中复杂的数据流量和混乱的攻击数据周期无法完全有效提供足够的网络保护，仍存在安全挑战。

网络安全态势感知（Network Security Situation Awareness，NSSA）旨在实时监测、分析和预测网络安全态势，并提供及时有效的对策。智能的 NSSA 系统可以监测和捕获各种类型的威胁，对其进行分析，并制定避免进一步攻击的计划。智能 NSSA 系统的全面设计可以帮助决策者了解系统的当前和即将到来的安全情况，增加他们在决策点上的认识。

1.2 国内外研究现状

1.2.1 网络安全态势评估

网络安全态势感知包含网络安全态势评估和网络安全态势预测。网络安全态势评估是对目前网络中收集的攻击信息进行网络安全态势要素提取和网络攻击类型判别。

通过判别攻击类型来评估目前整个网络的安全状况。同时把网络安全状况反馈给网络安全管理员用以对网络安全策略进行调整，达到更好的防御效果。

在传统方法的研究方面，Li[9]等人为了实验无人机（UAV）的态势评估，建立了一种基于贝叶斯网络的态势评估模型，针对贝叶斯网络参数难以获取的问题，提出了一种基于先验参数区间的改进鲸鱼优化算法（IWOA-PPI）用于参数学习。实验结果表明，IWOA-PPI 十分的有效。在情景实验中也证明了提出方法的正确性和可行性。Whelan 等人[10]提出了 MAVIDS，使用主成分分析（PCA）和单类分类器（如自编码器、OC-SVM 和 LOF）来检测异常情况。可以使用飞行记录作为训练数据，是一种多功能的方法。HE 等人[11]提出了一种基于数字孪生网络（DTN）的联合连续学习框架，其中使用堆叠广义学习系统（SBLS）进行 IDS 模型的快速连续学习和训练。为了提高训练和聚合过程中的效率和质量，采用了异步联邦学习架构，并提出了一种基于深度确定性策略梯度（DDPG）的辅助 DTN 的无人机选择方案，以帮助全局 IDS 模型的聚合。该算法使用了 CIC-IDS2017 数据集进行验证，模拟结果显示，该算法比现有的联邦学习方案实现了更高的效率和准确性，但未用无线数据集进行验证。Silva 等人[12]在这项工作中提出了一种用于检测无人机群飞行异常和网络攻击的入侵检测系统（IDS），分别应用了无监督和监督的机器学习方法。在无监督方法中，堆叠自编码器和联邦学习用于检测飞行中的异常情况。监督算法，如 LightGBM，用于识别对无人机网络的拒绝服务（DoS）攻击，并使用生成对抗网络（GAN）进行数据平衡。IDS 取得的结果是有希望的，表明选择的技术的有效性，特别是联邦学习，它利用了无人机群体的分布特性并确保数据隐私。

在深度学习研究的方面，Liu[13]等人为了解决无线网络数据具有大容量、多样性和高纬度特点导致的网络安全态势评估精准度低等问题，提出了一种基于简约记忆神经单元（PMU）的新型模型，即双向简单记忆单元（BIPMU）。与 PMU 相比，BIPMU 不仅可以通过其时间序列关系学习和表征数据，还可以全面有效的管理时间序列数据中长期和短期依赖潜在的连接。实验结果表明，与已有的网络安全态势评估工作相比，采用的方法在效率和准确性方面有所突破。Yang[14]等人为了解决现有网络安全态势评估方法中特征提取困难、时效性差的问题，提出了一种基于网络攻击行为分类的网络安全态势评估方法。设计了一个网络攻击行为分类模型，该模型结合了并行特征提取网络（PFEN）、双向门控循环单元（BiGRU）和注意力机制的特点和优势，从不同的

网络攻击行为中提取关键数据。实验结果表明，与传统方法相比网络攻击行为分类模型的准确率提高了 5.28%，召回率提高了 5.65%，证明了所提出方法的有效性。Ramadan 等人[15]提出了一种基于长短期记忆（LSTM）的分布式框架，用于检测无人机中的入侵。该框架涉及将循环神经网络（RNN）模块分布在每个无人机中，每个无人机试图检测对自身的攻击。此外，基站上的集中式 LSTM-RNN 模块验证攻击并做出最终决策，然后通知其他无人机。

上述方法通过对模型的改进，提高了网络安全态势评估的精准度和效率，但针对网络数量复杂、规模大的真实网络环境网络安全态势要素提取困难、网络安全态势评估精准度低的问题，并没有给出实质性的解决方案。

1.2.2 网络安全态势预测

网络安全态势感知（NSSA）的重要性日益增加，它使网络安全人员能够了解整个网络的安全状态，识别网络上的问题和异常活动，并及时提供反馈或进行改进而不延误[16]。作为 NSSA 的重要组成部分，网络安全态势预测已经得到广泛研究，旨在实现对网络攻击的早期检测和预防，并提高入侵检测系统的准确性和效率[17-18]。任务不是预测特定的攻击，而是对整个网络的状态进行预测。

已有的几项研究提出了考虑时间相关性的网络安全分析和预测方法。Werner 等人[19]提出了一种方法，利用每日网络攻击数量之间的时间相关性来预测未来网络时段的攻击强度。然而，这种方法存在一个限制，即没有考虑缺失数据中的日期，导致了一个不完整的数据集，从而导致了不准确的预测。Okutan 等人[20]提出了一种应用非传统信号的广义贝叶斯分类神经网络方法，用于提前预测网络攻击。训练模型的准确率可达 63%至 99%。Bar 等人[21-22]提出了一种基于蜜罐收集的数据来分析攻击传播模式的新方法。该方法将概率马尔可夫链模型与复杂网络研究领域的算法相结合。结果分析表明，攻击传播可能因攻击来源国的不同而有所差异。Uwagbole 等人[23]通过学习数据构建了一个使用支持向量机(SVM)算法和特征哈希进行分类器训练的定量预测分析的 Web 应用程序，取得了良好的结果。Yang 等人[24]探索了面向 5G 的 MIMO 系统安全的态势感知理论，并基于 MIMO 系统理论和态势感知技术理论构建了一个面向 5G 的大规模 MIMO 系统的安全态势感知系统模型。该模型使用 MIMO 系统的证据推理规则来评估安全情况并预测未来情况。

上述研究主要关注网络安全态势的短期预测。然而，长期预测的鲁棒性和准确性

也是至关重要的，因为一些攻击事件可能持续很长时间。He 等人[25]提出了一种基于数据驱动方法的 WNN-M 预测模型，该模型结合了 MODWT 方法和混合 WNN 架构，以提高长期预测的准确性。实验结果表明，相比传统的 WNN 模型，WNN-M 将均方根误差（RMSE）降低了 19.87%，绝对均方根误差（RMSE）降低了 4.05%，实现了更准确的长期预测。Yin 等人[26]提出了一种基于时间卷积网络（TCN）和 Transformer 的网络安全态势预测模型，以解决时间序列的长期预测问题。实验结果显示，该预测模型在大多数评价指标上具有更好的鲁棒性和准确性。

此外，Abdlhamed 等人[27]提出了一种新的入侵检测系统技术，解决了大数据环境中数据过载和瓶颈的问题。他们的系统利用进化统计方法进行预测，并展示了单一技术模型在构建通用入侵预测解决方案方面的不足。Leau 和 Manickam[28]提出了一种自适应灰色理论模型，考虑了网络攻击的特性，并克服了传统灰色理论的缺点。他们的实验结果表明，他们提出的方法在预测网络安全情况方面优于传统模型。

上述各种算法模型在态势预测领域的各个方向都取得了较好的成果，但在数据流量复杂、规模大、没有明显周期性的真实网络环境下，并不能很好的解决充分理解网络安全态势要素、精准预测网络安全状况的问题。

1.3 研究内容

针对真实网络环境中网络流量数据复杂、攻击行为周期不明确和网络安全态势要素提取困难等问题，提出了基于残差网络和注意力机制的网络安全态势感知研究，为主动防御提供科学依据、提高网络安全态势感知精准度。

(1) 针对真实网络环境中网络安全态势要素提取困难问题，本文对 ResNeXt 进行了改进，通过使用多尺度卷积交叉的结构取代单一尺度的卷积来实现从多角度、多尺度和多方位的全面提取网络安全态势要素，从而提高了复杂数据流量网络安全态势感知的精准度。

(2) 针对网络流量数据复杂、攻击行为周期不明确问题，本文提出了一种并行结构的网络安全态势预测模型。该模型通过分支注意力机制融合了多头自注意力机制改进的 BiLSTM、向量自回归和多尺度残差网络，使之能够从多长度周期学习网络安全态势要素，解决了攻击数据周期混乱情况下单一模型预测精准度低的问题。

(3) 为了提高网络安全态势感知的精准度，提出了一种适用于网络安全态势感知的注意力机制，通过方向平均池化进行压缩、扩散模型进行扩散，在使用多尺度卷积和分