CRGT-SA：基于交错式时空深度学习的网络入侵检测模型

陈珏，刘皖肖，邱禧荷，吕文静，熊玉洁
上海工程技术大学电子电气工程学院，中国上海市，310027

摘要：为应对网络攻击的挑战，人们引入入侵检测系统以识别入侵行为并保护计算机网络。在所有这些入侵检测系统中，传统机器学习方法依赖于浅学习，其性能不理想。与机器学习方法不同，深度学习方法是目前主流方法，因其能处理大量数据，而无需事先了解特定领域的专业知识。在深度学习中，长短期记忆（LSTM）和时间卷积网络（TCN）可以从不同角度提取时间特征，而卷积神经网络（CNN）则可以学习空间特征。基于此背景，本文提出一种新的交错式时空深度学习模型（CRGT-SA），该模型将CNN与门控TCN和LSTM模块结合以学习时空特性，并引入自注意力机制选择显著特征。具体而言，所提模型将特征提取分解为粒度逐渐增加的多个步骤，并结合CNN、LSTM和门控TCN模块执行每个步骤。基于UNSW-NB15数据集对所提CRGT-SA模型进行验证，并与其他方法比较，包括传统机器学习、深度学习模型以及最先进的深度学习模型。仿真结果表明，所提模型具有最高准确率和F1值。所提模型在二分类和多分类上的准确率分别为91.5%和90.5%，证明其保护互联网免受复杂网络攻击的能力。此外，在NSL-KDD数据集上进行了一系列模拟，并与其他模型比较；仿真结果进一步证明该模型的泛化能力。

关键词：入侵检测；深度学习；卷积神经网络；长短期记忆网络；时间卷积网络
https://doi.org/10.1631/FITEE.2400459