**文献综述**

Staudemeyer and Omli(doi:10.1145/2513456.2513490)评估了LSTM-RNN在对入侵检测数据进行分类方面的性能，LSTM网络能够将数据建模为时间序列。使用KDD Cup 99数据集的改进版进行训练和测试。结果表明，LSTM能够学习隐藏在训练数据中的所有攻击类别。

Javaid(doi: 10.4108/eai.3- 12-2015.2262516.)提出了一种基于深度学习的方法，通过在NSL-KDD数据集上使用了无监督学习来实现了有效而灵活的网络入侵检测系统，这表明该系统在检测未知网络入侵方面很有希望。

J.Kim等人(doi:10.1109/platcon.2016.7456805.)使用了基于LSTM-RNN的分类器，通过深度学习的方法实现了入侵检测模型，并对模型进行了评估。也是使用了KDD Cup 99数据集，实验调整了学习率和隐藏层大小。LSTM-RNN分类器显示出比其他分类器更高的检测率。但是，这个分类器的误报率还是很高。

Yu, Bin(doi:10.1109/icdmw.2017.96.)在论文讨论了使用深度学习检测恶意域名。 他们表明，与传统的ML算法相比（性能缓慢且性能较差），使用CNN，RNN和LSTM的深度学习算法表现出色，此外，深度学习算法在对抗性环境中仍然保持强大的性能。。

Dahl等人(doi:10.1109/icassp.2013.6638293.)提出了一种大规模的恶意软件分类系统，该系统利用随机投影来减少输入空间。与使用所有功能的基本逻辑回归系统相比，通过随机投影训练的神经网络能够将错误率降低43%。

Yuancheng Li等人(doi:10.14257/ijsia.2015.9.5.21.)提出了一种基于深度学习的混合恶意代码检测方案：首先，通过利用AE提取输入书记的主要特征，使用AutoEncoder降低数据的维数；然后，基于这些特征，将深度信念网络（DBN）设置为用于多次深度学习的分类器；最后，提高了检测精度并降低了混合模型的时间复杂度。

Saxe和Berlin(doi:10.1109/malware.2015.7413680.)引入了一种基于DNN的恶意软件检测器，该检测器使用静态分析功能，能够在极低的误报率前提下获得可观的检测率，并且使用低配版的硬件就能实现训练。它的高效的方法来自于传统的劳动密集型签名方法，同时还可以检测未知的恶意软件。

Pascanu(doi:10.1109/icassp.2015.7178304.)提出了一种类似于自然语言建模的方法，该方法通过执行指令来学习软件的语言，并通过随机时间投影提取时域特征。与标准三元组事件模型相比，性能最佳的混合模型将准确率提高到了98.3%，误报率为0.1%

Stokes(doi:10.1007/978-3-319-40667-1\_20.)提出了一种用于恶意软件分类的多任务深度学习架构，用于二进制恶意程序分类任务。所有模型都是从恶意或者良性样本中的动态分析中提取出来的数据进行训练。他们发现使用多层DNN架构能够对恶意软件的效率和性能有所改善。

Verma(doi:10.1145/3180445.3180456.)等人提出了反网络钓鱼的探测器，使用针对不平衡数据集的新指标评估了电子邮件中的网络钓鱼技术。 讨论了用于特征提取的各种技术，例如：词频-逆文档频率（TF-IDF），非负矩阵分解（NMF）和单词袋等。