研究提出基于变体GRU预处理网络数据包的入侵检测优化算法

作者：writer 来源：中国科学院声学研究所

本文原地址：https://www.iikx.com/news/progress/6020.html

研究提出基于变体GRU预处理网络数据包的入侵检测优化算法。在网络空间中，用入侵检测(Intrusion Detection System，IDS)判断网络数据包是否包含攻击对于防范网络攻击和保护信息安全具有重要意义。现有的IDS算法存在两个问题，一是利用人工经验大量提取的特征无法准确描述网络数据包;二是神经网络结构复杂、内存占用大、功耗大。 中国科学院声学研究所国家网络新媒体工程技术研究中心的博士生郝怡然与其导师、副研究员盛益强、研究员王劲林等人采用GRU(Encoded Gated Recurrent Unit)的两种变体预处理网络数据包对入侵检测进行了优化，其中E-GRU(Encoded Gated Recurrent Unit)能够获得优于先前方法的准确率和召回率;E-BinGRU(Encoded Binarized Gated Recurrent Unit)通过对权值和激活函数二值化处理将内存开销降低到E-GRU的1/21。相关研究成果2019年4月在线发表于学术期刊IEEE Access。

针对E-GRU算法，研究人员使用Auto-encoder的encoder部分对网络数据包进行自动预处理。将原始的网络数据包数据作为encoder模型的输入，则encoder模型的输出就是预处理后的网络数据包特征。encoder可以从输入中提取重要的特征并将其作为GRU的输入进行入侵检测，与原始输入相比通常能更好地表示输入;E-BinGRU将E-GRU的权重和激活函数二值化，以减少内存开销。

与传统的手工预处理相比，使用Encoder对网络数据包进行自动预处理可以更好地检测不同的攻击。 在ISCX2012数据集上进行的实验结果显示，E-GRU在对有攻击网络数据包的检测率(Detection Rate，DR)达到99.9%，比GRU的准确率高且比现有最先进方法高3%;E-BinGRU的准确率达到99.7%，且比Bin-GRU的准确率高。 最坏情况测试结果显示，该入侵检测模型在准确性、检出率和误报率方面的性能较稳定。为了减小内存大小，研究人员使用E-BinGRU进行网络入侵检测。E-BinGRU减小了内存开销，用逐位运算代替了大部分算术运算。结果表明，通过使用二进制权值和激活，可以将模型的内存使用量减少到E-GRU的1/21。

相关论文信息：DOI: 10.1109/ACCESS.2019.2910860