

RESUMO APRESENTAÇÃO ORAL PADRÃO - CENTRO DE TECNOLOGIA
(CT)/CIÊNCIA DA COMPUTAÇÃO

**UM ESTUDO DO FLUXO DE TRABALHO COM REDES
AUTOASSOCIATIVAS PROFUNDAS PARA DETECÇÃO DE ANOMALIAS**

Kaylani Bochie (kaylani@gta.ufrj.br)

Miguel Elias Mitre Campista (Orientador) (miguel@gta.ufrj.br)

As Redes Neurais Autoassociativas (Autoencoders) são largamente utilizadas para tarefas como compressão de dados, redução de ruído e detecção de anomalias. O sucesso desse tipo de rede neural se deve à organização particular das conexões entre seus neurônios. Desta forma a rede busca reproduzir os dados de entrada na sua saída, através do aprendizado de uma representação simplificada dos dados (BOCHIE et al., 2020).

O fluxo de trabalho normalmente utilizado em tarefas de aprendizado supervisionado, onde cada amostra de um conjunto de dados possui um rótulo associado, consiste em separar um conjunto de dados em três subconjuntos com o objetivo de treinar a rede neural, ajustar seus hiperparâmetros e avaliar seu resultado. Logo, dada a natureza de treinamento não supervisionado das redes neurais autoassociativas para tarefas de detecção de anomalias, esta técnica de avaliação não é apropriada. Para este caso de aprendizado multi-instância as amostras são agrupadas de acordo com sua classe, dessa forma as amostras não são rotuladas individualmente (GOODFELLOW et al., 2016). Durante o treinamento, as redes são expostas apenas a dados "normais", ou

seja, não anômalos. Esta etapa garante que o erro de reconstrução seja minimizado e, ao ser confrontada com uma nova amostra, a rede apresentará alto erro de reconstrução para amostras anômalas. Esta técnica permite treinar essas redes para detectar cenários como ataques a redes de computadores, motores defeituosos em redes industriais e tumores em imagens médicas.

A primeira fase deste trabalho consistiu no estudo e reprodução de técnicas do estado da arte em aprendizado de máquina e aprendizado profundo. Foi notado que grande parte dos trabalhos atuais utilizam conjuntos de amostras normais para o treinamento e ajuste de hiperparâmetros. Ainda, foi observado que algumas heurísticas diferentes são escolhidas para escolher o limiar de classificação em amostras anômalas, como a mediana do erro médio quadrático em um conjunto de amostras não anômalas (MEIDAN et al., 2018). Este trabalho, dessa forma, propõe um novo fluxo de trabalho, que diferente do fluxo tradicional usado nas redes neurais autoassociativas profundas, tem foco na divisão de dados para melhor exploração da arquitetura de redes neurais autoassociativas. Além das técnicas propostas neste trabalho, o estudo também resultou em dois artigos publicados em congressos nacionais, uma no SBSeg 2020 e outra nos minicursos do SBRC 2020.

A proposta é avaliada em múltiplos conjuntos de dados, incluindo dados coletados por um sistema de sensoriamento distribuído desenvolvido e implantado no laboratório do Grupo de Teleinformática e Automação (GTA) da UFRJ, e apresenta uma melhora de desempenho expressiva em tarefas de classificação quando comparada a arquiteturas similares que utilizam a divisão de dados clássica, com o custo de uma segunda etapa de ajuste de hiperparâmetros.

Bochie, K.; Gilbert, M. S.; Gantert, L.; Barbosa, M. S. M.; Medeiros, D. S. V.; Campista, M. E. M. Aprendizado profundo em redes desafiadoras: conceitos e aplicações. Em: Minicursos do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC). Rio de Janeiro, 2020.

Goodfellow, I.; Bengio, Y.; Courville, A. Deep Learning. MIT Press, 2016.
Disponível em <http://www.deeplearningbook.org>.

Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-Balot—network-based detection of IoT bot-net attacks using deep autoencoders, Em IEEE Pervasive Computing, 2018. Vol. 17. p. 12–22.