Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente / Redes de Computadores

Título: Análise e Predição de Tráfego na Internet usando Deep Learning

Orientador – Bruno José Torres Fernandes (bjtf@ecomp.poli.br)

Coorientador – Edison de Queiroz Albuquerque (edison@ecomp.poli.br)

Descrição

Monitoramento de tráfego é uma tarefa mandatória para que se possa dimensionar os recursos de rede necessários para que os serviços prestados sejam dotados de qualidade suficiente para satisfazer as expectativas dos usuários. Além disso, o estudo do tráfego permitirá identificar tráfego malicioso, classificando-o de modo que se possa tomar a atitude de contra-medida necessária.

Na década de 80, os estudos realizados para dimensionamento de redes de computadores utilizavam a distribuição de Poisson, tanto para o tráfego entrante no roteador como para o tempo que o roteador levava para processar os datagramas, antes de enviá-los para frente. Em 1995 foi publicado um estudo [4] em que se mostrava que o tráfego da Internet não tinha um comportamento que obedecia a alguma função distribuição de probabilidade conhecida. A este tráfego deu-se o nome de auto-similar, ou fractal. Algumas propostas foram feitas para contornar este problema como, por exemplo, usar Poisson e somar um Fator de Autosimilaridade aos valores encontrados para tamanho dos buffers dos roteadores e banda dos enlaces [5].

Na ausência de um método mais determinístico para fazer o dimensionamento de rede, o uso de Redes Neurais Artificiais é proposto para fazer a classificação e a predição do comportamento do tráfego [2, 3]. Mais especificamente, pretende-se fazer o uso de conceitos mais atuais de *deep learning* com o uso de plataformas conhecidas como o TensorFlow [1].

Um modelo de rede neural apresentado recentemente na literatura chamado de Generative Adversarial Networks (GANs) [6] tem por objetivo a geração de um padrão artificial a partir de uma aprendizagem construída com entradas reais previamente apresentadas. A hipótese é que GANs podem ser usadas para simular tráfegos maliciosos e otimizar a capacidade da rede de detecção de tais eventos.

Referências Bibliográficas

- Aurélien Géron, **Hands-On Machine Learning with Scikit-Learn &TensorFlow**. Sebastopol, CA: O'Reilly Media, Inc., 2017.
- Zubair Md. Fadlullah, et. al., **State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems,** IEEE Communications Surveys &Tutorials (Volume: 19, Issue: 4, Fourthquarter 2017).
- M. Lopez-Martin et al., **Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things,** IEEEAccess, 2017.
- Will E. Leland et al., **On the Self-Similar Nature of Ethernet Traffic**, ACM SIGCOMM, Computer Communication Review, 1995.
- Daniel A Menasce, Virgilio AF Almeida, **Capacity Planning for Web Performance: Metrics, Models, and Methods**, Prentice Hall, 1998.
- I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville e Y. Bengio. Generative Adversarial Networks. Arxiv, 2014.