Evento	Salão UFRGS 2020: SIC - XXXII SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2020
Local	Virtual
Título	Detecção de Ataques de Negação de Serviço Utilizando Florestas Aleatórias em Planos de Dados Programáveis
Autor	BRUNO LOUREIRO COELHO
Orientador	ALBERTO EGON SCHAEFFER FILHO

Título: Detecção de Ataques de Negação de Serviço Utilizando Florestas Aleatórias em Planos de Dados Programáveis
Autor: Bruno Loureiro Coelho
Orientador: Alberto Egon Schaeffer-Filho
Origem: Departamento de Informática Aplicada (Instituto de Informática)
Universidade Federal do Rio Grande do Sul
Resumo: Atualmente, muitos serviços dependem de acesso à internet para sua utilização. Assim, mesmo uma breve disrupção na conexão pode causar indisponibilidades, possivelmente levando a grandes prejuízos. Logo, é importante a rápida detecção de possíveis ataques de negação de serviço, que buscam afetar a disponibilidade ou qualidade de serviços *online*, a fim de prevenir ou minimizar a degradação destes. Com avanços recentes em redes programáveis - especificamente com a possibilidade de programar o plano de dados de um roteador ou *switch*, existem novas possibilidades de como realizar a detecção deste tipo de ataque. Este trabalho propõe o uso de uma técnica de inteligência artificial, Florestas Aleatórias, em um *switch* programável, utilizando a linguagem P4 a fim de extrair *features* e realizar o processamento de árvores de decisão no plano de dados, provendo eficiência e acurácia na detecção de ataques de negação de serviço. Florestas aleatórias, através do uso de várias árvores de decisão, oferecem rápida classificação, também podendo atingir alta qualidade de predição. Porém, a fim de obter uma boa acurácia de classificação, é necessário selecionar *features* adequadas, que consigam ajudar na distinção de um ataque malicioso de um fluxo legítimo. Dentre as *features* selecionadas, é necessário calcular a média de alguns valores, como tamanho dos pacotes, tempo médio entre chegada de pacotes, etc. Uma limitação da linguagem P4, porém, é a falta da operação de divisão, necessária para o cálculo de médias. Assim, em um primeiro momento, foi proposta uma maneira de aproximar a média móvel utilizando apenas somas, subtrações e deslocamento de *bits*. O método proposto consegue aproximar a média melhor do que outras soluções conhecidas, como a média móvel exponencial. Nos testes realizados, a solução desenvolvida consegue aproximar a média exata com acurácia média de 99.74%.