Evento	Salão UFRGS 2022: SIC - XXXIV SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2022
Local	Campus Centro - UFRGS
Título	Estudo sobre estratégias de identificação e mitigação de ataques SYN Flood
Autor	NICOLLE PIMENTEL FAVERO
Orientador	ALBERTO EGON SCHAEFFER FILHO

Ataques DoS/DDoS (negação de serviço) existem desde os primórdios da Internet e nos últimos anos eles têm crescido em volume e quantidade. O maior ataque DDoS já registrado foi em 2017 com um tráfego de 2.54 Tbps, e o segundo maior quase conseguiu ultrapassá-lo em 2021, com 2.4 Tbps. Um dos vetores mais comuns de um ataque de negação de serviço é o SYN Flood, que se aproveita do three-way handshake do protocolo TCP. Nele, o atacante gera um grande fluxo de pacotes SYN solicitando conexão com o servidor, porém ele nunca envia os pacotes finais, deixando as conexões pendentes e, assim, saturando os recursos do alvo. Portanto, estudos para a identificação, classificação e mitigação desses fluxos maliciosos são uma necessidade e podem ser levados a outro patamar quando combinados com redes programáveis, um novo paradigma de redes de computadores que permite novas possibilidades de abordagens de diversos problemas, incluindo ataques DDoS. O objetivo geral do nosso trabalho é investigar estratégias de identificação e mitigação de ataques SYN Flood em planos de dados programáveis usando P4, a fim de encontrar um meio de evitá-los. Pretendemos alcançar o objetivo através de duas frentes: (1) entender estratégias para identificar se uma conexão está meio aberta com auxílio do plano de dados programável; (2) investigar técnicas para mitigar as consequências do recebimento de uma quantidade massiva de pacotes SYN. Como trabalho em andamento, buscamos reproduzir a implementação de técnicas de mitigação existentes a fim de identificar possíveis melhorias, e estamos desenvolvendo uma abordagem alternativa que busca contar e relacionar as quantidades de pacotes SYN e ACK que passam por uma topologia de rede para que se consiga extrair, armazenar e analisar informações sobre a situação da rede e sobre a origem dos pacotes maliciosos.