DETECÇÃO DE ATAQUES DDOS EM REDES PROGRAMÁVEIS

Rafael Dalosto [1]

Ariel Góes de Castro [2]

Angelo Geovanni Amaral Menezes [3]

Douglas Lima Machado [4]

Francisco Germano Vogt [5]

Marcelo Caggiani Luizelli [6]

Resumo:

O gerenciamento eficiente das infraestruturas de rede é essencial para manter os serviços e aplicações em operação. Os dispositivos de encaminhamento que compõe as infraestruturas (como, por exemplo, roteadores) possuem os planos de dados e de controle integrados, o que dificulta (ou mesmo, impossibilita) inovar quanto ao funcionamento desses dispositivos. Recentemente, novos paradigmas de funcionamento das infraestruturas surgiram como, por exemplo, as redes definidas por software (SDN - Software-Defined Network) e os planos de dados programáveis (P4 - Programming Protocol-Independent Packet Processors). De uma maneira breve, o paradigma SDN permite desacoplar a lógica de funcionamento do plano de controle dos dispositivos de encaminhamento - permitindo que a lógica de controle seja executada em qualquer lugar da infraestrutura (por exemplo, em um servidor remoto). Essa separação trás inúmeros benefícios para a operação das infraestruturas como, por exemplo, o desenvolvimento de políticas de roteamento de tráfego diferentes das empregadas atualmente. Por sua vez, o paradigma P4 permite definir quais operações primitivas que o plano de dados suportam. Isso permite que se tenha lógicas de funcionamento mais sofisticadas sendo executadas no próprio dispositivo. Um dos benefícios da integração desses dois paradigmas é a telemetria in-band realizada no plano de dados. A telemetria in-band consiste em encapsular (de maneira oportunística) informações de monitoramento nos pacotes do tráfego de produção. Essa alternativa permite fornecer maior visibilidade da infraestrutura de rede para os operadores, permitindo identificar prematuramente problemas ou ataques às infraestruturas de rede. Um dos tipos de ataques comum é o Distributed Denial of Service (DDoS). Nesse ataque, um grande número de pacotes forjados são transmitidos através da infraestrutura, o que acarreta em uma sobrecarga dos recursos e, potencialmente, a degradação de serviços em operação. Neste trabalho, o objetivo consiste em identificar ataques DDoS lançando mão de paradigmas emergentes como SDN e P4. Diferentemente de abordagens existentes que utilizam informações de monitoramento tradicional, ao se utilizar telemetria in-band, almeja-se coletar informações com uma granularidade menor - o que possibilita identificar ataques de maneira mais eficiente e com um custo operacional menor. Para tanto, projeta-se algoritmos baseados em aprendizado de máquina para coordenar quais informações de telemetria são coletadas pelos dispositivos. Ao se implementar tais algoritmos em uma infraestrutura com suporte a P4 e SDN, espera-se que ataques DDoS sejam mitigados em um tempo menor que os existentes na literatura.

Palavras-chave: DDoS, SDN, P4, temeletria in-band, plano de dados, plano de controle, granularidade

Modalidade de Participação: Iniciação Científica

DETECÇÃO DE ATAQUES DDOS EM REDES PROGRAMÁVEIS

[1] Aluno de graduação. rafael.ertmann.dalosto@gmail.com. Autor principal

[2] Aluno de graduação. agcdragong@gmail.com. Co-autor

[3] Aluno de graduação. AngeloGiovanniMenezes@gmail.com. Co-autor

[4] Aluno de graduação. douglaslimamachado@gmail.com. Co-autor

[5] Aluno de graduação. franciscogermanovogt@gmail.com. Co-autor

[6] Docente. marceloluizelli@unipampa.edu.br. Orientador

O gerenciamento eficiente das infraestruturas de rede é essencial para manter os serviços e aplicações em operação. Os dispositivos de encaminhamento que compõe as infraestruturas (como, por exemplo, roteadores) possuem os planos de dados e de controle integrados, o que dificulta (ou mesmo, impossibilita) inovar quanto ao funcionamento desses dispositivos. Recentemente, novos paradigmas de funcionamento das infraestruturas surgiram como, por exemplo, as redes definidas por software (SDN – Software-Defined Network) e os planos de dados programáveis (P4 – Programming Protocol-Independent Packet Processors). De uma maneira breve, o paradigma SDN permite desacoplar a lógica de funcionamento do plano de controle dos dispositivos de encaminhamento – permitindo que a lógica de controle seja executada em qualquer lugar da infraestrutura (por exemplo, em um servidor remoto). Essa separação trás inúmeros benefícios para a operação das infraestruturas como, por exemplo, o desenvolvimento de políticas de roteamento de tráfego diferentes das empregadas atualmente. Por sua vez, o paradigma P4 permite definir quais operações primitivas que o plano de dados suportam. Isso permite que se tenha lógicas de funcionamento mais sofisticadas sendo executadas no próprio dispositivo. Um dos benefícios da integração desses dois paradigmas é a telemetria in-band realizada no plano de dados. A telemetria in-band consiste em encapsular (de maneira oportunística) informações de monitoramento nos pacotes do tráfego de produção. Essa alternativa permite fornecer maior visibilidade da infraestrutura de rede para os operadores, permitindo identificar prematuramente problemas ou ataques às infraestruturas de rede. Um dos tipos de ataques comum é o Distributed Denial of Service (DDoS). Nesse ataque, um grande número de pacotes forjados são transmitidos através da infraestrutura, o que acarreta em uma sobrecarga dos recursos e, potencialmente, a degradação de serviços em operação. Neste trabalho, o objetivo consiste em identificar ataques DDoS lançando mão de paradigmas emergentes como SDN e P4. Diferentemente de abordagens existentes que utilizam informações de monitoramento tradicional, ao se utilizar telemetria in-band, almeja-se coletar informações com uma granularidade menor – o que possibilita identificar ataques de maneira mais eficiente e com um custo operacional menor. Para tanto, projeta-se algoritmos baseados em aprendizado de máquina para coordenar quais informações de telemetria são coletadas pelos dispositivos. Ao se implementar tais algoritmos em uma infraestrutura com suporte a P4 e SDN, espera-se que ataques DDoS sejam mitigados em um tempo menor que os existentes na literatura.