Uma Abordagem de Aprendizado de Máquina Para Detecção Híbrida de Ataques no Plano de Dados SDN

Adiel Nascimento [1], **Diego Abreu** [1], **Antônio Abelém** [1]

[1]Grupo de Estudo em Redes de Computadores e Comunicação Multimídia (GERCOM)
Universidade Federal do Pará (UFPA)

adiel@cpqd.com.br, diegoabreuengcomp@gmail.com, abelem@ufpa.br

Abstract. *The programmability of the SDN data plane allows users to write algorithms that define how network devices should process packets, including the use of programming interfaces (APIs) to take advantage of the network controller. With this great flexibility, the use of machine learning applications has been proposed for packet classification and attack detection. In this scenario, trained models are used to complete the action and correspondence table of pipeline P4 offering equal detection and processing time. Another approach used is network telemetry, which allows obtaining information on the state of the network and using it by applications running on the controller or external agent. In contrast, this work advances the state of the art by proposing a hybrid AM management architecture for SDN networks, combining the use of the P4 pipeline and strategic agents in the network to provide detection of multilevel attacks.*

Resumo. *A programabilidade do plano de dados SDN permite que os usuários escrevam algoritmos que definem como os dispositivos de rede devem processar os pacotes, incluindo o uso de interfaces de programação (APIs) para aproveitar o controlador de rede. Com essa grande flexibilidade, o uso de aplicativos de aprendizado de máquina tem sido proposto para classificação de pacotes e detecção de ataques. Neste cenário, modelos treinados são usados para completar a tabela de ações e correspondências do pipeline P4 oferecendo igual tempo de detecção e processamento. Outra abordagem utilizada é a telemetria de rede, que permite obter informações sobre o estado da rede e utilizá-las por aplicativos executados no controlador ou agente externo. Em contrapartida, este trabalho propõe uma arquitetura de gerenciamento AM híbrida para redes SDN, combinando o uso do pipeline P4 e agentes estratégicos na rede para fornecer detecção de ataques multinível.*

1. Introdução

O paradigma de Rede Definida por *Software* (*Software Define Network* - SDN) tem sido amplamente estudado na última década [Prabakaran et al. 2019]. Sua principal característica é a separação entre o plano de dados e o plano de controle, permitindo melhor gerenciamento, controle, atualização dinâmica das regras, análise e visão global da rede utilizando um controlador centralizado. Por outro lado, o papel central do controlador o torna um alvo preferencial para ataques cibernéticos maliciosos. Além disso, ainda que os ataques não sejam direcionados ao controlador, as políticas de encaminhamento da rede podem sobrecarregá-lo comprometendo o devido funcionamento da rede.

Nesse contexto, diversas abordagens foram estudadas para identificar fluxos ativos em uma rede de computadores. Tradicionalmente, a carga útil dos pacotes e informações do cabeçalho são utilizados para tal [Amaral et al. 2016]. Porém, esse tipo de abordagem possui deficiências e Técnicas de Aprendizado de Máquina tem sido utilizadas para substituir a abordagem tradicional. O fluxo de trabalho de um modelo de AM, geralmente, segue uma sequência baseada em: pré-processamento de dados, extração de recursos, ajustes de modelos e validação. Dessa forma, balancear a execução desse processo entre os planos de controle e de dados de uma rede SDN é um desafio em aberto.

Ao centralizar a solução diretamente no controlador, aumenta-se a latência no tempo de detecção de ataques, que aumenta proporcionalmente com o número de dispositivos de rede sob autoridade do controlador [Bosshart et al. 2014]. Por outro lado, utilizar a programabilidade no plano de dados com o uso da linguagem de Pacotes Independentes de Protocolo de Programação (*Programming Protocol-Independent Packet Processors* - P4) para executar todo o processo de AM nos *switches*, pode implicar em uma sobrecarga de processamento, comprometendo as funções básicas desses equipamentos, como processamento das informações do cabeçalho, o controle de acesso ao meio, encaminhamento e filtragem de quadros.

Diante do exposto, o objetivo deste trabalho é propor e discutir com a comunidade uma arquitetura híbrida para detecção multinível de ataques em redes SDN. Para isso, pretende-se utilizar a junção de dois conceitos aplicados no plano de dados SDN, são eles: mapeamento de Modelos de AM no pipeline P4 e o uso de telemetria da rede para detecção de ataques. Desta forma, pode-se desenvolver mecanismos mais simples para execução nos *switches* e mecanismos complexos que sejam executados no controlador ou em outro agente externo. O trabalho está organizado da seguinte forma. A Seção 2 aborda os trabalhos relacionados. Em seguida, a Seção 3 apresenta a proposta, enquanto a Seção 4 realiza uma discussão sobre o funcionamento da proposta. Por fim, a Seção 5 conclui o trabalho e aponta os trabalhos futuros.

2. Trabalhos Relacionados

A detecção de ataques de negação de serviço (DoS) é proposta em diversos trabalhos no contexto da segurança cibernética. [Zargar et al. 2013] explora o escopo do problema do ataque de inundação DDoS e tentativas de mitigação. Categoriza-se os ataques de inundação de DDoS e classificando as contramedidas existentes com base em onde e quando elas previnem, detectam e respondem aos ataques de inundação de DDoS.

A evolução das redes tradicionais para o paradigma SDN possibilitou novas implementações de detecção e mitigação de ataques distribuidos de negação de serviço (DDoS) utilizando o plano de dados, como em [Carvalho et al. 2021]. Nesse contexto, [RT et al. 2014] utiliza o classificador SVM para detecção ataques DDoS que levam o controlador à exaustão de recursos. Em seguida, o classificador SVM é comparando com outros classificadores para detecção de DDoS. Os experimentos mostram que o SVM realiza uma classificação mais precisa do que outros no cenário do trabalho.

Como último avanço do paradigma SDN, as redes SDN-NG de nova geração possibilitaram inovações com o plano de dados programável. Nesse cenário, novos trabalhos buscando proveito dos benefícios do plano de dados programável foram propostos. [Lin et al. 2020] definiu um mecanismo para detectar ataques de inundação SYN e os ata-

ques *spoofing* em redes SDN, esse mecanismo detecta inundações de SYN com base em algumas regras de encaminhamento de pacotes. Além disso, a linguagem P4 é utilizada como técnica de mitigação para a carga do controlador, dando uma maior autonomia ma tomada de decisão para os *switches* da rede.

Em [Xiong and Zilberman 2019], é explorado o uso dos *switches* da rede para classificação de tráfego, apresentando um método de mapeamento de algoritmos supervisionados e não supervisionados para a criação de um *pipeline* de ação e correspondência. Além disso, o artigo discute a implementação e a aplicabilidade das mesmas destacando as dificuldades e benefícios.

As propostas mencionadas representam passos consistentes no sentido de conceber mecanismos a serem executados no plano de dados, mas enfrentam dificuldades por conta heterogeneidade topológica de rede e limitações de capacidade de processamento dos dispositivos de rede. Por outro lado, centralizar o monitoramento e detecção em dispositivos externos como servidores dedicados atrasam a detecção de ataques e levando a uma alta utilização da rede. Este trabalho avança o estado da arte permitindo o uso de diferentes abordagens em simultâneo. Desse modo, é possível contornar as dificuldades de ambas as abordagens e minimizar suas desvantagens.

3. Proposta

A arquitetura proposta utiliza o mapeamento de modelos de AM no pipeline P4, associado com o uso de telemetria da rede para detecção de ataques, com o intuito de reduzir o atraso na detecção, sem sobrecarregar os switches.

3.1. Uso de Telemetria da Rede Para Detecção

A telemetria de rede (Inband Network Telemetry - INT) é uma estrutura projetada para permitir a coleta e geração de relatórios do estado da rede, pelo plano de dados, sem exigir intervenção ou trabalho do plano de controle, coletando e entregando o estado do plano de dados. Dessa forma, propícia melhor escalabilidade, precisão, cobertura e desempenho da rede ao permitir o desenvolvimento de controles automatizados para atender aos requisitos de operação de rede. Nesse cenário, diversas aplicações podem ser desenvolvidas para tirar proveito desses recursos, como: análise de congestionamento, interface gráfica com alerta de anomalias e *dashboards*, retenção de dados e histórico de análises, rastreio de latência e encaminhamento, descoberta da topologia da rede e análise de descarte de pacotes.

Na Figura 1, mostra-se um switch que utiliza a telemetria de rede para espelhar os metadados para um servidor, que utiliza esses dados para gerar os modelos de classificação e monitorar o tráfego. Os dados são recebidos pelo framework de treino que tem como saída um modelo treinado. Em seguida, o classificador utiliza o modelo para classificar os pacotes recebidos via telemetria de rede e envia mensagens solicitando o descarte dos pacotes identificados como maliciosos. O controle de plano de dados é responsável por essa comunicação através do uso de APIs, que podem ser desenvolvidas pelo administrador da rede ou fornecidas por algum repositório.

Essa categoria de abordagem possui a vantagem de poder contar com *hardware* dedicado para o uso de aprendizado de máquina. No entanto, implementar essa categoria de servidor em todos os pontos da rede aumenta o custo da topologia. Além disso,

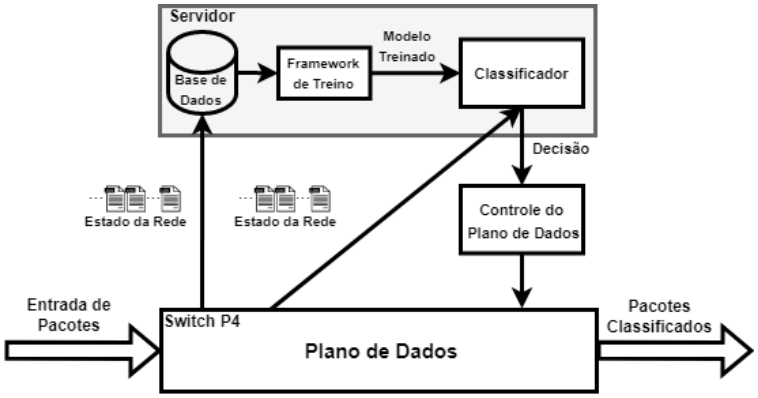

Figura 1. Exemplo de envio de dados de telemetria para um servidor IDS.

existe uma latência maior na classificação dos pacotes ou fluxos quando comparado com aplicações diretamente nos switches.

3.2. Mapeamento de Modelos de AM no Pipeline P4

O mapeamento de modelos de AM para o pipeline da linguagem P4 permite habilitar esse tipo de solução no plano de dados SDN. Para tal, a similaridade entre uma árvore de decisão e o pipeline P4 pode ser explorada para mapear as estruturas de decisões da árvore na tabela de ação e correspondência do pipeline P4. Na Figura 2, é possível visualizar um pipeline P4 obtido a partir de uma estrutura de uma árvore de decisão. O programa P4 precisa inicialmente descrever como os pacotes serão encaminhados. Em seguida, os nós de decisão da árvore são mapeados na tabela de ação e correspondência. Por fim, as folhas são utilizadas para chamar as ações pré definidas no código P4.

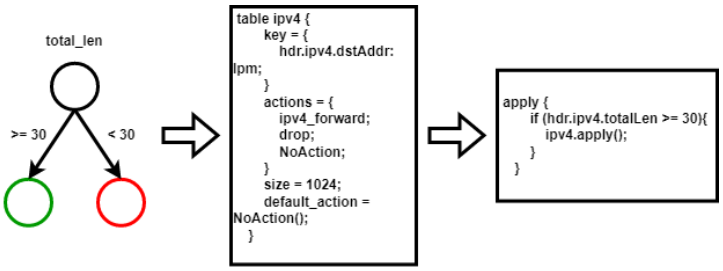

Figura 2. Exemplo de Mapeamento de uma pipeline P4

A Figura 2 mostra um exemplo de programa P4 escrito para classificar pacotes utilizando o tamanho total como critério de escolha. Nesse caso, o encaminhamento do pacote ipv4 através da função ipv4.apply() está condicionada a aplicação da regra, encaminhando pacotes com tamanho total maior ou igual a 30, e descartando pacotes menores que 30. A utilização desse tipo de abordagem permite oferece flexibilidade para implementar prontamente novos algoritmos de processamento de pacotes no switch. Os algoritmos implementados podem assumir um fluxo de pacotes como entradas e processá-los com o uso de primitivas elementares, acesso à memória e pesquisas de tabela.

A técnica apresentada na Figura 2 pode ser aplicada na arquitetura da Figura 3. Para isso, uma base de dados contendo a assinatura dos ataques alvos é utilizada para alimentar o framework de treino. Após isso, o modelo treinado obtido é mapeado para o

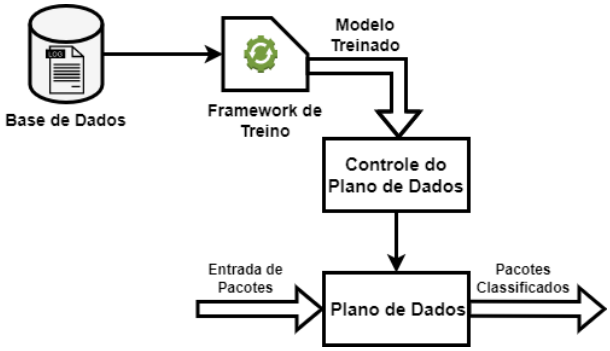

Figura 3. Exemplo de Mapeamento de uma pipeline P4

pipeline P4 e o switch passa a processar os pacotes conforme a estrutura de decisão do modelo de AM.

3.3. Arquitetura Híbrida

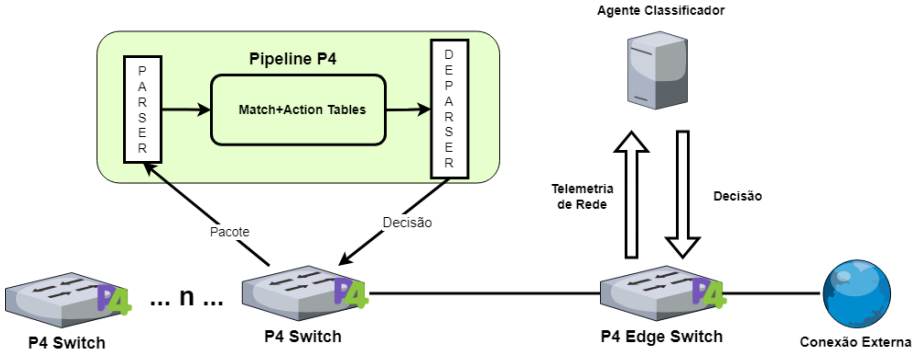

Figura 4. Arquitetura Híbrida para Soluções de AM no Plano de Dados SDN.

Partindo disso, este trabalho propõe explorar uma arquitetura hibrida mostrada na Figura 4. Os switches internos da rede executam um programa P4 para identificar ataques mais simples diretamente no processamento dos pacotes, possibilitando a diminuição da latência na identificação desses ataques. Outra vantagem importante é a possibilidade de escalar a proposta, garantindo o mínimo impacto ao controlador.

Em paralelo, o switch de borda utiliza a programabilidade de rede para espelhar os metadados para um servidor com CPU e GPU dedicados ao processamento de AM, que utiliza os dados para gerar os modelos e monitorar o tráfego. Isso permite explorar os switches de borda para coleta de dados de telemetria em banda para treinar os modelos, e classificar o tráfego de rede. O uso da telemetria, permite captar uma maior granularidade dos dados de rede, o que pode ajudar a identificar ataques que utilizam tráfego genuíno a partir de dispositivos sequestrados, tal como ataques que conseguem variar seus parâmetros. Normalmente esse tipo de ataque é de origem externa da rede, justificando o posicionamento do IDS em ponto um ponto estratégico da rede como junto ao switch de borda.

4. Considerações Finais

Este trabalho apresentou uma arquitetura alternativa para o desenvolvimento de arquiteturas hibridas baseada AM para o plano de dados. Tal arquitetura aumenta a independência

dos *switches* em relação ao controlador na tomada de decisões rápidas. A arquitetura hibrida pode fornecer um sistema multi-camadas para detecção de ataques em redes SDN, permitindo a implementação de uma ou mais técnicas de AM. Além disso, a telemetria da rede permite automatizar o dimensionando dessas soluções considerando características topológicas da rede.

Os próximos passos deste trabalho consistem na implementação e validação da arquitetura proposta em ambiente emulado e experimental. Com o dimensionamento da arquitetura, será possível avaliar o desempenho da proposta em diversos casos de uso.

5. Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior Brasil (CAPES) e do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD).

Referências

Amaral, P., Dinis, J., Pinto, P., Bernardo, L., Tavares, J., and Mamede, H. S. (2016). Machine learning in software defined networks: Data collection and traffic classification. In *2016 IEEE 24th International Conference on Network Protocols (ICNP)*, pages 1–5.

Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., and Walker, D. (2014). P4: Programming protocol-independent packet processors. *SIGCOMM Comput. Commun. Rev.*, 44(3):87–95.

Carvalho, R. N., Costa, L. R., Bordim, J. L., and Alchieri, E. A. P. (2021). Detecting ddos attacks on sdn data plane with machine learning. In *2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW)*, pages 138–144.

Lin, T. Y., Wu, J. P., Hung, P. H., Shao, C. H., Wang, Y. T., Cai, Y. Z., and Tsai, M. H. (2020). Mitigating syn flooding attack and arp spoofing in sdn data plane. In *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 114–119.

Prabakaran, P., Isravel, D. P., and Silas, S. (2019). A review of sdn-based next generation smart networks. In *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, pages 80–85.

RT, K., Thamarai Selvi, S., and Govindarajan, K. (2014). Ddos detection and analysis in sdn-based environment using support vector machine classifier. In *2014 Sixth International Conference on Advanced Computing (ICoAC)*, pages 205–210.

Xiong, Z. and Zilberman, N. (2019). Do switches dream of machine learning? toward in-network classification. In *Proceedings of the 18th ACM Workshop on Hot Topics in Networks*, HotNets '19, page 25–33, New York, NY, USA. Association for Computing Machinery.

Zargar, S. T., Joshi, J., and Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys Tutorials*, 15(4):2046–2069.