Criação de Redes Virtuais no MENTORED *Testbed*: Uma Análise Experimental

Bruno Henrique Meyer[1], **Davi Daniel Gemmer**[2], **Allex Magno Andrade**[3,4], **Emerson Ribeiro de Mello**[3], **Michele Nogueira**[1,2], **Michelle Silva Wangham**[4,5]

[1]Universidade Federal do Paraná - UFPR

[2]Universidade Federal de Minas Gerais - UFMG

[3]Instituto Federal de Santa Catarina - IFSC

[4]Rede Nacional de Ensino e Pesquisa - RNP

[5]Universidade do Vale do Itajaí - UNIVALI

Abstract. *The MENTORED Testbed aims at supporting research in prevention, detection, and mitigation of DDoS attacks in IoT. It handles a high volume of network traffic and a large number of participating devices. The testbed implementation overlays the Software Defined Infrastructure from the National Research and Education Network (IDS-RNP), which supports different technologies for creating virtual networks (Macvlan, KNetLab, and Calico). This work describes the MENTORED testbed experiments conducted with each of the network technologies to determine the advantages and drawbacks of the testbed use.*

Resumo. *O MENTORED Testbed auxilia pesquisas na área de prevenção, detecção e mitigação de ataques de DDoS em IoT. O ambiente lida com um alto volume de tráfego de rede e um grande número de dispositivos. Sua implementação justapõe a Infraestrutura Definida por Software da Rede Nacional de Ensino e Pesquisa (IDS-RNP) que suporta diferentes tecnologias para criação de redes virtuais (Macvlan, KNetLab e Calico). Este trabalho descreve os experimentos do ambiente conduzidos com cada uma das tecnologias de rede a fim de avaliar as vantagens e as limitações do seu uso.*

1. Introdução

A Internet of Things (IoT) tem atraído a atenção da indústria e da comunidade científica por inserir um número elevado de dispositivos conectados à rede e por se adequar aos mais variados casos de uso. Por apresentarem baixa capacidade de processamento, não é possível implementar mecanismos de segurança robustos. Desta forma, dispositivos IoT apresentam vulnerabilidades intrínsecas, que uma vez que forem exploradas, podem expor dados sensíveis de seus usuários ou ainda, podem participar de ataques de negação de serviço distribuído [Antonakakis et al. 2017].

Existem diferentes ambientes experimentais (*testbeds*) que visam dar suporte a pesquisas voltadas à prevenção, detecção e mitigação de ataques DDoS focados na IoT [Yusof et al. 2019, Rahal et al. 2020]. Esses ambientes são fundamentais para o desenvolvimento de soluções que tratam estes ataques, uma vez que montar um ambiente

real é custoso e demanda um grande investimento de tempo e de recursos sejam eles financeiros, computacionais e de rede. Tais demandas acabam por inviabilizar a pesquisa experimental, cada vez mais necessária para o progresso científico.

Diante deste cenário, o projeto MENTORED[1] visa à criação de um ambiente experimental capaz de suprir a demanda de pesquisadores por um ambiente para realização de testes relacionados a suas pesquisas sobre prevenção, detecção e mitigação de ataques DDoS na IoT. Além da construção do *testbed*, o projeto estuda atividades maliciosas em dispositivos IoT e desenvolve técnicas para predição, detecção e mitigação de ataques DDoS. Em trabalho anterior [Prates Jr et al. 2021], foi apresentada a modelagem da arquitetura do MENTORED *Testbed* e os esforços iniciais de seu desenvolvimento e uso.

A implementação do MENTORED *Testbed* toma como base a Infraestrutura Definida por Software da Rede Nacional de Ensino e Pesquisa (IDS-RNP) da RNP. Esta infraestrutura tem por objetivo atender às demandas de projetos de pesquisa acadêmicos na área de redes de computadores. A IDS-RNP utiliza a tecnologia Kubernetes e é composta por diversos servidores de processamento (*workers*) distribuídos pelos pontos de presença (PoPs) da rede Ipê gerenciada pela RNP. A quantidade de recursos disponibilizada é dinâmica e, assim, é possível que novos recursos sejam adicionados nos PoPs participantes da IDS-RNP ou o ingresso de novos PoPs.

Dentre os requisitos considerados na criação de *testbeds* para IoT, está a necessidade de gerar um grande volume de tráfego de rede pelas características dos ataques DDoS e por serem mais comuns em cenários com dispositivos IoT. Este trabalho apresenta alguns refinamentos da arquitetura do MENTORED *Testbed* e descreve uma pesquisa experimental sobre as tecnologias Macvlan, KNetLab e Calico utilizadas na criação de redes virtuais com o Kubernetes da IDS-RNP. Estes experimentos têm o objetivo de avaliar as vantagens e as limitações do seu uso no MENTORED *Testbed*. A tecnologia KNetlab foi escolhida devido ao seu potencial para simplificar a definição de topologias de redes complexas, o que pode ser um requisito para usuários de um *Testbed* de segurança. A tecnologia Calico foi escolhida devido à sua simplicidade de implementação e configuração. Por fim, a tecnologia Macvlan foi escolhida devido à sua baixa composição de componentes virtuais necessários para prover uma interface de rede para contêineres no Kubernetes.

Neste trabalho foram conduzidos experimentos com o Kubernetes, usado pelo IDS-RNP, para simular ataques DDoS em um servidor *web*. Além da vítima e dos atacantes, os experimentos contaram também com máquinas atuando como clientes corretos do serviço ofertado pela vítima. Foram coletados os tempos de respostas da vítima para atender cada pedido gerado pelo cliente. Por fim, também foram coletadas métricas relacionadas ao uso de CPU, memória RAM e tráfego de rede da vítima.

Este artigo procede como segue. A Seção 2 apresenta uma breve revisão da literatura para embasar o entendimento da pesquisa experimental conduzida. Na Seção 3, é apresentado o *Mentored Testbed*. A metodologia e os experimentos são apresentados na Seção 4. Na Seção 5, os resultados obtidos com os experimentos são analisados. Por fim, a Seção 7 conclui o trabalho e apresenta as direções futuras.

[1] `https://www.mentoredproject.org/about`

2. Revisão da Literatura

Um ataque real DDoS é gerado a partir de uma rede composta por uma grande quantidade de dispositivos infectados, oriundos de diferentes redes, espalhados geograficamente e com diferentes capacidades computacionais e de transmissão de dados. O uso de *testbeds* para avaliação de técnicas de cibersegurança e criação de *datasets* é relevante e traz maior rigor científico para os trabalhos acadêmicos. Contudo, a reprodução fiel de ataques DDoS em *testbeds* é uma limitação conhecida e algumas propostas tentam minimizá-la. Em [Zhu et al. 2022], os autores apresentam uma análise dos principais *testbeds* e concluíram que o gerenciamento de recursos é um desafio que precisa ser resolvido durante a construção de *testbeds*.

O Deterlab [Wroclawski et al. 2016, Mirkovic and Benzel 2013] é um dos principais *testbeds* disponíveis para pesquisa experimental em cibersegurança, sendo financiado por agências como NSF, DHS, e DARPA. Contudo, ele possui limitações relacionadas à usabilidade e especificidade para a experimentação com topologia de redes que considerem dispositivos IoT [Prates Jr et al. 2021]. Por exemplo a consideração de heterogeneidade de dispositivos presentes na topologia solicitada pelo usuário e as suas conexões. Em [Koroniotis et al. 2019], os autores utilizaram um *testbed* construído especificamente para criar uma base de dados chamada Bot-IoT. Porém, essa base considera um número baixo e fixo de dispositivos IoT. Em [Lee et al. 2018], os autores apresentam um *testbed* focado em IoT, porém os resultados apresentado não consideraram o desafio de se ter um ambiente de larga escala.

Quando um *testbed* é criado com a finalidade de atender a diversos experimentos, é importante definir uma tecnologia capaz de gerenciar os recursos disponíveis, como o Kubernetes [Prates Jr et al. 2021]. O Kubernetes é uma sistema de código aberto que permite a implantação, escalonamento e gerenciamento de aplicações disponibilizadas dentro de contêineres. Em um *cluster* Kubernetes, diversas outras tecnologias podem ser incorporadas, como as que gerenciam o tráfego de rede e as interfaces de redes de contêineres, ou *Container Networking Interface* (CNI). Junto com os enlaces físicos entre os dispositivos do *cluster*, as tecnologias de redes limitam o tráfego que pode ser gerado na experimentação de ataques. Isto é um problema no caso de ataques de DDoS que tem por natureza gerar grandes volumes de tráfego.

Em [Kapočius 2020], foi feita uma comparação entre diferentes tecnologias e modelos para criação de redes virtuais disponíveis no Kubernetes. O trabalho comparou a vazão de rede oferecida por cada tecnologia com a versão *baremetal*, onde nenhuma tecnologia de conteinerização ou virtualização foram utilizadas. O trabalho concluiu que as tecnologias de virtualização não apresentaram uma redução na vazão de rede. Porém, diversas limitações estavam presentes nos experimentos realizados, como o fato de desconsiderarem cenários de ataques cibernéticos e a topologia contava com apenas três locais diferentes, interconectados por meio de uma rede de longa distância.

Em [Prates Jr et al. 2021], definiu-se que o MENTORED *testbed* deve ser capaz de suportar experimentos em tamanho suficiente para ser representativo para capturar efeitos complexos dos ataques com tráfego massivo de dados na escala da Internet. A arquitetura do MENTORED *Testbed* se apoia nas redes de longa distância, nos recursos com alta disponibilidade e na modularidade da plataforma Kubernetes para criar cenários experimentais com redes heterogêneas, com conexões fim-a-fim e ambientes em nuvem.

3. MENTORED *Testbed*

Na Figura 1 é apresentada a arquitetura do MENTORED *Testbed*. o *MENTORED Master*, responsável por autenticar, controlar e gerenciar ações relacionadas às permissões de usuários usando uma *Clearinghouse*. O módulo MENTORED Master é o responsável por intermediar a interação de seus usuários com os recursos disponibilizados na IDS-RNP. O módulo *Worker* é responsável por instanciar os *pods* Kubernetes, sendo que nos *pods* são executadas as aplicações da vítima, cliente e atacante. O *MENTORED Master* oferece uma interface de linha de comando (*Command Line Interface* – CLI) e interface *web* (Portal MENTORED). Essas interfaces são usadas pelos usuários para instanciarem seus experimentos e coletarem os dados gerados. Esses experimentos serão então validados por um submódulo nomeado orquestrador, que é responsável por alocar os devidos recursos na IDS-RNP via Kubernetes.

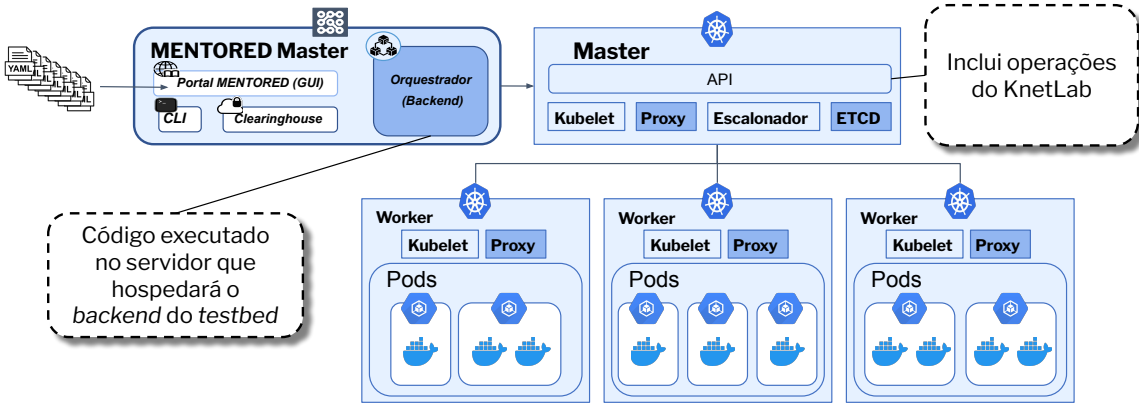


Figura 1. Arquitetura do MENTORED *Testbed*.

Na IDS-RNP, existe um nó central do *cluster* denominado *Master*, que é responsável por criar a topologia e iniciar o experimento. A topologia pode ser composta por um número arbitrário de nós, que serão instanciados sobre computadores físicos, denominados *workers*, que fazem parte da IDS-RNP. O IDS-RNP oferece diferentes tecnologias e modelos de virtualização de rede, além de funcionalidades de *plugins*.

Na Figura 2 é apresentado o fluxo para execução de um experimento no MENTORED *Testbed*. Após ser autenticado e autorizado, o usuário deve descrever o experimento com a linguagem YAML (em um formato de descrição específico do Testbed) e encaminhar tal descrição ao MENTORED Master. Se a descrição estiver correta, então é realizada a orquestração e o experimento é iniciado. Após o experimento ser iniciado, o usuário recebe as instruções para que possa acessar remotamente cada nó da topologia de seu experimento, usando a interface de linha de comando ou interface *web*, por meio da ferramenta *Web Kubectl*[2]. O usuário poderá monitorar em tempo real o experimento por meio da ferramenta *KNetLab Operator*. Um guia para condução de experimentos foi elaborado pela equipe do projeto e um vídeo foi gravado para demonstrar como executar um experimento básico usando o MENTORED *testbed*[3].

[2]`https://github.com/KubeOperator/webkubectl`

[3]Estes materiais estão disponível em `https://bit.ly/3hfe1rE` e `https://youtu.be/PzeDiObNOWY`, respectivamente

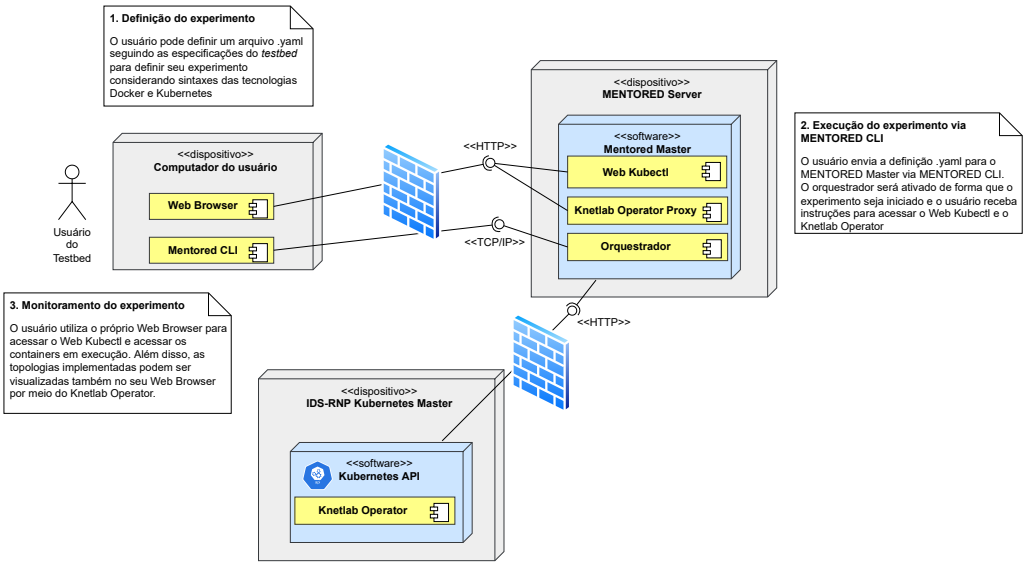


Figura 2. Diagrama de implantação do MENTORED *Testbed* e ilustração de um fluxo de execução de um experimento pela perspectiva do usuário.

A IDS-RNP oferece diferentes tecnologias para criação de redes virtuais e tal flexibilidade pode tornar mais difícil a experiência do usuário do *testbed*, uma vez que esse pode não ter o conhecimento sobre qual tecnologia é a mais adequada para condução de seus experimentos. Sendo assim, constatou-se a necessidade de compreender o comportamento de cada tecnologia para criação de redes virtuals, quando empregadas em experimentos com ataques como o DDoS, foco de interesse do MENTORED *Testbed*. Um ataque DDoS produz uma grande vazão de rede no alvo atacado a fim de exaurir seus recursos, acarretando assim na negação de serviço e impedimento que a vítima consiga atender os pedidos de clientes corretos. Contudo, em um *testbed* a própria rede pode ser comprometida quando estressada devido a sua limitação de recursos comparada à Internet como um todo. Dessa forma, é possível que o serviço seja negado por limitações dos recursos ou das tecnologias utilizadas.

Particularmente sobre as tecnologias e modelos de rede Kubernetes, que é a base do MENTORED *Testbed*, a conectividade é sua parte central. Desta forma, existem diferentes maneiras de implementar modelos de conectividade no *cluster*. No Kubernetes, a *Container Network Interface* (CNI) apoia a rede por meio de abordagens de redes definidas por *software* (SDN). A CNI consiste em especificações e bibliotecas entre os tempos de execuções do contêiner e os *plugins* CNI. Por meio da padronização da interface, a CNI fornece serviços de rede adequados para o tempo de execução do contêiner, na qual considera apenas a rede e a remoção de recursos alocados quando o contêiner é eliminado [Cha and Kim 2021]. Existem diferentes modelos de CNI, *plugins* e protocolos utilizados pelo Kubernetes com características distintas.

O Multus, por exemplo, corresponde a um *plugin* Multi CNI, utilizado pelo Kubernetes para suportar recursos *multi-networking*. O multus permite que várias interfaces de redes possam ser anexadas aos *pods*[4], possui suporte a diferentes CNI como o Ca-

[4]Um *pod* consiste na menor unidade de uma aplicação do Kubernetes, equivalente aos conceitos de contêineres ou máquinas virtuais.

lico e diferentes *plugins* como por exemplo o Macvlan [Kubernetes 2022]. O Calico é uma CNI que utiliza os princípios de roteamento da pilha nativa do Linux no tráfego dos dispositivos com conectividade Camada 2 ou Camada 3.

As informações de roteamento em cada dispositivo são transmitidas com o protocolo *Border Gateway Protocol* (BGP). O Calico oferece suporte a recursos *Network Policy* para regras de política de entrada e saída. O seu estado e configuração são mantidos no banco de dados *etcd* do *cluster* [Caban 2019]. Dois protocolos de rede comuns utilizados para o encapsulamento são VXLAN e IP-in-IP. O VXLAN consiste em uma tecnologia que possibilita o *overlay* de uma rede de Camada 2 em um *underlay* de Camada 3. Ele possui suporte para qualquer protocolo de roteamento IP e utiliza encapsulamento MAC em UDP [Mahalingam et al. 2014]. O IP-in-IP é um protocolo de encapsulamento IP para conexões que possuem capacidades ou políticas diferentes [Simpson et al. 1995].

O Macvlan é um *plugin* que funciona de forma similar a um *switch* conectado à interface do *host*, um dispositivo físico que é compartilhado com as interfaces virtuais. As interfaces do Macvlan são subinterfaces de uma interface *Ethernet* principal, sendo que cada uma possui endereço MAC individual e pode ser atribuído um endereço IP. Sua principal utilização é na virtualização de interfaces de redes em contêineres [CNI 2020].

O KNetLab é uma ferramenta utilizada na formação de redes em contêineres por meio do OpenvSwitch. Através da utilização de princípios de *Cloud Native*, o KNetLab permite criar redes virtuais em escala para a homologação e testes de redes [Hernandez 2021]. O OpenvSwitch (OVS) corresponde a um *software* projetado para a implementação de um *switch* virtual. É utilizado no encaminhamento de tráfego em ambientes virtualizados como contêineres e maquinas virtuais (VMs) [Pfaff and Davie 2013].

4. Metodologia e experimentos

Nesta seção, são apresentados dois cenários e experimentos conduzidos para determinar o comportamento das tecnologias Macvlan, KNetLab e Calico, quando usadas em experimentos que simulam um ataque DDoS direcionado para um único nó vítima. Na Tabela 1 é apresentada a lista de nós (*worker* Kubernetes) da IDS-RNP que foram usados na condução dos experimentos. Além da capacidade computacional de cada nó (CPU e memória RAM), a tabela apresenta em qual PoP da RNP o nó encontra-se. Os nós do tipo `ids` são servidores de processamento de alta capacidade e os nós do tipo `whx` são *switches white box* que possuem menor poder computacional, porém podem ser usados da mesma forma que os nós do tipo `ids`.

Cada cenário é composto por uma única vítima com uma aplicação que sofre o ataque; por um conjunto de clientes, que desejam acessar os recursos providos pela vítima, porém sem cometer qualquer tipo de abuso; e por um conjunto de atacantes, que objetivam esgotar os recursos da vítima e assim resultar na negação do serviço. A diferença entre os cenários está no número de clientes corretos e no número de atacantes.

No **cenário 1**, tem-se um único cliente, sendo este executado em um *pod*, de forma exclusiva, no nó `whx-SP` e tem-se somente um atacante, sendo este executado em um *pod*, de forma exclusiva, no nó `whx-BA`. O **cenário 2** é composto por doze clientes e por dez atacantes. Cada cliente ou atacante é executado em um único *pod*, porém, um mesmo nó (*worker*) executa mais de um *pod*. Na Tabela 2 é apresentada a quantidade de *pods* vítima, cliente e atacante instanciada em cada nó da IDS-RNP.

Tabela 1. Características dos nós IDS-RNP usados nos experimentos

Nó (*worker*)		Número de CPU	memória RAM (GB)
Tipo	PoP RNP		
ids	ES	48	188
ids	GO	48	188
ids	MG	48	188
ids	SC	48	188
ids	PE	24	174
whx	BA	8	16
whx	ES	8	16
whx	PA	8	16
whx	SP	8	16

Tabela 2. Disposição dos *pods* da vítima, clientes e atacantes nos nós

Cenário	Vítima		Atacantes		Clientes	
	Quantidade	Nó	Quantidade	Nó	Quantidade	Nó
1	1	whx-ES	1	whx-BA	1	whx-SP
2	1	whx-ES	2	ids-ES	4	whx-BA
			2	ids-GO	4	whx-PA
			2	ids-MG	4	whx-SP
			2	ids-SC		
			2	ids-PE		

Em ambos os cenários, a vítima consiste de um servidor *web* NGINX, com as configurações padrões e sem otimizações, que provê uma simples página HTML estática e que é executado, de forma exclusiva, em um *pod* no nó `whx-ES`. A aplicação cliente, desenvolvida em Python3 com a biblioteca `urllib`, faz simples requisições HTTP a cada 0,5 segundos com o intuito de obter a página HTML provida pela vítima. Cada atacante executa o aplicativo hping3[5] com os parâmetros "`-S --faster -p 80`".

Para cada cenário apresentado acima foram conduzidos experimentos que variaram a tecnologia para criação de redes virtuais (Macvlan, KNetLab e Calico). A tecnologia Macvlan só foi avaliada no cenário 1 devido a limitações impostas pela IDS-RNP. O *pod* da vítima teve seus recursos limitados a 2GB de memória RAM e 2 núcleos de CPU. Os *pods* dos clientes e atacantes tiveram seus recursos limitados a 128 MB de memória RAM e um único núcleo de CPU.

O experimento tem duração total de 5 minutos. Os clientes iniciam suas requisições desde o instante 0 e aguardam 0,5 segundos entre cada requisição. O ataque começa 1 minuto após o início do experimento. Durante a execução do experimento, foi feito uso da ferramenta Netdata[6] para coleta do uso de recursos (memória RAM e CPU) de cada *pod*. Essas métricas foram coletadas com o intuito de verificar se os ataques DDoS tiverem capacidade de influenciar no uso dos recursos de memória e processamento do

[5] `http://www.hping.org`
[6] `https://www.netdata.cloud/`

servidor alvo. Isso é uma possível maneira de identificar se uma negação de serviço foi efetiva devido à criação de gargalo nos recursos mencionados, ou limitações relacionados ao tráfego de rede.

5. Resultados

O experimento descrito na Seção 4 foi executado 30 vezes com cada uma das tecnologias (KNetLab, Calico e Macvlan) no **cenário 1**. No **cenário 2**, o mesmo experimento foi executado 30 vezes com as tecnologia KNetLab e Calico, uma vez que a limitação imposta pelo IDS-RNP não permitiu avaliar o Macvlan neste cenário. Na Subseção 5.1 e Subseção 5.2 são apresentados os resultados dos cenários 1 e 2, respectivamente. Por fim, a Subseção 5.3 apresenta o uso de Memória RAM e CPU da vítima.

Na Tabela 3 são apresentados os resultados consolidados das 30 execuções com cada tecnologia nos dois cenários propostos. Os resultados estão agrupados em: pré-ataque; e durante o ataque. Para cada grupo é apresentada a média do total de requisições de clientes que foram atendidas com sucesso, bem como a média da latência (em segundos), o qual considera o tempo que demorou desde o pedido do cliente até o recebimento da resposta. No período pré-ataque, ciente que cada cliente gerou 120 requisições, é possível perceber que a maioria das requisições foram atendidas em ambos os cenários.

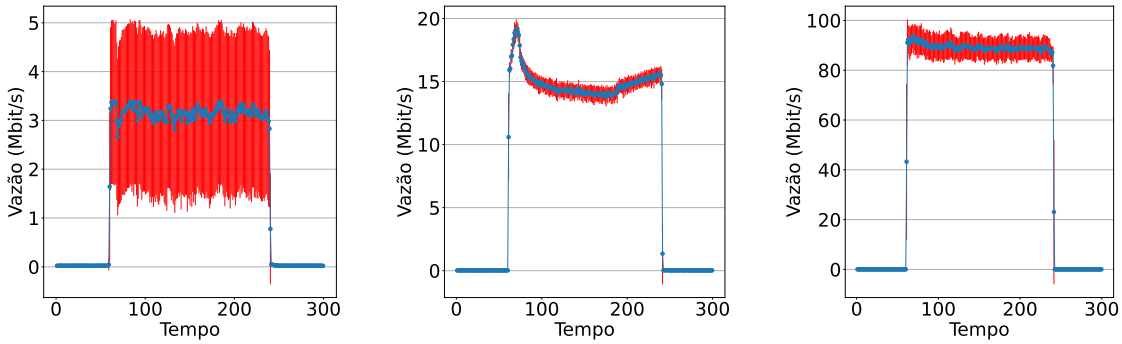
No período durante o ataque, onde cada cliente gerou 360 requisições, é possível perceber que o ataque gerou impactos principalmente no cenário 2, onde o número de requisições atendidas ficou entre 9% a 12% e a latência ficou quase 17 vezes maior, se comparado com o período pré-ataque.

Tabela 3. Média de latência e do total de requisições atendidas de cada cliente com diferentes cenários e tecnologias

Cenário	Tecnologia	Pré-ataque (0s à 59s59ms)				Durante o ataque (60s à 240s)			
		Total de req.	Desvio padrão	Latência (seg)	Desvio padrão	Total de req.	Desvio padrão	Latência (seg)	Desvio padrão
1	KNetLab	102,6	8,4	0,09	0,05	306,3	24	0,09	0,05
	Calico	111,8	0,7	0,04	0,01	258,3	61,0	0,16	1,2
	Macvlan	110,9	5,1	0,04	0,01	321,1	59,8	0,04	0,06
2	KNetLab	95,5	13,4	0,11	0,11	12,4	58,6	1,84	8,81
	Calico	107,5	7,9	0,06	0,06	9,7	3,3	0,96	6,28

5.1. Cenário 1

Ao observar as Figuras 3a, 3b e 3c, contata-se o aumento na vazão de rede da vítima ao ser iniciado o ataque. O KNetLab e o Macvlan obtiveram um comportamento similar, sendo que desde o início do ataque a vítima chegou ao limite da vazão descartando os demais pacotes. Essa característica pode estar associada ao fato de não existir uma ferramenta responsável pelo balanceamento de carga.



(a) KNetLab **(b)** Calico **(c)** Macvlan

Figura 3. Média e desvio padrão de vazão de rede nas vítimas dos experimentos.

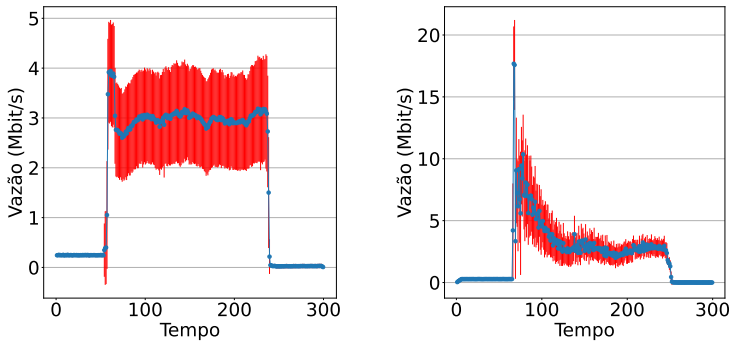
O KNetLab alcançou uma média de aproximadamente 3 Mbit/s na vazão de rede, sendo que, em alguns experimentos, o ataque não foi iniciado. Esses problemas estão associados às configurações da infraestrutura que, em alguns casos, gerou falhas na inicialização dos *pods*. Os resultados obtidos com o Macvlan foram os mais próximos as limitações existentes nos dispositivos físicos presentes na IDS-RNP, sendo que a média de vazão chegou aos 90 Mbit/s, alcançando a taxa máxima de vazão disponibilizada pelo enlace durante o experimento. Com o Calico, foi possível perceber um pico de aproximadamente 20 Mbit/s na vazão durante os primeiros segundos do ataque que passa a ser reduzido até aproximadamente 15 Mbit/s. Essa característica pode estar associada ao congestionamento de pacotes, que resulta na redução dos pacotes enviados. O Calico utiliza um conjunto de *plugins* e protocolos para lidar com o tráfego de maneiras diferentes.

5.2. Cenário 2

Como descrito anteriormente, este cenário teve como objetivo analisar a influência no tempo de resposta e vazão diante do aumento do número de clientes e de atacantes nos experimentos. O Macvlan não está presente neste cenário devido às características para sua implementação na IDS-RNP. O aumento no número de clientes e atacantes elevaram o tempo de resposta significativamente no KNetLab e no Calico. Como pode ser observado na Tabela 3, durante o período de ataque em média 12 das 360 requisições foram atendidas no KNetLab, O Calico obteve um valor ainda menor, com uma média de aproximadamente 10 requisições atendidas. Desse modo, o ataque negou o serviço em ambas as tecnologias durante o período em que a vítima estava sob ataque. Também foi observado que após o período de ataque a maior parte dos clientes não obtiveram mais resposta por parte da vítima até a conclusão do experimento.

Como pode ser observado na Figura 4a, a taxa de vazão foi similar ao observado na Figura 3a. Isso ocorre devido a limitações impostas no KNetLab, fazendo com que ambos experimentos utilizassem o limite de trafego imposto pela ferramenta. Deste modo, o aumento no número de clientes e atacantes não teve um maior impacto na taxa de vazão de rede da vítima. Ao comparar a Figura 3b com a Figura 4b, é possível perceber a redução na taxa de envio. Sendo que o aumento no número de clientes e atacantes teve um maior impacto na vazão, deste modo, o aumento de congestionamento afetou significativamente a taxa de envio. Como mencionado anteriormente, esta característica acontece devido ao

fato do Calico ser uma CNI na qual a retransmissão pode fazer com que o mecanismo de congestionamento diminua a taxa de envio.

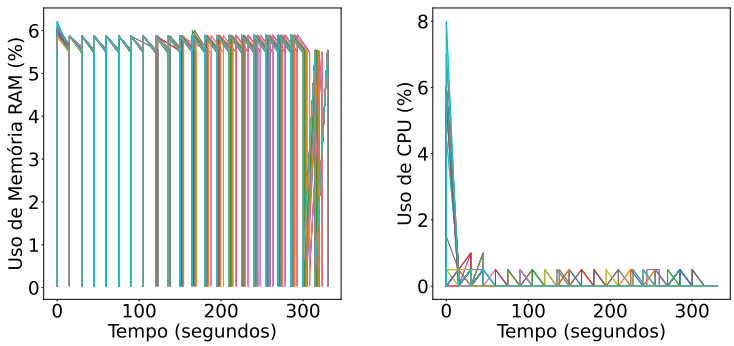


(a) KNetLab **(b)** Calico

Figura 4. Vazão de rede na vítima.

5.3. Monitoramento de CPU e memória RAM

Com o objetivo de analisar a utilização de recursos físicos da IDS-RNP, foi desenvolvido uma ferramenta incumbida de coletar as métricas referentes ao aproveitamento de Memória RAM e CPU no período do experimento. As métricas são coletadas a partir do *software* Netdata, que efetua a coleta individual dos *pods* que fazem parte do experimento. A Figura 5a mostra o gráfico com a utilização de Memória RAM e a Figura 5b apresenta a utilização de CPU. Esses resultados referem-se à utilização dos recursos por parte do KNetLab durante o experimento, como observado na Figura 4a. Os resultados do Calico e Macvlan foram similares aos observados no KNetLab.



(a) Memória RAM **(b)** CPU

Figura 5. Utilização de Memória RAM e CPU na vítima.

Ao observar as Figuras 5a e 5b, é possível perceber a não influência do ataque em recursos de Memória RAM e CPU na vítima durante o período de ataque. Isso ocorre devido ao sucesso do ataque estar relacionado à degradação dos recursos de rede e, consequentemente, a influência do ataque está na utilização de recursos disponibilizados pelo enlace da vítima. Os picos de utilização observados no inicio dos experimentos são referentes ao tempo de inicialização do *software* NGINX responsável pelo servidor HTTP.

6. Dificuldades e limitações

As análises realizadas sobre os resultados dos experimentos propostos neste artigo permitem concluir que a atual proposta do MENTORED testbed atende parcialmente os requisitos necessários para a simulação e estudo de ataques DDoS. Dentre as dificuldades observadas, está na definição de qual tecnologia de simulação de rede seria a mais adequada para reproduzir de forma fiel o padrão de tráfego gerado por esse tipo de ataque, considerando os limites da infraestrutura disponível no IDS-RNP e no projeto MENTORED. Outra dificuldade foi em determinar se o ataque DDoS estava exaurindo os recursos do serviço, alvo do ataque, e não os recursos do IDS-RNP, utilizados para condução do experimento. Contudo, foi possível observar que a tecnologia KNetLab possibilitou, de forma parcial, a reprodução das características esperadas pelos experimentos propostos.

7. Conclusão

Este trabalho apresentou experimentos realizados no MENTORED *Testbed* para determinar o comportamento de diferentes tecnologias para criação de redes virtuais que a IDS-RNP provê suporte.

Pode-se observar a necessidade de uma pré-configuração para a utilização do *plugin* Macvlan, além do uso diferentes ferramentas e técnicas de captura de dados gerados na IDS-RNP. Em algumas execuções usando o KNetLab, a base do *testbed*, este apresentou falhas na inicialização dos experimentos, ocasionando problemas na comunicação entres os *pods*. Observou-se também a falta de uma documentação do KNetLab contendo suas características de funcionamento, como por exemplo, a possível existência de limitações de tráfego de rede em seus enlaces virtuais, bem como a possível ausência de um mecanismo de aceleração de encaminhamento de pacotes.

Os resultados da pesquisa experimental conduzida neste trabalho serão utilizados para aprimorar a criação de redes virtuais no MENTORED *Testbed* e, consequentemente, para aumentar a fidelidade dos experimentos conduzidos no *testbed*. Como trabalhos futuros, pretende-se conduzir novas avaliações experimentais com maior número de nós físicos e virtuais, com outras tecnologias para criação de redes virtuais e ainda avaliar outros cenários de ataques de cibersegurança. Dessa forma, será possível identificar possíveis soluções para mitigar ou superar as dificuldades encontradas neste trabalho, onde se destacam principalmente a identificação de gargalos que limitam a vazão do tráfego de rede em simulações de ataques DDoS e a complexidade para elaboração de experimentos que consideram simulações de topologias complexas. Portanto, as próximas etapas desta pesquisa também consideram os avanços necessários para o desenvolvimento de tecnologias que facilitem a elaboração de experimentos pelos usuários do MENTORED testbed, o que inclui o desenvolvimento de um portal *web* que considera autenticação federada usando o sistema CAFe (Comunidade Acadêmica Federada). Também, serão estudadas novas tecnologias de simulação de rede que possam ser implementadas no IDS-RNP, como o uso de novas CNIs e recursos disponíveis na ferramenta Kubernetes, que podem ser escolhidas pelos usuários do *testbed* antes de iniciar os seus experimentos.

Referências

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., et al. (2017). Understanding the mirai botnet. In *USENIX Security*, pages 1093–1110.

Caban, W. (2019). *Architecting and Operating OpenShift Clusters: OpenShift for Infrastructure and Operations Teams*. Apress.

Cha, J.-G. and Kim, S. W. (2021). Design and evaluation of container-based networking for low-latency edge services. In *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1287–1289. IEEE.

CNI (2020). Macvlan. `https://www.cni.dev/plugins/current/main/macvlan/`. Acesso em Março de 2022.

Hernandez, M. (2021). KNetLab. `https://indico.rnp.br/event/46/contributions/365/`. Acesso em Março de 2022.

Kapočius, N. (2020). Overview of kubernetes cni plugins performance. *Mokslas–Lietuvos ateitis/Science–Future of Lithuania*, 12.

Koroniotis, N., Moustafa, N., Sitnikova, E., and Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, 100:779–796.

Kubernetes (2022). Cluster Networking. `https://kubernetes.io/docs/concepts/cluster-administration/networking/`. Acesso em 03/2022.

Lee, S., Lee, S., Yoo, H., Kwon, S., and Shon, T. (2018). Design and implementation of cybersecurity testbed for industrial iot systems. *The Journal of Supercomputing*, 74(9):4506–4520.

Mahalingam, M., Dutt, D. G., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and Wright, C. (2014). Virtual extensible local area network (vxlan): A framework for overlaying virtualized layer 2 networks over layer 3 networks. *RFC*, 7348:1–22.

Mirkovic, J. and Benzel, T. (2013). Deterlab testbed for cybersecurity research and education. *Journal of Computing Sciences in Colleges*, 28(4):163–163.

Pfaff, B. and Davie, B. (2013). The open vswitch database management protocol. *Internet Requests for Comments, RFC Editor, RFC*, 7047.

Prates Jr, N. G., Andrade, A. M., de Mello, E. R., Wangham, M. S., and Nogueira, M. (2021). Um ambiente de experimentação em cibersegurança para internet das coisas. In *Anais do VI Workshop do testbed FIBRE*, pages 68–79. SBC.

Rahal, B. M., Santos, A., and Nogueira, M. (2020). A distributed architecture for ddos prediction and bot detection. *IEEE Access*, 8:159756–159772.

Simpson, W. et al. (1995). Ip in ip tunneling. Technical report, RFC 1853, October.

Wroclawski, J., Benzel, T., Blythe, J., Faber, T., Hussain, A., Mirkovic, J., and Schwab, S. (2016). Deterlab and the deter project. In *The GENI Book*, pages 35–62. Springer.

Yusof, A. R., Udzir, N. I., and Selamat, A. (2019). Systematic literature review and taxonomy for ddos attack detection and prediction. *International Journal of Digital Enterprise Technology*, 1(3):292–315.

Zhu, S., Yang, S., Gou, X., Xu, Y., Zhang, T., and Wan, Y. (2022). Survey of testing methods and testbed development concerning internet of things. *Wireless Personal Communications*, 123(1):165–194.