Abordagem Adaptativa para Proteção de Redes SDN Utilizando Moving Target Defense

Emídio Neto (UFRN), Rodrigo S. S. Nunes (LaTARC/IFRN)

Cristian H. M. Souza (LaTARC/IFRN), Felipe S. Dantas Silva (LaTARC/IFRN), Túlio Pascoal (University of Luxembourg)

XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2022) - 26/05/2022

Agenda

- Motivação
- Visão geral da proposta
- Validação da proposta e Resultados
- Conclusões e trabalhos futuros

Motivação

Motivação

- *Softwarization:*
  - Facilitador para implementação de mecanismos de defesa para redes de próxima geração
  - Diversos trabalhos na literatura demonstram maneiras de comprometer redes softwarizadas **(SDN)** através de ataques direcionados
    - DoS/DDoS
    - Slow TCAM
    - **Scanning (Inferência dos *timeouts* da rede, serviços, etc)**

Motivação

- *Moving Target Defense (MTD)*:
  - Objetiva mudar parâmetros e/ou características de sistemas de forma dinâmica;
  - Reduzir as janelas de oportunidades que atacantes podem detectar para atacar sistemas e ou redes de computadores;
  - Atualmente bastante utilizada para prevenção de ataques scanning.
- MTD + *Softwarization*:
  - MTD requer alta capacidade de programabilidade;
  - Facilita a aplicação e mudanças de características da rede de forma dinâmica;
  - Pode ser implementado tanto no plano de dados quanto no plano de controle.

Motivação

- A literatura revela alguns trabalhos que se propuseram a proteger redes softwarizadas contra ataques de scanning com MTD:
  - As soluções encontradas baseiam-se na adição de latência a pacotes maliciosos para dificultar a identificação de informações da rede;
- Apesar de serem efetivas, essas soluções impactam a performance da rede (e.g., QoS)

Motivação

- *MTD Adaptive Delay System* (MADS):
  - Uma solução adaptativa para proteção de redes softwarizadas apoiada na abordagem MTD
- Diferentemente das soluções relacionadas, MADS aciona o mecanismo de MTD de forma adaptativa:
  - Aplica latência de forma baseada no comportamento da rede alvo
    - Somente em situações em que a rede é realmente impactada pelo ataque
  - Mantém o **mesmo nível de proteção** das soluções na literatura com **menor degradação**

Motivação

- Dessa forma, evita que a rede e os pacotes legítimos não sejam impactados pelo mecanismo MTD de forma contínua
- MADS baseia-se na modelagem de ataques *scanning* para determinar limiares:
    - São utilizados para identificar a existência e o impacto de ataque na rede em um determinado momento
    - Com base nisso, é realizado a ativação do mecanismo MTD

Trabalhos relacionados

Trabalhos relacionados

Proposta	Estratégia principal	Abordagem	Técnica de melhora da QoS	Limitações
[Ma et al. 2014]	Atraso contínuo dos pacotes.	Adição de latência nas portas dos *switches*.	Não há	Degradação da performance da rede de forma contínua e seleção do valor de latência é realizada considerando estado anterior da rede (tempo de resposta).
[Yuwen et al. 2016]	Atraso seletivo dos pacotes, baseado em probabilidade.	Envio dos pacotes selecionados para o controlador.	Utiliza probabilidade para selecionar os pacotes que serão atrasados.	Sobrecarga no controlador dependendo do tamanho da rede.
[Hou et al. 2020]	Atraso seletivo dos pacotes, baseado no IP e MAC do dispositivo de origem.	Envio dos pacotes selecionados para o controlador.	Atrasa apenas os pacotes gerados por possíveis dispositivos maliciosos.	Sobrecarga no controlador dependendo da quantidade de possíveis ameaças.
MADS (esta proposta)	Atraso dinâmico dos pacotes, baseado na identificação do ataque.	Adição de latência nas portas dos *switches*.	Não aplica latência na ausência de um ataque.	A seleção do valor de latência é realizada considerando estado anterior da rede (tempo de resposta).

Tabela 1. Comparação entre os trabalhos relacionados e a nossa proposta MADS

Trabalhos relacionados

- Em [Ma et al. 2014] a latência é aplicada diretamente nas portas dos switches, de maneira contínua;
- Os trabalhos de [Yuwen et al. 2016] e [Hou et al. 2020] além de aplicarem latência de forma contínua, ambos necessitam de tomada de decisão por parte do controlador;
- A abordagem introduzida por MADS é semelhante à de [Ma et al. 2014]:
    - Entretanto, a técnica empregada por MADS utiliza um método para adição/remoção da latência em determinados momentos, com o intuito de tornar a rede mais eficiente

Proposta

Proposta - MADS

- MADS aplica configurações de latência na rede de forma adaptativa, ao invés de forma contínua (como exaustivamente realizado pelos trabalhos anteriores)
- Minimiza os possíveis impactos negativos que uma técnica MTD baseada em adição de latência pode acarretar no que diz respeito à QoS da rede
- Fornece suporte à configuração adaptativa de latência como sendo um bloco funcional inserido no plano de controle da rede
- Capacidades adaptativas são suportadas pelo monitoramento do estado da rede

Proposta - MADS - Ativação do mecanismo

- MADS realiza o monitoramento de status dos fluxos a cada **Tmr** (segundos). Por exemplo, **Tmr = 10s** [Zarek et al.]
- MADS define limiares de bytes trafegados para as interfaces dos switches através de um período de observabilidade prévio definido por **SR**;
- **Trd** é o produto entre ***SR*** multiplicado pelo valor de **Tmr:**
    - Por exemplo, **Trd** = **SR** * **Tmr** -> 12 * 10 = 120s
    - **Trd** é utilizado como gatilho para desativação do mecanismo (atua como um *hard timeout*)
- Se a taxa atual de vazão de pacotes suspeitos ultrapassar os valores definidos **(SR)** entre cada intervalo de monitoramento **Tmr**, MADS aciona o mecanismo MTD

Proposta - MADS - Computação da latência

- Metodologia baseada no trabalho de Ma et al. 2014:
  - Utiliza pacotes ICMP para definir valores para FirstPacket (t1) e LastPacket (t2);
  - Constrói uma lista Dt a partir da subtração dos valores de t2 por t1;

$$Dt = \{dt(i) | dt(i) = t_1(i) - t_2(i), i > 0\} \quad (1)$$

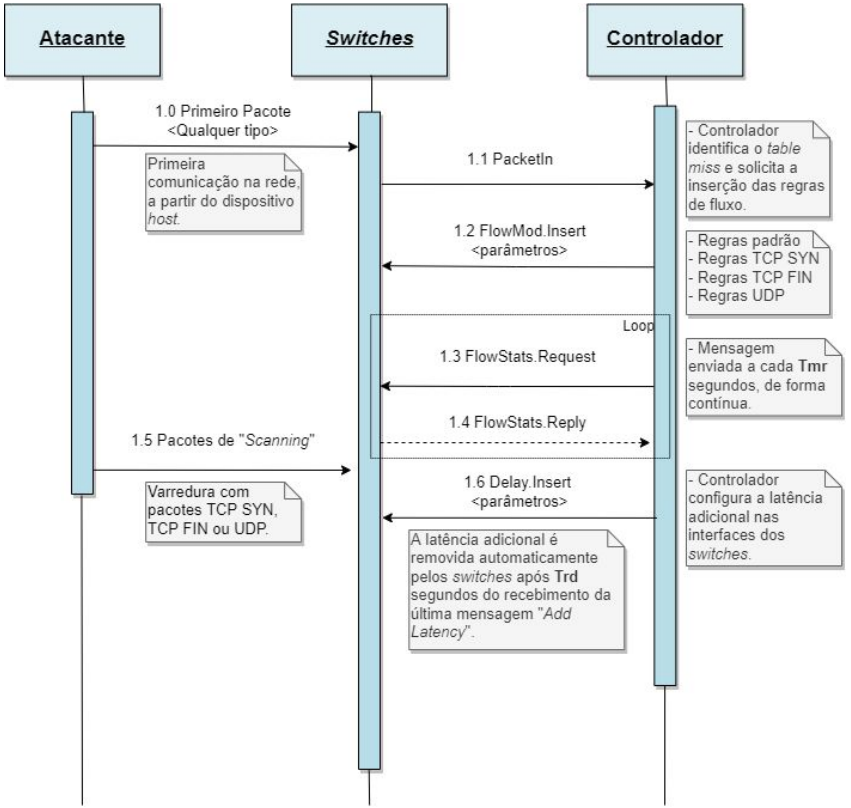
Proposta - MADS - Computação da latência

- Metodologia baseada no trabalho de Ma et al. 2014:
  - Seleciona um valor de forma randômica, que deve estar entre os limites mínimo e máximo presentes na lista Dt;
  - Valor randômico é somado a t2 para obtenção do valor de *delay* a ser adicionado na interface do switch em que o *scanning* foi originado

$$T2 = \{t_2'(i) | t_2'(i) = t_2(i) + Random[Min(Dt), Max(Dt)], i > 0\} \quad (2)$$

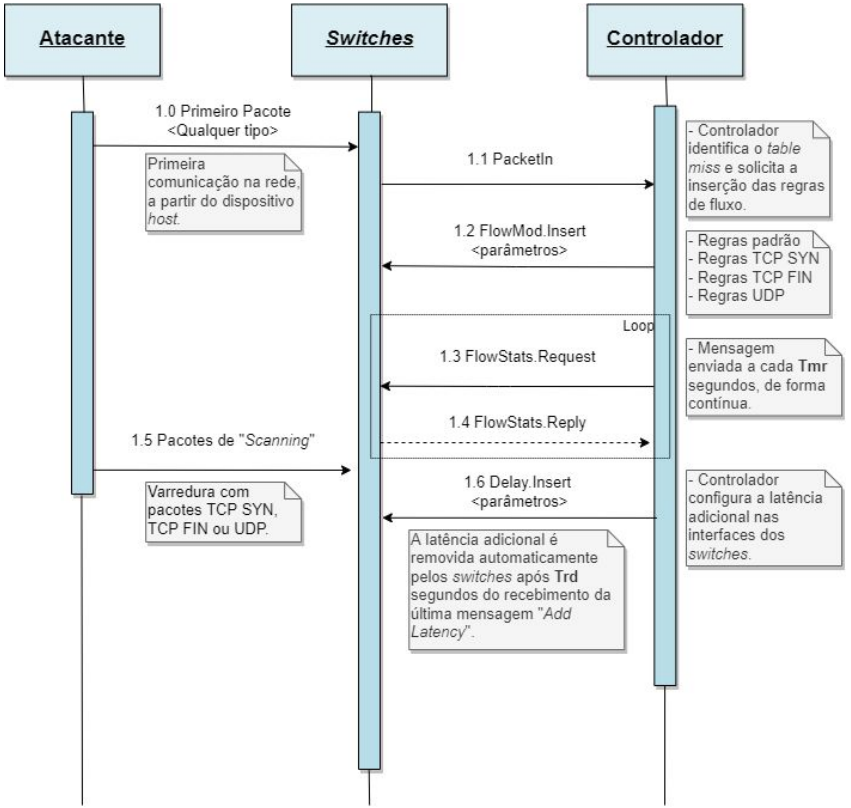
Proposta - MADS

- MADS realiza o monitoramento do estado das regras de fluxo em intervalos definidos por **Tmr** (Etapa 1.3 e 1.4)
- Scanning (Etapa 1.5), faz com que o contador de bytes de alguma(s) regras aumente de forma a não condizer com o **SR.**



Proposta - MADS

- MADS aciona o mecanismo MTD enviando uma mensagem Delay.Insert (Etapa 1.6)
- A latência é removida automaticamente pelo plano de dados após não receberem mais mensagens Delay.Insert de MADS durante **Trd** segundos

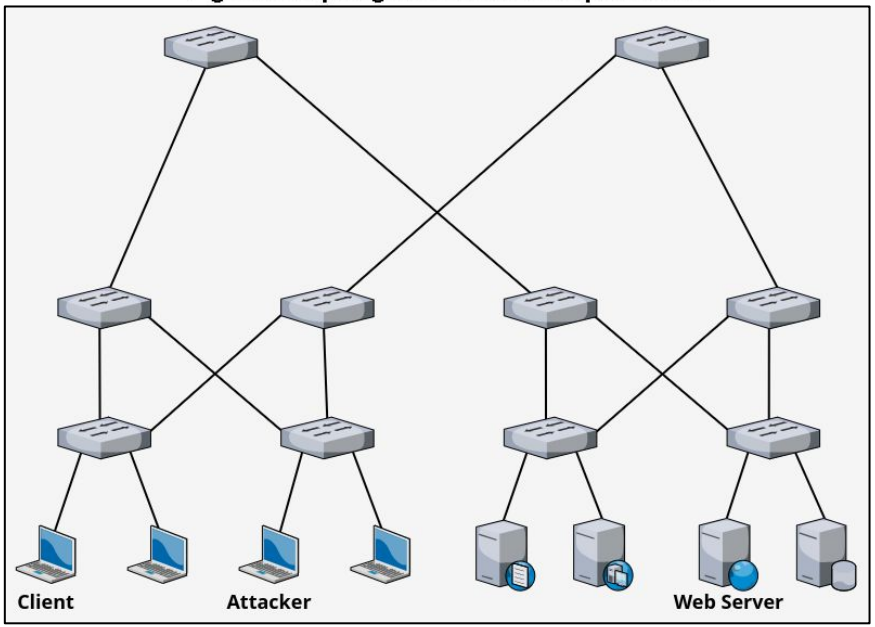


Validação da proposta

Validação da proposta

- Avaliar o impacto gerado por defesas MTD no desempenho da rede;
- Comparamos [Ma et al. 2014], [Hou et al. 2020] e MADS
- Observamos métricas como:
  - RTT
  - Vazão
  - Bad TCP

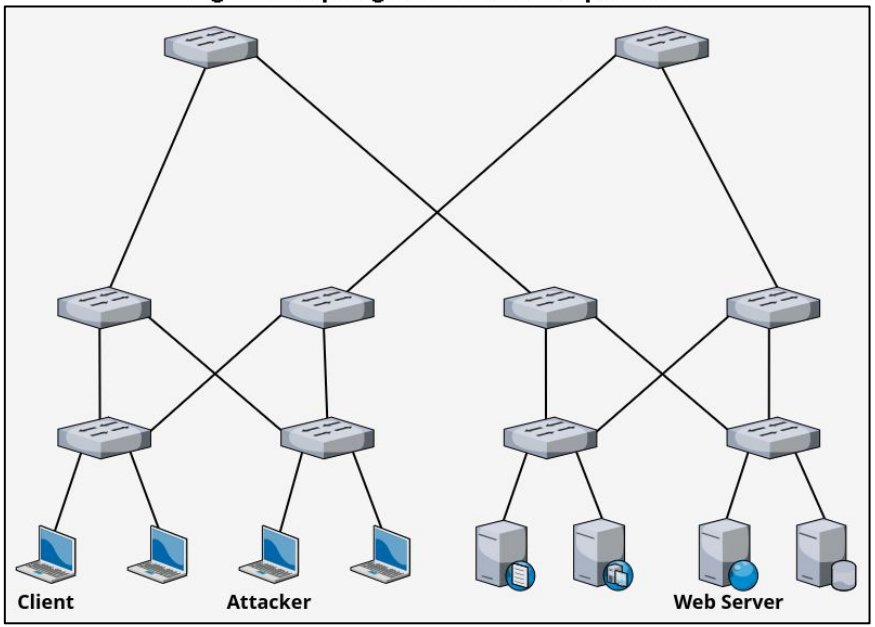
Figura 2. Topologia utilizada nos experimentos



Validação da proposta

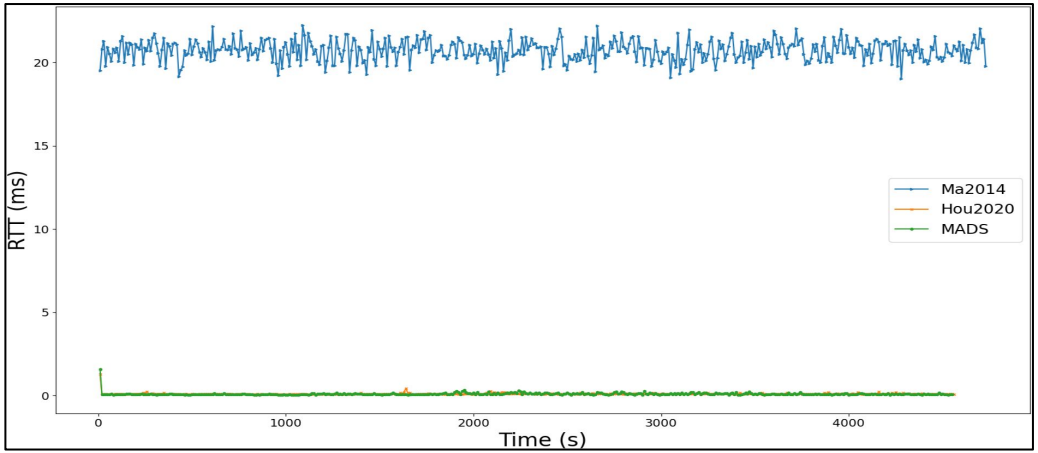
- Cada experimento teve duração de 4700 segundos com a seguinte abordagem:
  - *Client* gera tráfego HTTP ao servidor web em intervalos de 1 segundo;
  - *Attacker* executa um ataque scanning, enviando requisições à rede em busca de portas TCP abertas com duração de 800 segundos
- Consideramos **Tmr** = 10 e **Trd** = 120 segundos;

Figura 2. Topologia utilizada nos experimentos



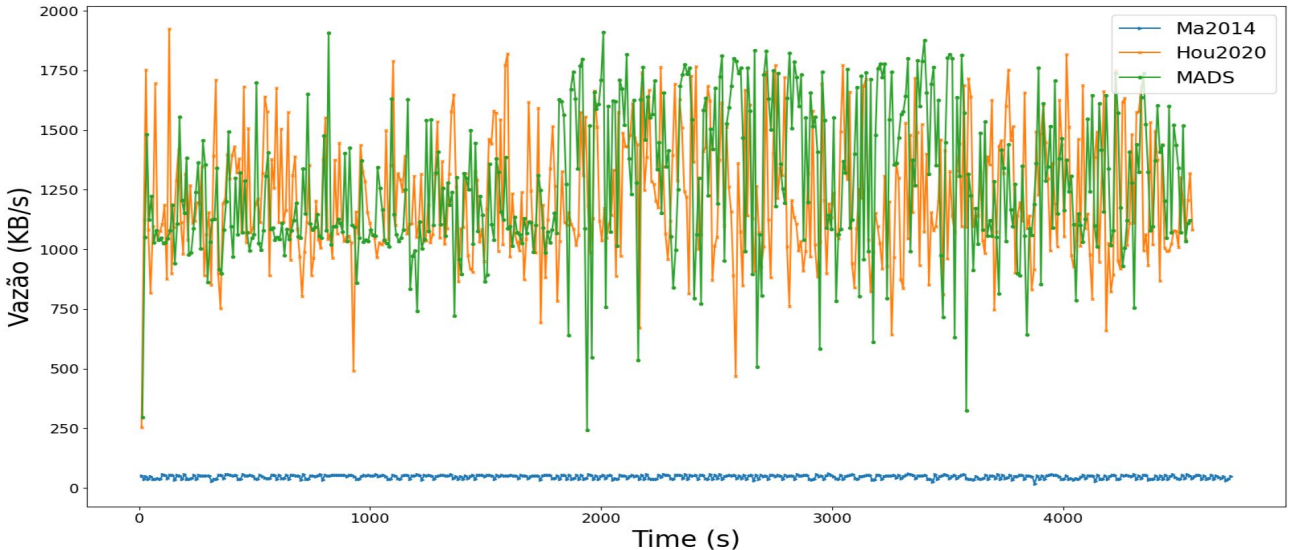
Resultados

- RTT
  - MADS e [Hou2020] apresentaram um RTT semelhante, permanecendo abaixo de 0.2ms na maior parte do tempo, atingindo uma latência 99.4% menor em relação a proposta [Ma2014]



Resultados

- Vazão
  - MADS atingiu uma vazão 4.87% maior quando comparada a [Hou2020]
  - [Ma2014] obteve uma taxa de vazão 27 vezes menor



Resultados

- Para todos os parâmetros, as propostas [Hou2020] e MADS tiveram seus resultados muito semelhantes (4.87%);
- A latência adicional é inserida apenas para o tráfego gerado pelo atacante;
- [Hou2020] pode representar um problema para a rede pela sobrecarga de processamento de pacotes no controlador

Conclusões e trabalhos futuros

Conclusões e trabalhos futuros

- É evidente que técnicas de MTD estão sendo cada vez mais utilizadas, principalmente para o combate à ataques de DoS, scanning etc;
- Consideramos MTD para proteção contra ataques *scanning* em redes softwarizadas;
- MADS é capaz de manter a eficiência da estratégia MTD para mitigar os ataques de scanning;
- Além disso, os efeitos da degradação do QoS observados na operacionalização de MADS são mais amenos quando comparada com o estado da arte;

Conclusões e trabalhos futuros

- Adoção de novos parâmetros (quantidade de saltos e o tamanho da topologia) para equação do mecanismo MTD;
- IA em tempo real para apoiar o processo de tomada de decisão (valor dos atrasos)
    - De acordo com o comportamento e nível de segurança da rede

Obrigado

Abordagem Adaptativa para Proteção de Redes SDN Utilizando Moving Target Defense

Emídio Neto (UFRN) - emdneto@ufrn.edu.br

Rodrigo S. S. Nunes (LaTARC/IFRN), Cristian H. M. Souza (LaTARC/IFRN),

Felipe S. Dantas Silva (LaTARC/IFRN), Túlio Pascoal (University of Luxembourg)

XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2022) - 26/05/2022