Dinâmica da Propagação de Botnets em Redes Definidas por Software Usando Modelos Epidêmicos

"Dynamics of Botnet Propagation in Software Defined Networks Using Epidemic Models"

Juan F. Balarezo Song Wang Karina Gomez Chavez Akram Al-Hourani
Sithamparanathan Kandeepan

IEEE Access (Volume: 9) 2021

RMIT University, Melbourne, Austrália

Contexto

- Cenário pós-COVID-19:
  - Aumento exponencial de dispositivos conectados (20.4 bi em 2020)
  - Crescimento de 557% em botnets (Mirai: 35k→230k dispositivos)
  - 4.83 milhões de ataques DDoS registrados (1º sem. 2020)
- Problema:
  - Arquitetura centralizada de SDN é vulnerável a DDoS
  - Necessidade de entender dinâmica de propagação de botnets
- Solução proposta:
  - Modelagem epidemiológica aplicada a redes SDN
  - Analogia com doenças humanas (COVID-19 e Zika)

Modelos Epidemiológicos

- Abordagem compartimental: SEIRS
  - Suscetível (S), Exposto (E), Infectado (I), Recuperado (R)
- Diferença crítica:
  - Humanos: imunidade após recuperação
  - Dispositivos: podem ser reinfectados (novas vulnerabilidades)

- Número de reprodução básica (R_0):
  - Métrica para o potencial de disseminação de uma infecção.
  - Se $R_0 < 1$, a infecção tende a desaparecer (extinção).
  - Se $R_0 > 1$, a infecção pode se espalhar na população (endemia).

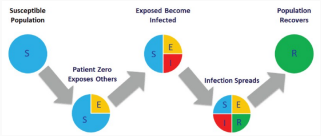

Figure 1: Modelo compartimental SEIRS.

Modelos Propostos

Enterprise SDN

- Único controlador
- Propagação entre *switches*
- Modelo SEIRS simples
- Equações:

$$\frac{dS_S}{dt} = -\beta S_S I_S + \alpha R_S$$
$$\frac{dE_S}{dt} = \beta S_S I_S - \epsilon E_S$$
$$\frac{dI_S}{dt} = \epsilon E_S - \gamma I_S$$
$$\frac{dR_S}{dt} = \gamma I_S - \alpha R_S$$

Service Provider SDN

- Múltiplos controladores
- 2 vetores de infecção:
  1. Controlador → Controlador
  2. Controlador → *Switch* (e entre switches)
- Modelo SEIRS-SEIRS acoplado
- 8 equações diferenciais

Análise de R_0

Enterprise SDN

$$R_0 = \frac{\beta S_S}{\gamma} \quad \text{(Matriz de próxima geração)}$$

Cálculo baseado na Next Generation Matrix (NGM) para o sistema em equilíbrio livre de doença (DFE).

Service Provider SDN

$$R_0 = \frac{\beta_C S_C}{\gamma_C} \quad \text{(Autovalor dominante)}$$

Obtido como o autovalor dominante da NGM para o modelo de múltiplos vetores.

Interpretação

- $R_0 > 1$: Botnet se propaga exponencialmente
- $R_0 < 1$: Infecção é controlada e tende à erradicação
- Fatores críticos: Taxa de infecção (β) e recuperação (γ)

Simulações e Resultados

Enterprise SDN

- Parâmetros baseados no modelo COVID-19
- $\beta = 0.506$, $\gamma = 0.0668$
- $R_0 = \frac{0.506 \times S_S}{0.0668} = 7.57$. Simulação com $S_S(0) = 0.70$ evolui para equilíbrio endêmico quando $R_0 > 1$.

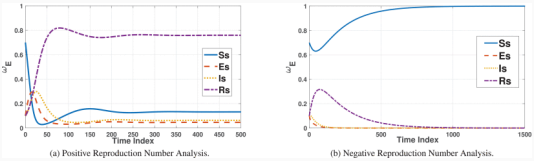

Figure 2: Enterprise: Equilíbrio endêmico ($R_0 > 1$) vs. livre de doença ($R_0 < 1$).

Service Provider SDN

- Parâmetros baseados no modelo Zika
- $\beta_C = 0.261$, $\gamma_C = 0.1137$
- $R_0 = \frac{0.261 \times S_C}{0.1137} = 2.29$. Simulação com $S_C(0) = 0.55$ evolui para equilíbrio endêmico quando $R_0 > 1$.

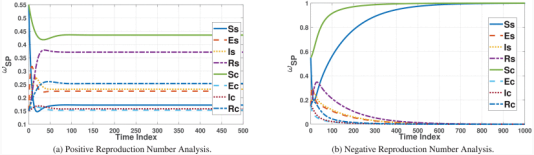

Figure 3: Provedor de Serviço: Equilíbrio endêmico ($R_0 > 1$) vs. livre de doença ($R_0 < 1$).

Validação e Contribuições

Validação Teórica

- Teorema do Valor Final (FVT) aplicado às EDOs do modelo
- Comparação estado estacionário (Enterprise, $R_0 > 1$):
  - Simulação: $S_S = 0.1321$
  - FVT: $S_S = 0.1120$ (erro ± 0.01)

Contribuições Chave

1. Primeiros modelos epidêmicos detalhados (SEIRS e SEIRS-SEIRS) para botnets em SDN
2. Análise de estabilidade via R_0 e NGM para ambos os cenários SDN
3. Compreensão de vetores de infecção específicos em SDN:
   - Enterprise: Propagação horizontal entre dispositivos de encaminhamento
   - Service Provider: Infecção cruzada entre controladores e destes para switches

Conclusões e Recomendações

- **Conclusões**:
  - Propagação de botnets em SDN similar a epidemias humanas
  - R_0 é essencial para controle de surtos
- **Recomendações**:
  - Reduzir β: Hardening, patches, segmentação
  - Aumentar γ: Detecção rápida, respostas automatizadas
  - Monitorar R_0: Alertas precoces
- **Futuro**:
  - Modelos para redes IoT
  - Modelos estocásticos
  - Aprendizado de máquina para estimativa e detecção

Obrigado!

Artigo completo:
IEEE Access 9 (2021) 119406-119417
DOI: 10.1109/ACCESS.2021.3108181