ANTÔNIO CARLOS BASTOS DE GODÓI

Modelo de contenção de Malware em redes com alerta

São Paulo

2022

ANTÔNIO CARLOS BASTOS DE GODÓI

Modelo de contenção de Malware em redes com alerta

Versão Original

Tese apresentada à Escola Politécnica da Universidade de São Paulo, como requisito para a obtenção do Título de Doutor em Ciências.

São Paulo

2022

ANTÔNIO CARLOS BASTOS DE GODÓI

Modelo de contenção de Malware em redes com alerta

Versão Original

Tese apresentada à Escola Politécnica da Universidade de São Paulo, como requisito para a obtenção do Título de Doutor em Ciências.

Área de Concentração: Engenharia de Sistemas

Orientador: Prof. Dr. José Roberto Castilho Piqueira

São Paulo

2022

Catalogação-na-publicação

Godoi, Antonio Carlos Bastos de

Modelo de contenção de Malware em redes com alerta / A. C. B. Godoi -- São Paulo, 2022.

74 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Telecomunicações e Controle.

1.Segurança de redes 2.Segurança de computadores 3.Redes de computadores 4.Hackers 5.Autômatos celulares I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Telecomunicações e Controle II.t.

À memória do querido amigo, médico e professor, Henrique
que cuidou de mim e com quem conheci a amizade verdadeira

RESUMO

GODÓI, A. C. B. **Modelo de contenção de Malware em redes com alerta**. 2022. Tese (Doutorado) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2022.

Nos últimos anos, o progresso tecnológico, representado pelo aperfeiçoamento e amplo uso das redes de comunicação, da robótica, digitalização e Internet das coisas, tornou os sistemas da informação parte fundamental, presente nas diversas atividades e situações cotidianas. Conforme o cenário evolui para a interconexão dos sistemas distribuídos, as vulnerabilidades e ameaças de ataques cibernéticos se intensificam. Desejando responder a estes desafios e contribuir com o estado da arte sobre segurança cibernética, este trabalho apresenta o modelo epidemiológico espaço-temporal *SASIR* (Susceptível-Alerta-Susceptível-Infectado-Recuperado). Neste modelo, as máquinas que identificam a presença de invasores, adaptam seu funcionamento, passando para um modo de operação mais seguro, e alertando seus vizinhos na rede. A transição destas máquinas para o modo seguro, no qual o risco de contaminação é menor, altera a dinâmica da propagação, que converge para cenários mais favoráveis, onde o número de infectados e o impacto na rede diminuem. O desempenho do modelo foi avaliado através de simulações, sob diferentes cenários de ataques cibernéticos. Em um dos casos, por exemplo, em que 2% das máquinas foram infectadas, a propagação que atingiria todas as vulneráveis, foi contida, preservando mais de 96% das máquinas da rede. Além disso, mesmo sob situações menos favoráveis, foi capaz de achatar a curva de infectados e preservar intacta parte dos sistemas, evidenciando sua eficácia e robustez. As capacidades de reduzir a propagação e preservar os sistemas de um ataque cibernético, atendem às necessidades contemporâneas de táticas de segurança, capazes de proteger contra ameaças que escapam dos recursos de proteção convencionais, e cujas velocidades de propagação exigem atuação imediata de sistemas automatizados. Os resultados deste estudo encorajam o desenvolvimento de ferramentas que incorporem a estratégia apresentada, como software ou hardware, para serem empregadas em sistemas computacionais reais.

Palavras-chave: SASIR. Malware. Contenção. Segurança. Cibernética.

ABSTRACT

GODÓI, A. C. B. **Malware containment model in networks under alert**. 2022. Thesis (PhD Science) – Polytechnic School, Universidade de São Paulo, 2022.

In recent years, technological progress whereby the improvement and widespread use of communication networks, robotics, digitalization, cloud computing and the Internet of Things were integrated into an operational infrastructure, where information technology systems play a prominent role to reach a new stage of industry evolution. As the landscape evolves towards the interconnection of distributed systems, the vulnerabilities and risks of cyberattacks intensify. In order to tackle these challenges and provide a contribution in the field of cybersecurity, this work presents the SASIR (Susceptible-Alert-Susceptible-Infected-Recovered) epidemiological model. This work describes a mitigation scheme whereby computers that detect compromised peers engage in a safe operating mode, reducing their risks of being infected, and sending alert messages to their neighbor hosts. By running computer simulations, under different attack scenarios, this strategy was able to limit the spread and reduce the number of infected hosts. The results showed that, as the probability of detecting the contaminated hosts increases and the risks of being infected under safe mode operation decreases, the overall performance improves. As an example, in one experimental condition, the strategy could prevent more than 96% of the computers of being infected. Furthermore, the robustness of the model was proven under less favorable conditions, still being able to flatten the infection curve and protect part of the network. The ability to quickly react and protect against a rapidly spreading cyberattack, demonstrated by the model, meet the contemporary needs of security alternatives, capable of protecting against threats that escape conventional defense systems, and whose propagation velocity demand immediate intervention from automated mechanisms. Thus, the results of this study encourage the development of tools that incorporate the model's strategy, such as software or hardware, to be employed in real computing infrastructures.

Keywords: Cyber. Security. Worms. Malware. Containment. SASIR.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

A disseminação do uso de computadores em rede ampliou as interações e trocas de informações entre indivíduos e corporações, contudo os sistemas computacionais amplamente interligados proporcionam também meios para propagação de malware, termo que se refere a programas maliciosos, como aqueles que invadem computadores e perpetram ações indesejadas (SAEED; SELAMAT; ABUAGOUB, 2013). Diante deste cenário, conforme representado em obras como a de Mishra e Piqueira (2020), a segurança cibernética solidifica-se como assunto de interesse universal dado o extenso envolvimento da tecnologia da informação nas diferentes áreas de atuação humana.

Dentre os diversos tipos de malware, os worms ou "vermes" constituem uma classe de programas que se multiplicam e propagam pelas redes de forma autônoma, sem intervenção humana, explorando vulnerabilidades de segurança dos sistemas (LI; SALOUR; SU, 2008). Os worms podem utilizar estratégias muito eficientes de propagação e infecção, e com isso multiplicarem-se pela rede com extrema rapidez. As características desta classe e, em particular, sua elevada taxa de propagação trazem grandes riscos potenciais para a sociedade, em virtude da sua dependência cada vez mais ampla dos sistemas computacionais. Em 2003, por exemplo, o Slammer ganhou notoriedade por se tornar o worm com maior velocidade de proliferação registrada até aquela data, quando foi capaz de infectar mais de 90% das máquinas vulneráveis em um intervalo de 10 minutos, atingir pelo menos 75 mil máquinas e causar interrupções nas redes, cancelamentos de voos, além de comprometer o funcionamento de caixas eletrônicos (MOORE. et al., 2003).

Staniford et al. (2004) calcularam em 2004, que um worm estrategicamente desenvolvido poderia contaminar 95% de um total de um milhão de máquinas vulneráveis na Internet em um intervalo de tempo de 510 milissegundos. Devido ao contínuo aumento de desempenho dos sistemas computacionais e melhorias na performance de transmissão das redes, podemos esperar que esta velocidade teórica de propagação tenha aumentado consideravelmente desde aquela época.

A Internet tem sido atacada por worms capazes de interromper serviços (AHMAD; WOODHEAD, 2015), causar danos aos sistemas (FALLIERE; MURCHU; CHIEN, 2011), espionar informações (BENCSÁTH et al., 2012) e provocar prejuízos financeiros da ordem de

milhões até bilhões de dólares (FOSNOCK, 2005). Devido à variedade da natureza dos ataques e capacidade de proliferação, o estudo da dinâmica dos worms e o aperfeiçoamento de estratégias de combate representam áreas importantes e de grande interesse para pesquisa e desenvolvimento.

Com o propósito de contribuir para o estudo e desenvolvimento de estratégias de mitigação de ameaças cibernéticas, este trabalho tem como foco apresentar um novo modelo de contenção de malware, cujo desempenho será avaliado através de simulações computacionais, considerando distintos cenários de ataque, e discutindo os resultados para diferentes taxas de propagação e parâmetros do modelo.

Este trabalho é divido da seguinte maneira: o próximo capítulo oferece uma revisão da literatura sobre modelos epidemiológicos de malware e descreve as contribuições desta tese; o capítulo três, introduz o modelo proposto, que é baseado na teoria de autômatos celulares, e em seguida, apresenta e descreve a estratégia utilizada para contenção de malware. No capítulo quatro, são mostrados e discutidos alguns resultados de simulações de ataques cibernéticos. Por último, o capítulo cinco apresentada as conclusões, além de sugestões para trabalhos futuros.

2 REVISÃO DA LITERATURA E CONTRIBUIÇÕES

Este capítulo fará uma revisão da literatura sobre estratégias de combate e modelos de propagação de malware, incluindo modelos determinísticos, estocásticos e espaço-temporais. Serão abordados também modelos de propagação com alerta e, particularmente, será apresentado um trabalho que descreve uma estratégia de contenção de malware com envio de mensagens de alerta pela rede. Por último, serão descritas as contribuições do presente trabalho.

2.1 Estratégias de Combate à Propagação de Malware

Várias técnicas de combate aos worms são empregadas usando métodos de detecção, mitigação e contenção. Segundo uma sugestão de proposta, as técnicas podem ser divididas em cinco grupos (PORRAS et al., 2004):

- Detecção de assinatura de comportamento (BSD, do inglês Behaviour Signature Detection);
- Geração automática de assinaturas (ASG, do inglês Automatic Signature Generation);
- Limitação de recursos (RL, do inglês Resorce Limiting);
- Estratégia de passo à frente (LA, do inglês Leap Ahead);
- Combate móvel (MC, do inglês Mobile Combat).

A) Detecção de Assinatura de Comportamento (BSD)

As soluções do tipo BSD consistem na busca por padrões de comportamento anômalo na rede. Uma assinatura de comportamento descreve certos aspectos das atividades do worm. Como assinaturas de comportamento podemos citar, por exemplo, envios recorrentes de dados semelhantes para computadores da rede, propagação e varredura em forma de "árvore" ao longo da rede, ausência de pesquisa de DNS (ELLIS et al., 2004; WHYTE; KRANAKIS; OORSCHOTVAN, 2005; WHYTE; OORSCHOTVAN; KRANAKIS, 2005). Sistemas de BSD tentam localizar os worms através da identificação de uma ou mais assinaturas de comportamento na rede. Apesar dos sistemas BSD serem eficazes na detecção de worms, não

têm a mesma eficiência para transmitir alertas para a rede de modo a conseguir conter a proliferação.

B) Geração Automática de Assinaturas (ASG)

Os sistemas ASG geram assinaturas de comportamento automaticamente após a detecção de atividades suspeitas na rede. Por exemplo, Kim e colaboradores (KIM; KARP, 2004) propuseram um sistema denominado *Autograph*, que rotula automaticamente worms desconhecidos, que se propagam usando o protocolo TCP.

Singh et al. (2004) conceberam um sistema de geração automática de padrões chamado *Earlybird*, que identifica novos vírus e worms baseado em duas características de comportamento. Contudo, os sistemas ASG estão sujeitos a erros do tipo falso-positivo e, da mesma forma que os BSDs, não são eficazes para alertar as regiões não infectadas da rede sobre a presença de possíveis ameaças.

C) Limitação de Recursos (RL)

Os mecanismos RL usam estratégias para retardar a propagação de worms diminuindo os recursos exigidos para a rápida transmissão. Williamson (2002) sugere que através da limitação do número de novas conexões é possível reduzir significativamente a taxa de transmissão, sem comprometer substancialmente a comunicação normal da rede. Chen e Tang (2004) propuseram uma estratégia de limitação que pressupõe que as máquinas infectadas irão gerar um grande número de falhas de conexões TCP. A estratégia, implementada nos roteadores da rede, tenta limitar o número de conexões provenientes das máquinas que exibirem tais comportamentos. A vantagem principal das soluções RL é a simplicidade e facilidade de implementação, porém admitem altas taxas de falso-positivo.

D) Passo à Frente (LA)

As estratégias do tipo LA buscam conter e limitar a propagação dos worms espalhando sinais de alerta aos segmentos da rede ainda não contaminados. Estas estratégias consistem em compartilhar informações de maneira hierárquica ou por modelos de comunicação ponto a ponto. Por exemplo, Nojiri, Rowe e Levitt (2003) propuseram um sistema de alerta cooperativo que utiliza o protocolo denominado "*Friends*". Um outro exemplo de sistema cooperativo é apresentado pelo trabalho de Anaganostaki et al. (2003).

E) Combate Móvel (MC)

São chamadas de Combate Móvel as soluções que adotam estratégias de rápida interceptação e "patching". Estas soluções buscam eliminar malware através da disseminação na rede, de programas, os quais, de maneira análoga aos vírus, se replicam e se propagam, mas trazem consigo rotinas específicas para a eliminação dos malwares. Toyoizumi e Kara (2002), por exemplo, fizeram uma análise matemática de um MC denominado "Predator" e, inspirados nas equações de Lotka-Volterra, chegaram a uma metodologia para a escolha do menor número de predadores capaz de oferecer desempenho satisfatório no combate aos vírus. Apesar de serem alternativas em desenvolvimento, os sistemas MC apresentam questões ainda controversas quanto a legalidade do uso.

O trabalho de Moore et al. (2003), por sua vez, divide de modo genérico as abordagens usadas para mitigar as ameaças dos worms em três grupos: prevenção, tratamento e contenção. Cada uma das categorias é descrita abaixo:

A) Prevenção - As abordagens de prevenção buscam reduzir os tamanhos das populações vulneráveis e, deste modo, limitar a capacidade de disseminação das ameaças pela rede. As vulnerabilidades encontradas nos softwares, que são exploradas para a realização de ataques, embora possam ser minimizadas por meio de melhores práticas de desenvolvimento de programas, representam problemas que ainda estão distantes de serem solucionados;

B) Tratamento - Uma vez que as vulnerabilidades são identificadas, os programadores criam e disponibilizam soluções, "patches" ou atualizações que corrigem as falhas. Contudo, estas soluções levam tempo para serem disponibilizadas. Além disso, nem todos os usuários atualizam seus softwares e as suas máquinas acabam permanecendo vulneráveis. Os programas de antivírus podem reduzir o número de computadores atingidos através de ações para desinfetar as máquinas, contudo o desenvolvimento de novas vacinas demanda tempo e não é eficaz caso o sistema já tenha sido contaminado.

C) Contenção - Tecnologias de contenção, tais como, firewalls e filtros de conteúdo podem ser usadas para interromper a comunicação com computadores infectados e parar a transmissão de malware. Em tese, esta abordagem permite reduzir rapidamente ou mesmo encerrar o processo de proliferação pela rede, o que embora não represente uma solução definitiva, garante tempo adicional para o desenvolvimento de atualizações, patches e vacinas.

Existem argumentos que sustentam que esta última abordagem merece destaque dentre as três estratégias. Em primeiro lugar, porque detectar e caracterizar o worm é muito mais fácil que entender seu funcionamento e a natureza da vulnerabilidade. Além disso, existe a possibilidade de que o processo de contenção seja totalmente automatizado. Outra vantagem do sistema de contenção de rede é que através da atuação em alguns nós é possível restringir o acesso a grandes departamentos ou mesmo regiões inteiras. Por último, quando o ataque do worm for bem-sucedido e os recursos de segurança e proteção convencionais não conseguirem deter a propagação, caberá, em última instância, aos mecanismos de contenção a tarefa de evitar que a epidemia seja deflagrada. O trabalho de Li, Salour e Su (2008) apresenta três formas diferentes de contenção:

- Desaceleração: são técnicas, que reduzem a taxa de transmissão pela rede, permitem ganhar tempo para que intervenções definitivas possam ser realizadas. Diversos métodos têm sido sugeridos, tais como: realimentação para retardar tráfego suspeito (DANTU; YELIMELI, 2004) e limitação de velocidade para diminuir a taxa de contaminação (WONG et al., 2004). O fato dos worms se propagarem muito rapidamente comparado ao tempo de resposta humano faz com que, na prática, estes métodos se tornem ineficazes;
- Bloqueio: consiste em isolar as máquinas infectadas da rede através da interrupção do fluxo de dados. Esta técnica é geralmente usada com a Desaceleração, que num primeiro momento reduz a velocidade do tráfego e, em seguida interrompe o fluxo de informações caso seja atingido um limiar de alerta. O uso da Desaceleração tem o propósito de amenizar a queda de velocidade na rede para os casos falso-positivos. As técnicas de bloqueio usadas são duas: a de Conteúdo e a de Endereço. Moore et al. (2002) simularam a contenção através das duas técnicas e a de Conteúdo mostrou-se mais eficiente e eficaz que a de Endereço. Para ambas o desafio é decidir o momento e as máquinas que devem ser bloqueadas de modo a minimizar o número de falso-

positivos. As técnicas de Bloqueio de Endereço foram propostas por diversos autores, como nos trabalhos de Chen e Tang (2004) e de Weaver, Staniford e Paxson (2004), e basicamente consiste em interromper o link de dados de e para computadores infectados e é geralmente implementada na interface roteador/gateway. Os endereços bloqueados devem ser mantidos na memória e regularmente atualizados. Já o Bloqueio de Conteúdo permite o tráfego legítimo, mas impede o fluxo de dados suspeitos pela rede, o que ocasiona menos impacto nos casos de falso alarme. O algoritmo proposto por Weaver e Paxson (2004), por exemplo, interrompe o tráfego suspeito e permite que apenas as conexões pré-estabelecidas permaneçam ativas;

- Armadilha: são sistemas computacionais vulneráveis presentes na rede, que podem atrair o ataque cibernético. Provos (2004) usou em seu trabalho armadilhas virtuais, denominadas HoneyD, que ao serem atacadas por malware respondiam com medidas de descontaminação. Neste trabalho foi mostrado que se o sistema fosse ativado em 20 minutos após o início do surgimento dos worms, seriam necessárias cerca de 262000 armadilhas para parar completamente a epidemia. Em casos reais, no entanto, nem sempre existem medidas de descontaminação disponíveis, o que torna a abordagem de pouca utilidade.

2.2 Modelos de Propagação de Malware

A modelagem epidemiológica tem as suas origens no estudo de propagação de doenças infecciosas, sendo que, os trabalhos de Kermack e McKendrick (1927, 1932, 1933) de grande influência sobre o desenvolvimento de modelos matemáticos epidemiológicos. Estes trabalhos propuseram modelos que descrevem a dinâmica da propagação de infecções da população, que era dividida em três grupos de indivíduos, descritos a seguir:

- **Suscetível (S):** indivíduos nesta categoria não foram infectados, embora sejam vulneráveis e possam ser infectados;
- **Infectado (I):** os indivíduos desta classe foram infectados e podem espalhar a doença;
- **Recuperado (R):** os que estão nesta classe foram infectados e morreram ou ficaram imunes da doença e não podem mais ser infectados.

O comportamento da epidemia era determinado através de equações que permitiam calcular o número de indivíduos, em cada uma das classes ao longo do tempo. Além disso, outros autores propuseram modelos de propagação semelhantes, que dividiam os indivíduos da população em classes ou compartimentos. Podemos citar dentre os modelos epidemiológicos clássicos, o SI (suscetível-infectado), o SIS (suscetível-infectado-suscetível) e o SIR (suscetível-infectado-recuperado) (Allen, 1994).

Além dos modelos clássicos, foram apresentados diversos trabalhos, com diferentes estratégias para descrever os comportamentos das epidemias. De modo geral, de acordo com Peng, Yu e Yang (2014), os modelos epidemiológicos podem ser classificados em três categorias: determinísticos, estocásticos e espaço-temporais.

2.2.1 Modelos Epidemiológicos Determinísticos

Esta seção abordará os modelos SI, SIS, SIR e SIRS. Nestes quatro modelos, os indivíduos da população são classificados em: suscetível (S), infectado (I) e recuperado (R). As Figuras 1(a), 1(b), 1(c) e 1(d), representam as transições de estados para os modelos SI, SIS, SIR e SIRS, respectivamente.

Os parâmetros destes modelos são:

- **μ** é a taxa de natalidade, que significa o número de indivíduos recém-nascidos na população por unidade de tempo;
- **λ** é a taxa de mortalidade, que representa o número de mortes por infecção por unidade de tempo;
- **N** é o número de indivíduos na população, que é igual à soma dos suscetíveis, infectados e recuperados. Quando μ for diferente de λ, o número de indivíduos, N, será variável no tempo;
- **S(t)** é o número de indivíduos suscetíveis em função do tempo;
- **I(t)** é o número de indivíduos infectados em função do tempo;
- **R(t)** é o número de indivíduos recuperados em função do tempo;
- **β** é a taxa de infecção, que é interpretada como a taxa com a qual os indivíduos infectados transmitem a doença;

- **α** representa a taxa de recuperação;
- **δ** é a taxa de perda de imunidade, que representa a taxa com a qual o indivíduo recuperado torna-se novamente suscetível;
- **βSI** é o número de infecções por unidade de tempo;
- **αI** é o número de novos recuperados por unidade de tempo;
- **δR** é o número de novos suscetíveis por unidade de tempo.

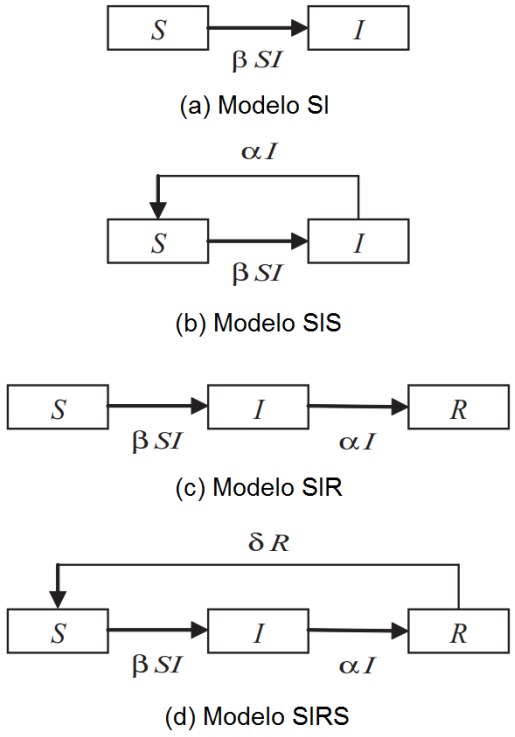


Figura 1 - Modelos Epidemiológicos determinísticos

Fonte: Adaptado de PENG, S.; YU, S.; YANG, A., 2014

A) Modelo SI

No modelo SI, consideramos que os indivíduos suscetíveis são contaminados através do contato com infectados, e permanecem neste estado indefinidamente. A dinâmica deste modelo é dada pelo sistema de equações a seguir:

$$\begin{cases} S(t) = \dfrac{\left(\frac{N-I_0}{I_0}\right)\cdot Ne^{-N\beta t}}{1+\left(\frac{N-I_0}{I_0}\right)\cdot e^{-N\beta t}} \\ I(t) = \dfrac{N}{1+\left(\frac{N-I_0}{I_0}\right)\cdot e^{-N\beta t}} \\ N = S(t) + I(t) \\ I_0 = I(0) \end{cases}$$

B) Modelo SIS

No modelo SIS, o indivíduo suscetível, depois de ser contaminado e se tornar infectado, pode retornar ao estado anterior, isto é, voltar a ser suscetível. O comportamento do modelo é descrito pelas equações abaixo:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{\beta S(t)I(t)}{N} + (\alpha+\lambda)I(t) \\ \dfrac{dI(t)}{dt} = \dfrac{\beta S(t)I(t)}{N} - (\alpha+\lambda)I(t) \\ N = S(t) + I(t) \end{cases}$$

C) Modelo SIR

Neste modelo, os indivíduos suscetíveis, que foram infectados, adquirem imunidade e passam a fazer parte da classe de recuperados. Estes não voltam a ser infectados novamente. O conjunto de equações que descreve o modelo é:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{\beta S(t)I(t)}{N} + \lambda(I(t)+R(t)) \\ \dfrac{dI(t)}{dt} = \dfrac{\beta S(t)I(t)}{N} - (\alpha+\lambda)I(t) \\ \dfrac{dR(t)}{dt} = \alpha I(t) - \lambda R(t) \\ N = S(t) + I(t) + R(t) \end{cases}$$

Para o caso em que o número de indivíduos na população (N) é constante, o sistema de equações do modelo pode ser escrito como:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta S(t)I(t) \\ \dfrac{dI(t)}{dt} = \beta S(t)I(t) - \alpha I(t) \\ \dfrac{dR(t)}{dt} = \alpha I(t) \end{cases}$$

D) Modelo SIRS

O modelo epidemiológico SIRS (suscetível-infectado-recuperado-suscetível) considera que quando o indivíduo infectado se recupera, ele pode voltar ao estado suscetível. As equações que regem este modelo são apresentadas abaixo:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{\beta S(t)I(t)}{N} + \lambda(I(t) + R(t)) + \delta R(t) \\ \dfrac{dI(t)}{dt} = \dfrac{\beta S(t)I(t)}{N} - (\alpha + \lambda)I(t) \\ \dfrac{dR(t)}{dt} = \alpha I(t) - \lambda R(t) - \delta R(t) \\ N = S(t) + I(t) + R(t) \end{cases}$$

2.2.2 Modelos Epidemiológicos Estocásticos

Os modelos estocásticos incluem três tipos principais (PENG; YU; YANG, 2014): **(1)** modelo de cadeia Markov de tempo discreto (CMTD), **(2)** modelo de cadeia de Markov de tempo contínuo (CMTC), **(3)** modelo estocástico de equação diferencial (EED). Estes modelos estocásticos diferem em seus pressupostos sobre as variáveis de tempo e espaço. No modelo CMTD ambas as variáveis de tempo e espaço são discretas, enquanto no CMTC, o tempo é contínuo e a variável de estado é discreta. No modelo EED, tanto a variável de estado quanto o tempo são contínuos. Nesta revisão de modelos epidemiológicos, abordamos os modelos CMTD Suscetível-Infectado-Suscetível e CMTC Suscetível-Infectado-Suscetível.

Seja Y(t) a variável aleatória no tempo t. Assumimos que a taxa de incidência, β_i, e a taxa de recuperação, α_i são funções contínuas e diferenciáveis da população de tamanho i. Além disso, assume-se que existem números K e N tais que $0 < K < N$ e: (1) $\beta_0 = \alpha_0 = 0$ e $\beta_i = 0$ para $i \geq N$, (2) $\beta_i > 0$ e $\alpha_i > 0$ para $0 \leq i \leq N$, (3) $\beta_i > \alpha_i$ para $0 \leq i \leq K$, (4) $\beta_i < \alpha_i$ para $K < i \leq N$.

No modelo epidemiológico CMTD SIS, tanto o tempo quanto o tamanho da população têm valores discretos. Seja Δt um intervalo de tempo fixo e t ∈ {0, Δt, 2Δt, · · · }. Assume-se que Δt é suficientemente pequeno, de modo que no máximo um evento ocorre durante o intervalo de tempo Δt. Este evento será uma infecção, recuperação, nascimento ou morte, que depende apenas dos valores das variáveis de estado no momento atual. Como o tamanho da população permanece constante, o nascimento e a morte devem ocorrer simultaneamente. Sejam as probabilidades associadas a Y(t) denominadas $p_i(t) = \text{Prob}\{Y(t) = i\}$ e $p(t) = (p_0(t), ..., p_N(t))^T$. Assim, as probabilidades de transição são escritas à seguir.

$$\begin{cases} P\{Y(t+\Delta t) = i-1 | Y(t) = i\} = \alpha_i \Delta t \\ P\{Y(t+\Delta t) = i+1 | Y(t) = i\} = \beta_i \Delta t \\ P\{Y(t+\Delta t) = i | Y(t) = i\} = 1 - (\alpha_i - \beta_i)\Delta t \\ P\{Y(t+\Delta t) = k | Y(t) = i\} = 0, |i-k| \geq 2 \end{cases}$$

Como as probabilidades acima satisfazem as equações de diferença $p_i(t+\Delta t)$ e $p_i(t+\Delta t) = \beta_{i-1}\Delta t p_{i-1}(t) + \alpha_{i+1}\Delta t p_{i+1}(t) + (1-(\beta_i + \alpha_i)\Delta t)p_i(t)$, as equações de diferença para o modelo de tempo discreto podem ser expressas em forma de matriz, com a matriz de transição P (N+1)x(N+1) abaixo:

$$\begin{pmatrix} 1 & \alpha_1 \Delta t & \dots & 0 \\ 0 & 1-(\beta_1+\alpha_1)\Delta t & \cdots & 0 \\ 0 & \beta_1 \Delta t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha_N \Delta t \\ 0 & 0 & \cdots & 1-\alpha_N \Delta t \end{pmatrix}$$

Para garantir que *P* é uma matriz estocástica, assumimos

$$\max_{i \epsilon \{i,2,\dots,N\}} \{(\beta_i + \alpha_i)\Delta t\} \leq 1$$

No modelo epidemiológico CMTC SIS, o modelo de tempo contínuo correspondente é um processo de salto de Markov, com os saltos formando uma cadeia de Markov, e o processo estocástico depende do conjunto de variáveis aleatórias discretas $t \in [0, \infty)$, $Y(t) \in \{0, 1, 2, ..., N\}$ e suas funções de probabilidade associadas $p(t) = (p_0(t), ..., p_N(t))^T$, onde $p_i(t) = \text{Prob}\{Y(t) = i\}$. As probabilidades de transição para o modelo CMTC são as seguintes:

$$\begin{cases} P\{Y(t+\Delta t)=i-1|Y(t)=i\}=\alpha_i\Delta t+o(\Delta t) \\ P\{Y(t+\Delta t)=i+1|Y(t)=i\}=\beta_i\Delta t+o(\Delta t) \\ P\{Y(t+\Delta t)=i|Y(t)=i\}=1-(\alpha_i+\beta_i)\Delta t+o(\Delta t) \\ P\{Y(t+\Delta t)=k|Y(t)=i\}=o(\Delta t), |i-k|\geq 2 \end{cases}$$

Tomando o limite como $\Delta t \to 0$, podemos mostrar que um sistema de equações diferenciais para as probabilidades $p_i(t) = \text{Prob}\{Y(t) = i\}$ satisfazem as equações diferenciais diretas de Kolmogorov: $\frac{dp_i(t)}{dt}=\beta_{i-1}p_{i-1}(t)+\alpha_{i+1}p_{i+1}(t)-(\beta_i+\alpha_i)p_i(t)$, onde i ∈ {1, · · · , N} e $\frac{dp_0(t)}{dt} = \alpha_1 p_1(t)$. Assim, as equações de diferença para o modelo de tempo contínuo podem ser expressas na forma matricial com a definição da matriz de transição Q.

$$Q=\begin{pmatrix} 0 & \alpha_1 & 0 & \cdots & 0 \\ 0 & -(\beta_1+\alpha_1) & \alpha_2 & \cdots & 0 \\ 0 & \beta_1 & -(\beta_2+\alpha_2) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_N \\ 0 & 0 & 0 & \cdots & -\alpha_N \end{pmatrix}$$

2.2.3 Modelos Epidemiológicos Espaço-Temporais

Autômatos Celulares (AC) são uma classe de sistemas dinâmicos discretos, consistindo em uma matriz de nós (células) de dimensão *n*. Cada célula pode estar em um dos k diferentes estados em um determinado instante de tempo *t*. A cada instante, as células podem mudar seus estados, de maneira determinada pelas regras de transição do AC. As regras de transição descrevem como uma determinada célula deve mudar de estado, dependendo de seu estado atual e dos estados de seus vizinhos (SONG; JIANG; GU, 2008).

Podemos definir o autômato celular pela quádrupla:

$$\text{AC} = (N, Q, V, F),$$

onde:

N é o espaço celular, no qual, a cada instante, cada célula deve estar em um dos possíveis estados. Este espaço celular pode ter dimensões quaisquer. Por exemplo, um autômato celular unidimensional pode ser apresentado como uma cadeia de células dispostas em uma dimensão ao longo de um eixo. Enquanto, um autômato

bidimensional pode ser apresentado como uma matriz de células de mesmo tamanho apoiadas sobre um plano cartesiano. Os elementos do conjunto *Q* representam todos os possíveis estados das células. O estado de cada célula *i* no instante *t* é representado por $s_i(t)$, enquanto o estado das células em sua vizinhança é dado por $s_{Vi}(t\text{-}1)$, e V_i é a vizinhança da célula *i*. Finalmente, *f* denota as regras de transição de estado, que estabelece a dinâmica do autômato. As regras definem para qual estado cada célula deve ir, em função do seu estado e dos estados dos seus vizinhos no tempo presente. Algebricamente, podemos representar:

$$s_i(t) = f(s_i(t-1), s_{V_i}(t-1))$$

Para um autômato unidimensional, por exemplo, podemos definir a sua vizinhança *V* por um conjunto de duas células, isto é um vizinho de cada lado. Para um autômato bidimensional, podemos definir a vizinhança por $V = \{(x_k, y_k), 1 \leq k \leq N\} \subset Z \times Z$. Para o autômato bidimensional, dois tipos importantes de vizinhança são a de Von Neumann e a de Moore, ilustradas nas figuras 2(a) e 2(b), respectivamente.

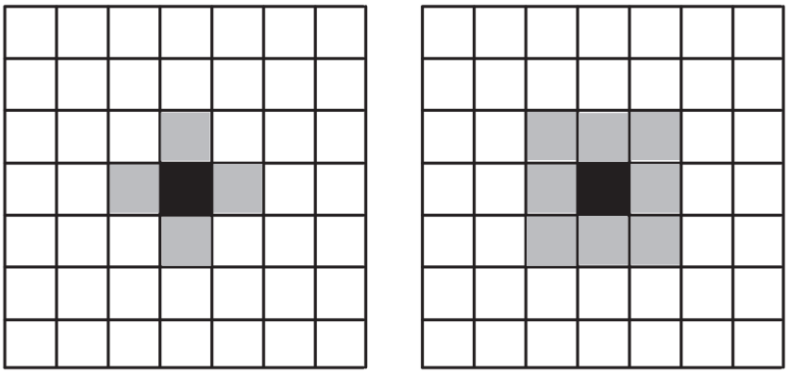


Figura 2 - Vizinhanças de Von Neumann e Moore

Fonte: Adaptado de Peng, Yu e Yang (2014)

2.3 Modelos de Contenção de Malware com Alerta

Com o propósito de estudar os impactos da propagação de malware nas redes de computadores, assim como avaliar os desempenhos de estratégias de combate, diversos modelos de propagação foram propostos na literatura, desde os que abordam o sistema do ponto de vista macroscópico (KEPHART; WHITE, 1991; PIQUEIRA; ARAUJO, 2009; MISHRA; PANDEY, 2011), os que observam o problema de média escala (PASTOR-SATORRAS;

VESPIGNANI, 2001; BARTHÉLEMY et al., 2004; YANG; CHEN; FU, 2011) e os que consideram o problema ao nível individual (VAN MIEGHEM; OMIC; KOOIJ, 2009; VAN MIEGHEM, 2011).

Modelos epidêmicos com estratégia de alerta também foram propostos, como o SAIS (Suscetível-Alerta-Infectado-Suscetível) (SAHNEH; SCOGLIO, 2011; SAHNEH; CHOWDHURY, 2012; SAHNEH; SCOGLIO, 2012; JUHER; KISS; SALDAÑA, 2015). A importância de alertar no estágio inicial da invasão reside no fato de que antes que uma solução eficaz contra um novo vírus esteja disponível, a propagação de alertas sobre o vírus através das redes ajuda a reduzir a possibilidade de infecção de nós suscetíveis (ZHANG et al, 2017).

O modelo epidemiológico proposto por Sahneh e Scoglio (2011) acrescentava o estado alerta ao modelo Suscetível-Infectado-Suscetível (SIS) e foi assim denominado SAIS. Neste modelo, cada indivíduo poderia estar infectado, suscetível ou alerta. Os indivíduos suscetíveis poderiam ficar alertas com uma dada frequência, quando existissem indivíduos infectados em sua vizinhança. Quando em estado de alerta, o comportamento mais cauteloso do indivíduo faria com que a sua probabilidade de ser infectado diminuísse. O modelo foi elaborado como um processo de Markov de tempo contínuo e formulado como um sistema de equações diferenciais ordinárias.

O trabalho de Sahneh, Scoglio e Mieghem (2013), apresenta um exemplo usando o modelo epidemiológico SAIS, ilustrado na Figura 3. Neste exemplo, a passagem do estado infectado (*I*) para suscetível (*S*), que representa a cura da doença, ocorre segundo a taxa ou razão δ. A taxa de infecção é dada por $\beta \cdot Y_i(t)$, a passagem do estado suscetível (*S*) para o estado alerta (*A*) ocorre com taxa $k \cdot Y_i(t)$, enquanto a transição do estado alerta (*A*) para infectado (*I*) acontece com taxa $\beta_a \cdot Y_i(t)$. Sendo $\beta_a < \beta$ e $Y_i(t)$ o número de vizinhos infectados do nó *i* no instante *t*.

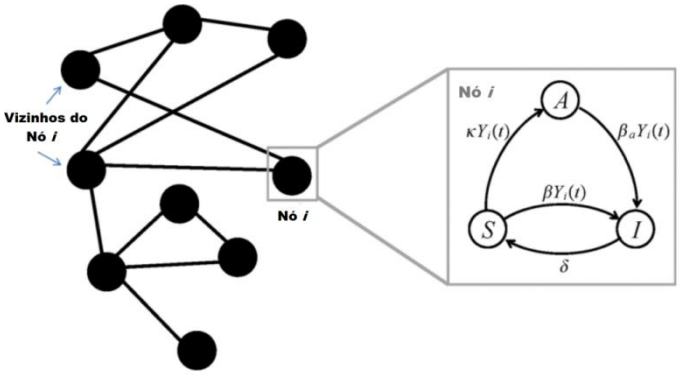


Figura 3 - Exemplos de aplicação do modelo SAIS
Fonte: Adaptado de Sahneh, Scoglio e Mieghem (2013)

2.3.1 Contenção de Malware com Alerta Baseado no Modelo SAIS

O trabalho de Zhang et al. (2017) descreve uma estratégia de contenção de malware, baseada no modelo epidemiológico SAIS, com envio de mensagens de alerta pela rede. O estudo mostrou que a estratégia foi capaz de conter a propagação e reduzir significativamente o ataque cibernético. O trabalho formula e trata o problema de controle ótimo baseado no modelo epidemiológico. A seguir são apresentadas as hipóteses sobre as transições de estado do modelo, e o problema de controle ótimo que se deseja resolver.

As hipóteses [H1-H7] sobre as transições de estado são mostradas abaixo:

H1 No instante t, o nó suscetível i é alertado através do nó j, com uma probabilidade $\alpha_{ij}(t)$, onde (a) $\alpha_{ij}(t) \in L^2[0, T]$, e (b) $\underline{\alpha} \leq \alpha_{ij} \leq \overline{\alpha}$, $0 \leq t \leq T$.

H2 Em qualquer instante, o nó suscetível i pode ser contaminado por um nó j infectado, com probabilidade $\beta_{1ij} \geq 0$. Assim, no instante t, o nó suscetível torna-se infectado com probabilidade $\sum_{j=1}^{N} \beta_{1ij} I_j(t)$.

H3 O nó alerta i pode ser contaminado por um nó infectado j, com probabilidade $0 \leq \beta_{2ij} \leq \beta_{1ij}$. Assim, o nó alerta i é infectado com probabilidade $\sum_{j=1}^{N} \beta_{2ij} I_j(t)$.

H4 O nó infectado i pode ser curado no instante t e tornar-se susceptível, com probabilidade $\gamma_i(t)$, onde (a) $\gamma_i(t) \in L^2[0, T]$, e (b) $\underline{\gamma} \leq \gamma_i(t) \leq \overline{\gamma}$, $0 \leq t \leq T$.

H5 O valor da perda de um nó infectado i é dado por $c_i > 0$.

H6 O custo do nó j alertar o nó suscetível i, no instante t, é dado por $g(\alpha_{ij}(t))$, onde a função g é diferenciável.

H7 O custo para curar o nó infectado i, no instante t, é dado por $h(\gamma_i(t))$, onde a função h é diferenciável.

A Figura 4 ilustra o modelo descrito pelas hipóteses H_1 a H_4:

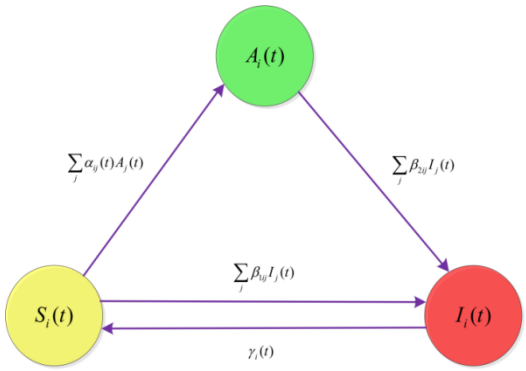


Figura 4- Diagrama do modelo SAIS
Fonte: Adaptado de Zhang et al. (2017)

Fazendo o intervalo de tempo Δt muito pequeno, as hipóteses H_1-H_4 implicam que as probabilidades das transições de estado do nó i satisfazem as seguintes relações:

Pr(i é alerta no instante t+Δt | i é suscetível no tempo t) = $\Delta t \sum_{j=1}^{N} \propto_{ij} (t) A_j(t) + o(\Delta t)$

Pr(i é infectado no instante t+Δt | i é alerta no tempo t) = $\Delta t \sum_{j=1}^{N} \beta_{1ij}(t) I_j(t) + o(\Delta t)$

Pr(i é infectado no instante t+Δt | i é alerta no instante t) = $\Delta t \sum_{j=1}^{N} \beta_{2ij}(t) I_j(t) + o(\Delta t)$

Pr(i é suscetível no instante t+Δt | i é infectado no instante t) = $\gamma_i(t)\Delta t + o(\Delta t)$

Invocando a lei da probabilidade total, reorganizando os termos, e fazendo $\Delta t \to 0$, obtemos o seguinte sistema dinâmico:

$$\begin{cases} \dfrac{dA_i(t)}{dt} = [1 - A_i(t) - I_i(t)]\sum_{j=1}^{N} \alpha_{ij}(t)A_j(t) - A_i(t)\sum_{j=1}^{N} \beta_{2ij}I_j(t), & t \geq 0 \quad , \quad 1 \leq i \leq N \\ \dfrac{dI_i(t)}{dt} = [1 - A_i(t) - I_i(t)]\sum_{j=1}^{N} \beta_{1ij}I_j(t) + A_i(t)\sum_{j=1}^{N} \beta_{2ij}I_j(t) - \gamma_i(t)I_i(t), & t \geq 0, \quad 1 \leq i \leq N \end{cases}$$

O modelo é chamado de SAIS controlado, onde o controle é dado por:

$$\mathbf{u}(t) = (\alpha_{11}(t),...,\alpha_{1N}(t),...\alpha_{N1}(t),...,\alpha_{NN}(t),\gamma_1(t),...,\gamma_N(t))^T$$

E o conjunto de controle admissível é

$$\mathcal{U} = \left\{\boldsymbol{u}(t) \in (L^2[0,T])^{N(N+1)} | \underline{\alpha} \leq \alpha_{ij}(t) \leq \overline{\alpha}, \quad \underline{\gamma} \leq \gamma_i(t) \leq \overline{\gamma}, 0 \leq t \leq T, 1 \leq i,j \leq N\right\}$$

Este modelo pode ser escrito usando notação matricial assim:

$$\frac{d\boldsymbol{x}(t)}{dt} = \boldsymbol{f}\big(\boldsymbol{x}(t), \boldsymbol{u}(t)\big) \quad t \geq 0$$

O propósito é determinar $\mathbf{u}(t) \in \mathcal{U}$, tal que o compromisso (tradeoff) cumulativo, denominado J($\mathbf{u}$(t)), o qual é definido como a soma da perda cumulativa devida às infecções e o custo cumulativo do alerta e tratamento, seja minimizado. Isto é, desejamos minimizar a expressão:

$$J\big(\boldsymbol{u}(t)\big) = \sum_{i=1}^{N} c_i \int_0^T I_i(t)dt + \sum_{ij=1}^{N} \int_0^T g\left(\alpha_{ij}(t)\right)dt + \sum_{i=1}^{N} \int_0^T h\big(\gamma_i(t)\big)dt$$

Finalmente, chega-se ao seguinte problema de controle ótimo que o trabalho deseja resolver:

Minimizar

$$\mathbf{u} \in \mathcal{U} \;\; J(\boldsymbol{u}) = \int_0^T F\big(\boldsymbol{x}(t), \boldsymbol{u}(t)\big)dt \text{ sujeito a } \frac{d\boldsymbol{x}(t)}{dt} = \boldsymbol{f}\big(\boldsymbol{x}(t), \boldsymbol{u}(t)\big), \; 0 \leq t \leq T,$$

onde

$$F\big(\boldsymbol{x}(t), \boldsymbol{u}(t)\big) = \sum_{i=1}^{N} c_i I_i(t) + \sum_{ij=1}^{N} g(\alpha_{ij}(t)) + \sum_{i=1}^{N} h(\gamma_i(t))$$

2.4 Contribuições deste Trabalho

Diversos trabalhos têm apoiado o uso de modelos de propagação baseados no paradigma *SIR* (Suscetível-Infectado-Recuperado) para representar ataques a sistemas computacionais (LOPEZ; PEINADO; ORTIZ, 2019; MAHBOUBI; CAMTEPE; MORARJI, 2017; CISOTO; BADIA, 2016). Além disso, o uso de modelos epidemiológicos associados a estratégias de alerta foi demonstrado por diversos autores (SAHNEH; SCOGLIO, 2011; SAHNEH; CHOWDHURY, 2012; SAHNEH; SCOGLIO, 2012; JUHER; KISS; SALDAÑA, 2015).

Diversos exemplos de modelos epidemiológicos baseados no *SIR* que levam em conta informações de alerta vêm sendo recentemente apresentados na literatura. Por exemplo, os trabalhos de Zheng et al. (2018) e o Wang et al. (2019) descrevem dois tipos de propagação que ocorrem através de redes diferentes: uma por onde são transmitidas informações de alerta, e a outra, do tipo SIR, através da qual a epidemia é disseminada. Os artigos de Kabir, Kuga e Tanimoto (2019) e o de Bajiya et al. (2022) adotam o modelo epidemiológico SIR com informações de alerta, no qual os indivíduos suscetíveis alertados têm menor chance de serem contaminados que os suscetíveis não alertas.

O estudo de Kabir e Tanimoto (2019) descrevem um modelo, que além de incorporar informações sobre alerta, acrescentam o estado *vacinado* ao SIR, sendo que os suscetíveis e alerta têm menor chance de serem infectados que os suscetíveis não alertas. O trabalho de Goel, Kumar e Nilam (2020) discorre sobre um modelo epidemiológico que acrescenta dois estados ao SIR: *parcialmente alerta* e *completamente alerta*. Estes dois e o estado suscetível são vulneráveis à infecção, mas aquele *completamente alerta* têm menor probabilidade que os demais de ser infectado.

Kumar, Nilam e Kishor (2019) apresentaram o modelo epidemiológico *SAIR* (Suscetível-Alerta-Infectado-Recuperado), que consiste no modelo clássico *SIR* com mais um compartimento, o *alerta*. Os indivíduos *alertas* podem ser contaminados, mas com probabilidade diferente dos *suscetíveis*.

Os modelos epidemiológicos com alerta, além de aplicados em estudos envolvendo propagação de doenças infecciosas, também foram propostos especificamente como estratégia de contenção de malware (ZHANG et al., 2017). Para contribuir com a área, descrevendo um modelo de contenção, que alie o paradigma *SIR* a uma estratégia de transmissão de alertas pela

rede, este trabalho apresenta o modelo epidemiológico espaço-temporal *SASIR* (Susceptível-Alerta-Susceptível-Infectado-Recuperado). A descrição deste modelo, através da plataforma espaço-temporal, contribui para o estado da arte e é particularmente oportuna porque evidencia a natureza espacial envolvida na dinâmica do mecanismo de alerta. O desempenho deste sistema será examinado através de simulações com exemplos de ataques cibernéticos, usando diferentes parâmetros de funcionamento e em distintos cenários de ataques.

Além disso, para o modelo espaço-temporal *SIR*, serão determinados o valor e a configuração espacial na qual a derivada do número de **infectados** em função do **tempo** é máxima. Esta medida é importante uma vez que para que seja deflagrada a epidemia é condição necessária que este valor seja maior que zero.

O texto também discorre sobre uma proposta de medida de eficiência, sob o ponto de vista da redução dos impactos causados pelos ataques cibernéticos. Estes impactos são representados pelos custos operacionais envolvidos, e a eficiência é obtida pelo cálculo da redução dos custos, conseguida pelo *SASIR*, quando comparados àqueles do modelo clássico *SIR*.

3 O MODELO EPIDEMIOLÓGICO ***SASIR***

Este capítulo traz uma revisão sobre autômatos celulares e, em seguida, apresenta o modelo de contenção de malware *SASIR* (Susceptível-Alerta-Susceptível-Infectado-Recuperado). O modelo espaço-temporal será implementado como autômato celular bidimensional, além disso, serão discutidas motivações sobre o uso do modelo sob o ponto de vista de custos operacionais.

Para ε1=0, será demonstrada a condição necessária para que a epidemia seja deflagrada, e será calculada a derivada máxima do número de *infectados* pelo tempo e a configuração espacial em que ela ocorre.

3.1 Revisão sobre Autômato Celular

Autômatos Celulares (ACs) são uma classe de sistemas dinâmicos discretos, consistindo em uma matriz de nós (células) de dimensão n. Cada célula pode estar em um dos k estados diferentes em um determinado instante de tempo t. A cada instante de tempo discreto, cada célula pode mudar seu estado, de maneira determinada pelas regras de transição locais do AC em questão. As regras de transição descrevem como uma determinada célula deve mudar de estado, em função de seu estado atual e dos estados de seus vizinhos. Isto exige também que as vizinhanças das células sejam definidas (SONG; JIANG; GU, 2008).

O autômato celular é definido pela quádrupla:

$$AC = (N,Q,V,f)$$

onde:

N é o espaço celular, no qual cada célula pode estar em um determinado estado de um conjunto de estados distintos possíveis, em cada instante de tempo discreto. Este espaço celular pode ser de qualquer dimensão e é de extensão infinita. Assim, por exemplo, um AC unidimensional pode ser visualizado como tendo uma célula em cada número inteiro na reta numérica real. Um AC bidimensional pode ser representado por células em todos os pontos do plano de coordenadas (*x*, *y*), onde *x* e *y* são inteiros. O conjunto *Q* é finito e seus elementos são todos os estados possíveis das células. O estado

da célula i no tempo t é denotado por $s_i(t)$ e o estado de sua vizinhança por $s_{vi}(t)$, onde V_i denota a vizinhança da célula i. A vizinhança de qualquer célula, pode ser definida como um vetor espacial incluindo v célula(s) vizinhas. Por último, f denota o conjunto de regras de transição locais, que definem o comportamento dinâmico do autômato. Cada célula vai para o estado seguinte de acordo com as regras de transição, e em função do seu estado e do estado de sua vizinhança no instante atual. Assim, temos:

$$s_i(t) = f(s_i(t-1), s_{V_i}(t-1))$$

3.2 Modelo SASIR com Autômatos Celulares

O modelo epidemiológico *SASIR* acrescenta o estado *alerta* ao modelo *SIR*. A inclusão deste estado no modelo clássico permite aos indivíduos suscetíveis reagir diante da presença de infectados, alterando os seus comportamentos, para reduzir a probabilidade de serem infectados, e alertando os seus vizinhos para que façam o mesmo.

Quando na presença de uma célula vizinha infectada, a célula suscetível, no instante seguinte, pode infectar-se, com probabilidade $\beta_1 \geq 0$ ou ficar alerta, com probabilidade $\varepsilon_1 \geq 0$. Além disso, as células que entram em alerta em determinado instante, alertam os seus vizinhos suscetíveis no instante seguinte. Uma vez no estado alerta, a probabilidade da célula ser infectada passa a ser igual a $0 \leq \beta_2 < \beta_1$ e a probabilidade de permanecer no estado alerta quando o vizinho está *infectado* passa para a ser igual a $\varepsilon_2 > \varepsilon_1$. O aumento da probabilidade ε_2 em relação a ε_1 representa a maior capacidade da célula alerta, quando comparada à suscetível, de detectar a presença de infectados na vizinhança. As células *infectadas* podem ser *recuperadas*, com probabilidade γ, e as células que foram *recuperadas* permanecem indefinidamente neste estado.

De maneira formal, o modelo do autômato pode ser definido da seguinte maneira:

Células: todos os nós da rede são células, isto é, cada nó é uma célula

Espaço celular: o espaço pode ter dimensão n qualquer

Vizinhança: podemos definir a matriz de adjacência A da rede que denota a vizinhança das células, e o elemento a_{ij} referindo-se à conexão entre as células *i* e *j*

Espaço de estados: no modelo *SASIR*, cada nó pode ser suscetível (estado S), infectado (estado I), recuperado (estado R) e alerta (estado A). Fazemos Q = {S,I,R,A}, e denotamos $s_i(t) \in Q$ a variável de estado do nó *i* no tempo *t.* Assim, temos:

$$s_i(t)\begin{cases} A, \text{nó } i \text{ está alerta no instante } t \\ R, \text{nó } i \text{ é recuperado no instante } t \\ I, \text{nó } i \text{ está infectado no instante } t \\ S, \text{nó } i \text{ é suceptível no instante } t \end{cases}$$

Função de transição: $s_i(t)$ é estatisticamente dependente de $s_i(t-1)$ e de $s_{Vi}(t-1)$.

As transições de estados do modelo são determinadas pelas seguintes regras:

1) Para cada célula *suscetível i* no instante *t* ($s_i(t)=S$), com *j* vizinhos.

Para cada vizinho *infectado* V_ξ da célula *i,* seja a variável aleatória uniforme

$$0 \leq X_\xi \leq 1$$

$$\begin{cases} Se\ 0 \leq X_\xi < \beta_1 \rightarrow\ I_\xi = 1\ e\ A_\xi = 0 \\ Se\ \beta_1 \leq X_\xi < \beta_1 + \epsilon_1\ \rightarrow\ I_\xi = 0\ e\ A_\xi = 1 \end{cases}$$

Seja *m* o número de vizinhos em estado alerta no instante *t.*

As células suscetíveis no instante *t* ($s_i(t)=S$), mudam de estado no instante *t*+1 segundo:

$$\begin{cases} \text{Se} \sum_{j \in V_\xi} I_j > 0\ \rightarrow\ s_i(t+1) = I \\ \text{Se} \sum_{j \in V_\xi} I_j = 0\ \wedge \sum_{j \in V_\xi} A_j > 0\ \rightarrow\ s_i(t+1) = A \\ \text{Se} \sum_{j \in V_\xi} I_j = 0\ \wedge \sum_{j \in V_\xi} A_j = 0 \wedge m > 0\ \rightarrow\ s_i(t+1) = A \\ \text{Se} \sum_{j \in V_\xi} I_j = 0\ \wedge \sum_{j \in V_\xi} A_j = 0 \wedge m = 0\ \rightarrow\ s_i(t+1) = S \end{cases}$$

2) Para cada célula *alerta i* no instante *t* ($s_i(t)=A$), com *j* vizinhos.

Para cada vizinho *infectado* V_ξ da célula *alerta i*, seja a variável aleatória uniforme

$$0 \leq X_\xi \leq 1$$

$$\begin{cases} Se\ 0 \leq X_\xi < \beta_2 \rightarrow I_\xi = 1\ e\ A_\xi = 0 \\ Se\ \beta_2 \leq X_\xi < \beta_2 + \epsilon_2 \rightarrow I_\xi = 0\ e\ A_\xi = 1 \end{cases}$$

Seja *m* o número de vizinhos em estado *alerta* no instante *t*.

As células *alertas* no instante *t* ($s_i(t)=A$), mudam de estado no instante *t*+1 segundo:

$$\begin{cases} Se \sum_{j \in V_\xi} I_j > 0 \rightarrow s_i(t+1) = I \\ Se \sum_{j \in V_\xi} I_j = 0 \wedge \sum_{j \in V_\xi} A_j > 0 \rightarrow s_i(t+1) = A \\ Se \sum_{j \in V_\xi} I_j = 0 \wedge \sum_{j \in V_\xi} A_j = 0 \wedge m > 0 \rightarrow s_i(t+1) = A \\ Se \sum_{j \in V_\xi} I_j = 0 \wedge \sum_{j \in V_\xi} A_j = 0 \wedge m = 0 \rightarrow s_i(t+1) = S \end{cases}$$

3) Para cada célula *infectada i* no instante *t* ($s_i(t)=I$)

Seja a variável aleatória uniforme $0 \leq X_i \leq 1$. A célula *infectada i* mudará de estado segundo:

$$\begin{cases} Se\ 0 \leq X_i < \gamma \rightarrow s_i(t+1) = R \\ Se\ \gamma \leq X_i \leq 1 \rightarrow s_i(t+1) = I \end{cases}$$

4) As células *recuperadas* não mudam de estado, isto é, cada célula *recuperada i* no instante *t* permanecerá neste estado no instante seguinte *t*+1. Isto é, se $s_i(t) = R$ então $s_i(t+1) = R$.

As regras de transição de estados também podem ser implementadas pelo seguinte pseudocódigo:

INÍCIO
INTEIROS viz_a1, viz_i

```
REAIS beta1, beta2, gama, epsilon1, epsilon2
// beta1: Probabilidade de S ser infectado
// beta2: Probabilidade de A1 ou A2 serem infectados
// epsilon1: Probabilidade de S ir para o estado A1
// epsilon2: Probabilidade de A1 ou A2 irem para o estado A1
// gama: Probabilidade do infectado (I) ir para o estado R
/// Ambos A1 e A2 correspondem ao estado Alerta (A). Porém, aqui no algoritmo, chamamos de A1, a célula susceptível que entrou em alerta devido ao contato com vizinho infectado, e de A2, os vizinhos de A1 que foram alertados por este. ///
PARA c ∈ células do autômato FAÇA
viz_a1 = número de vizinhos(A1)
viz_i = número de vizinhos(I)
        SE c = A1 OU c = A2 ENTÃO
                PARA X = 1 ATÉ viz_i
                        r = rand()
                        CASO r < beta2 ENTÃO
                                estado(c) = I
                        CASO r ≥ beta2 E r < beta2+epsilon2 ENTÃO
                                estado(c) = A1
                        CASO viz_a1 > 0 E r ≥ beta2+epsilon2 ENTÃO
                                estado(c) = A2
                        CASO CONTRÁRIO
                                estado(c) = S
                        FIM CASO
                FIM PARA
        FIM SE
        SE c = S ENTÃO
                PARA X = 1 ATÉ viz_i
                        r = rand()
                        CASO r < beta1 ENTÃO
                                estado(c) = I
                        CASO r ≥ beta1 E r < beta1+epsilon1 ENTÃO
                                estado(c) = A1
                        CASO viz_a1 > 0 E r ≥ beta1+epsilon1 ENTÃO
                                estado(c) = A2
                        CASO CONTRÁRIO
                                estado(c) = S
                        FIM CASO
                FIM PARA
        FIM SE
```

```
            SE c = I ENTÃO
            r = rand()
            SE r < gama ENTÃO
                  estado(c) = R
            SENÃO
                  estado(c) = I
            FIM SE
            FIM SE
            SE c = R ENTÃO
            estado(c) = R
            FIM SE
FIM PARA
PARE
FIM
```

O pseudocódigo acima, que descreve a dinâmica do modelo *SASIR*, determina os estados *suscetível*, *infectado*, *alerta* e *recuperado*, nos quais as células podem estar ao longo do tempo. Apesar de haver um único estado de *alerta* (A), o código denomina A1, o estado de *alerta* para o qual o *suscetível* pode ir quando tiver contato direto com o *infectado* e, de A2, o estado de *alerta* para o qual vão todos os vizinhos *suscetíveis* de A1. Esta diferenciação é feita para que o alerta enviado pela célula aos seus vizinhos suscetíveis não se propague para além das células que estão em contato direto com ele.

A Figura 5 ilustra o diagrama com as possíveis transições de estado do modelo *SASIR*, onde são identificadas por δ_{xy} as regras de transição do estado *x* para o estado *y*. Observa-se que a célula pode passar mais de uma vez do estado *suscetível* (*S*) para o estado *alerta* (*A*) e vice-versa, enquanto para os demais estados (*Infectado* e *Recuperado*) ela pode passar apenas uma vez.

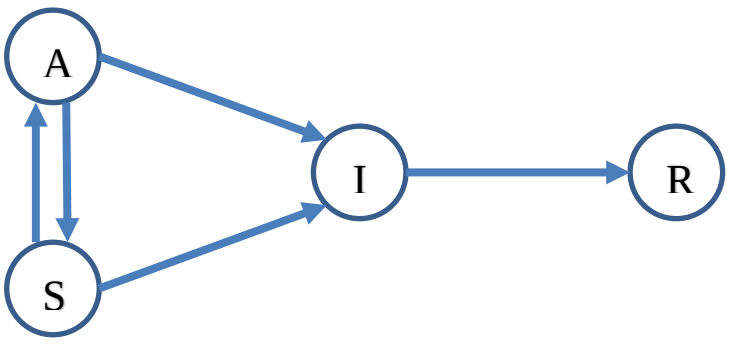


Figura 5 - Diagrama de transições de estado do modelo SASIR

3.2.1 Modelo SASIR com Autômato Bidimensional

Embora, em princípio, o modelo possa ser implementado usando autômato com espaço celular de dimensão qualquer, neste trabalho, adotaremos o espaço celular de dimensão igual a dois. O modelo bidimensional facilita a visualização, permitindo apresentar o autômato em um plano, além de conseguir representar adequadamente ataques cibernéticos e a dinâmica da propagação de malware em redes computacionais.

Este modelo utiliza a vizinhança de Moore, conforme Figura 6.

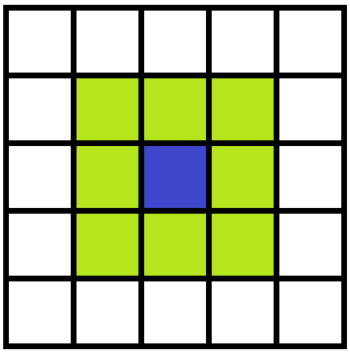
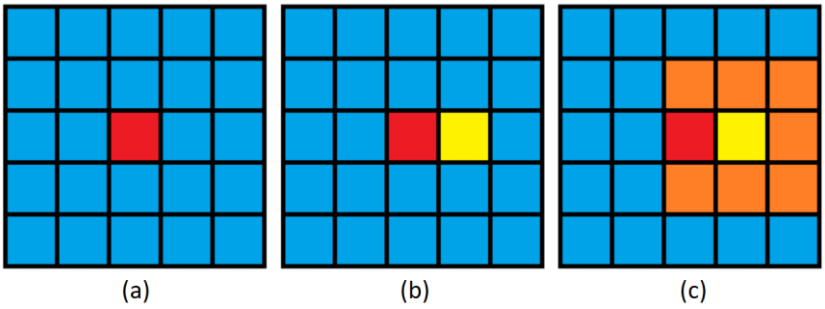


Figura 6 - Célula com vizinhança de Moore

A Figura 7 ilustra o mecanismo de contenção da propagação do malware, implementado pelo modelo bidimensional: (a) no instante inicial há uma célula infectada representada em vermelho, (b) no instante seguinte uma célula vizinha, em amarelo, entra em alerta, e (c) em seguida, esta célula dispara alertas para todos as suas células vizinhas suscetíveis (em laranja).

Por meio desta estratégia, as máquinas suscetíveis detectam as vizinhas infectadas, e entram em modo de alerta, adaptando os seus comportamentos de modo a reduzir os riscos de contaminação e alertando as vizinhas vulneráveis para que façam o mesmo. A propagação da infecção é mitigada uma vez que as células vizinhas das infectadas acabam atuando como barreiras, cercando as infectadas e retardando a transmissão.



(a) célula infectada (em vermelho),

(b) uma célula vizinha entra em alerta (em amarelo),

(c) a célula alerta todos os seus vizinhos suscetíveis (em laranja)

Figura 7- Mecanismo de contenção

3.2.2 Considerações sobre os Custos e Motivação para o uso do Modelo

A justificativa para o emprego do modelo epidemiológico com alerta, *SASIR*, reside no fato de que esta estratégia promove a redução dos danos causados pelo ataque cibernético. Assim, devemos estabelecer a maneira pela qual estes danos são mitigados e, avaliar, através de uma métrica, os impactos esta redução.

Uma estratégia para avaliar quantitativamente esta redução pode ser através do cálculo da diferença entre os custos acarretados pela disseminação do malware nos cenários descritos pelos modelos *SIR* e *SASIR*. Esta comparação permite medir a redução dos custos promovida pela adoção da estratégia do modelo de alerta em comparação com o modelo sem alerta.

Podemos considerar que o custo da disseminação do malware é dinâmico, e varia conforme os efeitos do ataque cibernético vão surgindo. É possível ponderar que o custo total é a soma dos diversos custos envolvidos na operação do sistema, tais como aqueles relacionados às transições entre os estados (S↔A→I→R), além dos referentes às operações nos estados *alerta*, *suscetível*, *infectado* e *recuperado*, aqui denominados $c(A)$, $c(S)$, $c(I)$ e $c(R)$, respectivamente. Isto é, podemos associar a cada um dos quatro estados possíveis da máquina uma função custo de operação. Assim, por exemplo, o custo do prejuízo causado pela infecção de uma máquina da rede ao longo do tempo, seria dado pela função $c(I)$.

Neste trabalho não serão considerados os custos associados às transições de estados, mas apenas os envolvidos nas operações, isto é, $c(A)$, $c(S)$, $c(I)$ e $c(R)$, que podem ser definidos arbitrariamente, conforme a natureza dos fenômenos que se deseja observar. Contudo, aqui por simplificação, cada uma deles será definido como constante. Assim, de maneira formal, fazendo $c(s_i(t))$, o custo de cada célula i, no estado $s_i(t)$ no instante t, podemos dizer que o custo total para um sistema *SASIR* com N células, ao longo do intervalo de tempo de 0 a T é dado por $\mathrm{C_{SASIR}}(T) = \sum_{t=0}^{T}\sum_{i=1}^{N} c\left(s_i(t)\right)$.

Embora este texto admita o uso do termo *tempo* como parâmetro nas equações do modelo, deve ser observado que as mudanças de estado do autômato celular ocorrem a cada iteração. Assim, o vocábulo *tempo* está sendo usado aqui com o sentido de passos de tempo discreto do autômato.

Definiremos a eficiência relativa (Er) do sistema *SASIR* como sendo um menos a razão entre o custo total para este sistema, com autômato de N células, ao longo do intervalo de tempo de 0 a T, e o custo total para o sistema *SIR*, sem alerta, nas mesmas condições. Assim, podemos escrever:

$$Er(T) = 1 - \frac{\mathrm{C_{SASIR}}(T)}{\mathrm{C_{SIR}}(T)} \quad (1)$$

Onde $\mathrm{C_{SIR}}(T)>0$.

Os gráficos de $\mathrm{C_{SASIR}}(T)$ e $\mathrm{C_{SIR}}(T)$ serão determinados ao longo do tempo, através da soma dos custos dos estados das máquinas a cada instante, isto é, $\sum_{t=0}^{T}\sum_{i=1}^{N} c\left(s_i(t)\right)$, para os modelo *SASIR* e *SIR*, respectivamente. A diferença do modelo *SIR* para o *SASIR* é que no primeiro, $\varepsilon_1=0$, que torna nula a probabilidade do *suscetível* entrar em *alerta*, deixando o modelo com apenas três estados: *suscetível*, *infectado* e *recuperado*.

A eficiência relativa positiva, $Er(T)>0$, indica que o uso do modelo *SASIR* é economicamente viável em determinado instante de tempo, e significa que o uso do modelo *SASIR*, é capaz de reduzir os custos operacionais quando comparado com o modelo *SIR* no mesmo instante.

Neste trabalho, por simplificação, admitiremos $c(S) = 0$ e $c(R) = 0$. Assim, podemos reescrever $Er(T)$ como:

$$Er(T) = 1 - \frac{\mathrm{N}^{\mathrm{A}}_{\mathrm{SASIR}}(T)\cdot c(A) + \mathrm{N}^{\mathrm{I}}_{\mathrm{SASIR}}(T)\cdot c(I)}{\mathrm{N}^{\mathrm{I}}_{\mathrm{SIR}}(T)\cdot c(I)} \quad (2)$$

Onde, $\mathrm{N}^{\mathrm{A}}_{\mathrm{SASIR}}(T)$, $\mathrm{N}^{\mathrm{I}}_{\mathrm{SASIR}}(T)$ e $\mathrm{N}^{\mathrm{I}}_{\mathrm{SIR}}(T)$ correspondem, respectivamente, ao número de células no estado *alerta* no instante *T* do modelo *SASIR*, ao número de células no estado *infectado* no instante *T* do modelo *SASIR* e ao número de células *infectadas* no instante *T* do modelo *SIR*. Assim, a equação (2) pode ser reescrita da seguinte forma:

$$Er(T) = \frac{\mathrm{N}^{\mathrm{I}}_{\mathrm{SIR}}(T)\cdot c(I) - \mathrm{N}^{\mathrm{A}}_{\mathrm{SASIR}}(T)\cdot c(A) - \mathrm{N}^{\mathrm{I}}_{\mathrm{SASIR}}(T)\cdot c(I)}{\mathrm{N}^{\mathrm{I}}_{\mathrm{SIR}}(T)\cdot c(I)} \Leftrightarrow$$

$$Er(T) = \frac{[\mathrm{N}^{\mathrm{I}}_{\mathrm{SIR}}(T) - \mathrm{N}^{\mathrm{I}}_{\mathrm{SASIR}}(T)] - \mathrm{N}^{\mathrm{A}}_{\mathrm{SASIR}}(T)\cdot \eta}{\mathrm{N}^{\mathrm{I}}_{\mathrm{SIR}}(T)} \quad (3)$$

Onde, $\eta = \frac{c(A)}{c(I)}$ corresponde à razão entre os custos dos estados *alerta* e *infectado*.

3.2.3 Consideração sobre o modelo SASIR com ε1=0 e o limiar da epidemia

Tomando o modelo *SASIR* com ε_1=0, temos o equivalente ao modelo *SIR*. Para este modelo, adotamos a probabilidade de o *suscetível* ser contaminado pelo vizinho *infectado* como sendo igual a β, e a probabilidade do *infectado* ser *recuperado* como sendo γ, e supomos que todos os oito vizinhos de cada *infectado* são *suscetíveis* e que estão na vizinhança de apenas um vizinho *infectado*. A Figura 8 ilustra esta condição, na qual cada suscetível possui no máximo um vizinho *infectado*.

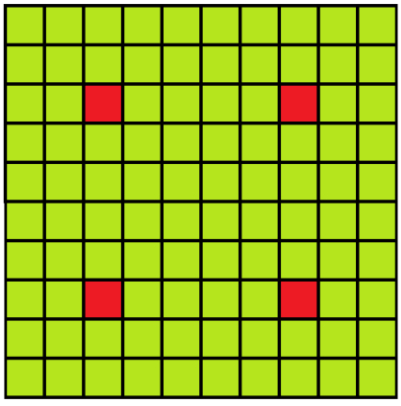


Figura 8- Disposição de células infectadas, em vermelho, onde cada célula suscetível, em verde, possui no máximo um vizinho infectado

Neste caso, podemos escrever a derivada do número de *infectados* em função do tempo como:

$$\frac{\mathrm{dI(t)}}{\mathrm{dt}} = \sum_{i=1}^{S(t)} \beta_i\,(\mathrm{t}) - \gamma \cdot \mathrm{I(t)} \quad (4)$$

Onde β_i(t) é a probabilidade de célula *suscetível i* ser contaminada no instante *t*, *S*(*t*) é o número de *suscetíveis* em *t* e *I*(*t*) é o número de *infectados* no instante *t*. Mas, apenas as oito células *suscetíveis* vizinhas de cada *infectado* têm probabilidade β>0 de serem contaminadas. Reescrevendo a equação (4), temos:

$$\frac{\mathrm{dI(t)}}{\mathrm{dt}} = \mathrm{I(t)} \cdot (8 \cdot \beta - \gamma) \quad (5)$$

A cada novo *infectado* que for inserido na rede, de tal modo que todos os seus oito vizinhos *suscetíveis* não tenham mais de um vizinho *infectado*, fará com que a derivada de infectados pelo tempo $\frac{\mathrm{dI(t)}}{\mathrm{dt}}$ varie Δ_{max} dada por:

$$\Delta_{max} = 8 \cdot \beta - \gamma \quad (6)$$

Logo, após a inclusão do infectado, a derivada $\frac{\mathrm{dI(t)}}{\mathrm{dt}}$ terá o seu novo valor dado por:

$$\frac{dI(t+1)}{dt} = [I(t) + 1] \cdot (8 \cdot \beta - \gamma) \quad (7)$$

Mas, I(t+1) = I(t)+1, logo, a equação (7) equivale a:

$$\frac{dI(t+1)}{dt} = I(t+1) \cdot (8 \cdot \beta - \gamma) \quad (8)$$

Chamando o instante *t*+1 de *u* podemos reescrever (8) como:

$$\frac{dI(u)}{dt} = I(u) \cdot (8 \cdot \beta - \gamma) \quad (9)$$

E, portanto, a inclusão de novos *infectados*, cujos seus oito vizinhos *suscetíveis* não tenham mais de um vizinho *infectado* não altera a equação de $\frac{\mathrm{dI(t)}}{\mathrm{dt}}$

$$\Delta = \sum_{i=1}^{8} x_i \cdot a_i - b - \gamma \quad (10)$$

Onde, x_i é a quantidade de vizinhos da célula *c*, que têm *i* vizinhos *infectados*, e a_i e *b* são os coeficientes abaixo:

$$a_i = \left[1 - (1-\beta)^i\right] - \left[1 - (1-\beta)^{i-1}\right] \quad (11)$$

$$b = 1 - (1-\beta)^j \quad (12)$$

E *j* é igual ao número de vizinhos *infectados* da célula *c*.

Sendo a probabilidade de que uma célula *suscetível* com *i* vizinhos *infectados* seja contaminada igual a $1-(1-\beta)^i$, o coeficiente a_i advém do fato de que a inclusão da célula *c* faz com que os seus vizinhos *suscetíveis* ganhem um novo vizinho *infectado*, fazendo com que a probabilidade do *suscetível* ser contaminado aumente, de $1-(1-\beta)^{i-1}$ para $1-(1-\beta)^i$. E o coeficiente *b* corresponde à probabilidade que tinha a célula *suscetível* de ser contaminada antes que ela fosse substituída pela célula *c*.

Assim, por exemplo, para uma nova célula *infectada c* que é introduzida na rede ilustrada na Figura 9, onde as células em vermelho representam as *infectadas* e, as em verde, as *suscetíveis*, os números nos centros das células indicam a quantidade de vizinhos *infectados* para cada um dos suscetíveis na vizinhança da célula *c*. Para este caso, Δ é dado por:

$$\Delta = 3 \cdot a_1 + 2 \cdot a_2 + 1 \cdot a_3 - b - \gamma$$

E, $b=1-(1-\beta)^j$, onde *j*=1 pois a célula *c* possui apenas um vizinho *infectado*.

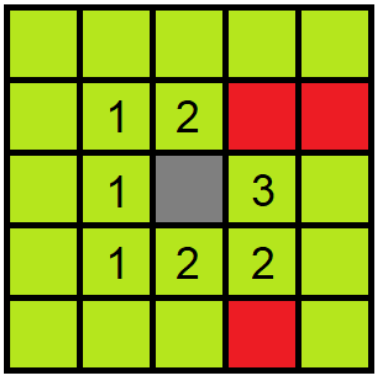


Figura 9- Exemplo mostrando o número vizinhos contaminados de cada uma das células suscetíveis vizinhas da célula infectada (em cinza) que é inserida na rede, onde há três infectados (em vermelho) e 21 suscetíveis (em verde)

Mas, desenvolvendo o coeficiente a_i dado pela equação (11) temos:

$$a_i = \left[1 - (1-\beta)^i\right] - 1 + (1-\beta)^{i-1} \quad (13)$$

Fazendo i-1=u e substituindo em (13), temos:

$$\mathrm{a_i} = [1 - (1-\beta)^{u+1}] - 1 + (1-\beta)^u \Leftrightarrow a_i = -(1-\beta)^{u+1} + (1-\beta)^u \Leftrightarrow$$

$$\Leftrightarrow \mathrm{a_i} = (1-\beta)^{\mathrm{u}} \cdot [1 - (1-\beta)] \Leftrightarrow$$

$$\Leftrightarrow \mathrm{a_i} = (1-\beta)^{\mathrm{u}} \cdot \beta \quad (14)$$

Como $0 \leq \beta \leq 1$ e $0 \leq u \leq 7$, então $(1-\beta)^{\mathrm{u}} \leq 1$ e portanto $(1-\beta)^{\mathrm{u}} \cdot \beta \leq \beta$, logo a equação (14) implica que $a_i \leq \beta$.

Assim, podemos escrever que o valor de Δ, dado pela equação (10) atende à seguinte inequação:

$$\Delta = \sum_{i=1}^{8} x_i \cdot a_i - b - \gamma \leq 8 \cdot \beta - b - \gamma \quad (15)$$

Sabemos, da equação (12), que o valor mínimo de b é igual a zero, e que este ocorre quando o número de vizinhos j da célula c é igual a zero. Assim, podemos escrever:

$$\Delta \leq 8 \cdot \beta - \gamma \quad (16)$$

Logo, a variação da derivada de *infectados* pelo tempo (Δ) é sempre menor que Δ_{max} dada pela equação (6), isto é, $\Delta \leq \Delta_{max}$, onde Δ_{max} é aquela que corresponde à situação na qual todos os oito vizinhos *suscetíveis* de cada *infectado* inserido não têm mais de um *infectado* como vizinho. A Figura 10 ilustra esta situação, onde a célula *c infectada* (em vermelho) foi incluída na rede, as células em verde são *suscetíveis* e os números indicam a quantidade de *infectados* na vizinhança de cada *suscetível* vizinho de *c*.

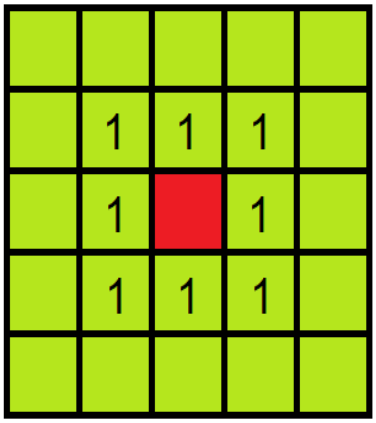


Figura 10- Situação em que a inclusão de uma nova célula c infectada (em vermelho) causa variação máxima da derivada de infectados pelo tempo (Δ_{max}), onde as células em verde são suscetíveis e os números indicam a quantidade de vizinhos infectados na vizinhança de c

Como cada novo *infectado* que é inserido na rede faz com que a derivada de *infectados* pelo tempo $\frac{dI(t)}{dt}$ varie no máximo Δ_{max}, então podemos dizer que $\frac{dI(t)}{dt}$ será sempre menor ou igual ao valor máximo, calculado na equação (9), isto é:

$$\frac{dI(t)}{dt} \leq I(t) \cdot (8 \cdot \beta - \gamma) \quad (17)$$

Mas, podemos garantir que a epidemia não ocorra se tivermos $\frac{dI(0)}{dt} \leq 0$, isto é:

$$I(t) \cdot (8 \cdot \beta - \gamma) \leq 0 \quad (18)$$

Como $I(t) \geq 0$, então a condição se torna:

$$(8 \cdot \beta - \gamma) \leq 0 \Leftrightarrow 8 \cdot \beta \leq \gamma \Leftrightarrow$$

$$\Leftrightarrow \frac{\gamma}{\beta} \geq 8 \quad (18)$$

A Figura 11 a seguir mostra a variação da população de *infectados* para diversos valores de $\frac{\gamma}{\beta}$. Estes gráficos foram obtidos através de simulações do modelo *SIR*, com a população inicial de *infectados* ($I(0)$) igual a 2% da população total. Os gráficos ilustram que quando a condição (18) é satisfeita, isto é, $\frac{\gamma}{\beta} \geq 8$ o número de *infectados* diminui continuamente ao longo do tempo e é sempre inferior ao valor inicial, enquanto que para $\frac{\gamma}{\beta} < 8$ os *infectados* aumentam, e ultrapassam o valor inicial de 2% da população.

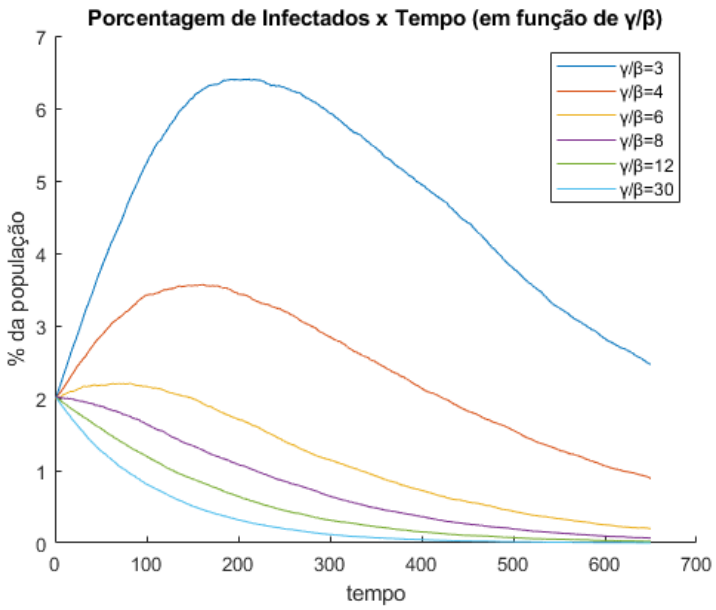


Gráfico 1 – Proporção de infectados ao longo do tempo com o modelo SIR para diferentes valores de $\frac{\gamma}{\beta}$

3.2.4 Considerações sobre o controle da epidemia pelo modelo SASIR com $\varepsilon_1 \neq 0$

Para o modelo *SASIR*, quando $\varepsilon_1 > 0$, isto é, quando a probabilidade das células suscetíveis entrarem em alerta for maior que zero, as células *suscetíveis* com vizinhos *infectados* poderão ir para o estado *alerta*, no qual as suas probabilidades de serem infectadas serão reduzidas de β_1 para $\beta_2 < \beta_1$. Quanto menor for β_2 e maiores forem ε_1 e ε_2, a probabilidade das células suscetíveis com vizinhos *infectados* entrarem em alerta, e a probabilidade das células no estado *alerta* com vizinhos *infectados* irem para o estado *alerta* no instante seguinte, respectivamente, menor será a derivada de *infectados* pelo tempo e, consequentemente a velocidade da propagação.

Assim, o surgimento das células em estado *alerta* contribui para reduzir o valor de $\frac{dI(t)}{dt}$, e consequentemente diminuir a inclinação da curva de *infectados* pelo tempo. No caso particular onde $\varepsilon_1 = 0$, quando as células *infectadas* tinham na vizinhança células *suscetíveis* com apenas um vizinho *infectado*, foi possível determinar de forma relativamente simples, e de maneira algébrica as condições nas quais $\frac{dI(t)}{dt} \leq 0$. Quando $\varepsilon_1 > 0$, a determinação para quaisquer valores

de ε_1, ε_2, β_1, β_2, γ e com distribuição espacial arbitrária das células na rede, torna-se um problema, envolvendo cálculos de probabilidades para múltiplas combinações, demasiado trabalhoso para ser resolvido algebricamente.

Uma das vantagens dos modelos epidemiológicos espaço-temporais é conseguir descrever de forma concisa as dinâmicas de sistemas, tais como o *SASIR*, cujas representações matemáticas não podem ser obtidas sem considerável esforço algébrico. Para estes casos, os seus desempenhos podem ser retratados através de simulações computacionais, para diversas condições iniciais e com diferentes parâmetros de operação. No capítulo seguinte serão apresentados resultados de simulações, sob condições iniciais e com parâmetros convenientemente escolhidos, para demonstrar a eficácia do modelo na contenção da epidemia.

4 SIMULAÇÃO DO MODELO ***SASIR*** E RESULTADOS

A seguir, são apresentados resultados de simulações computacionais com o modelo de autômato celular *SASIR*. As simulações foram realizadas em ambiente MATLAB, no espaço bidimensional de 30x30 células e os resultados foram calculados através da média de 90 simulações.

Para quatro casos, com diferentes parâmetros do modelo, são apresentadas e discutidas as curvas a seguir:

- População de infectados pelo tempo, para diversos valores de ε_1;
- População de infectados pelo tempo, quando $\gamma=0$ e para diversos valores de ε_1;
- Eficiência relativa pelo tempo, para diferentes valores de η e de ε_1;

4.1 Dinâmica do modelo ***SASIR*** em função do parâmetro ε_1

O parâmetro ε_1 determina a probabilidade da célula *suscetível* entrar em *alerta* quando tiver um vizinho *infectado*, sendo $0 \leq \varepsilon_1 \leq 1-\beta_1$. No valor extremo inferior, isto é, para $\varepsilon_1 = 0$, as células nunca entram no estado *alerta*, assim a infecção se propaga livremente e o modelo se comporta de maneira equivalente ao *SIR*. No extremo superior, quando $\varepsilon_1 = 1-\beta_1$, a chance das células suscetíveis com vizinhos *infectados* irem para o estado *alerta* é máxima.

A seguir são apresentados resultados das simulações computacionais, usando diversos valores para o parâmetro ε_1, para determinar a sua influência sobre o desempenho do modelo:

Caso 1) Para $\beta_1 = 0{,}04$; $\beta_2 = 0{,}005$; $\gamma = 0{,}02$; $\varepsilon_2 = 0{,}96$

A curva de proporção da população *infectada* ao longo do tempo, para diversos valores de ε_1 {0; 0,0005; 0,001; 0,002; 0,003; 0,004; 0,005; 0,01; 0,025; 0,05; 0,10; 0,96} é apresentada no Gráfico 2.

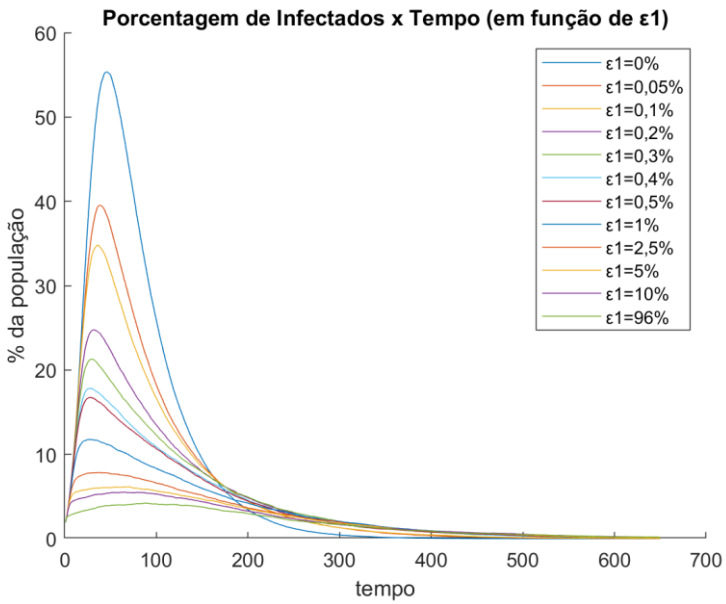


Gráfico 2 - Percentagem de infectados para o caso 1 ao longo do tempo, em função de ε_1

Através do Gráfico 2, observa-se que o número de células *infectadas* diminui à medida que ε_1 aumenta. Entretanto, as reduções são proporcionalmente mais significativas para valores menores de ε_1 e tendem a diminuir para valore maiores de ε_1. Assim, por exemplo, o pico máximo de *infectados* diminui de mais de 55% para um pouco abaixo de 40% quando ε_1 vai de zero para 0,0005, mas reduz apenas para cerca de 34,8% quando ε_1 dobra de valor, e vai para 0,001. Quando ε_1 assume o maior valor possível, isto é, 0,96, a redução do número de *infectados* é máxima, e o pico da curva atinge 4,2%.

O Gráfico 3 ilustra a dinâmica da população suscetível ao ataque cibernético, que inclui as células nos estados *suscetível* e *alerta*, em função de ε_1. Através dos gráficos é possível observar que o modelo *SASIR* é capaz de mitigar o ataque, que seria capaz de infectar todas as células da rede dentro de cerca de 100 passos de tempo. O modelo, com disparo de células de alerta, preserva parte da população do ataque cibernético, impedindo que estas máquinas sejam atingidas. A proporção das máquinas que permanecem incorruptas aumenta com o valor do parâmetro ε_1.

A dinâmica do modelo *SASIR* admite duas possíveis situações de equilíbrio, que representam os possíveis estados do sistema em regime estacionário:

- Equilíbrio, onde todas as células foram infectadas e mudaram para o estado recuperado;

- Equilíbrio no qual parte das máquinas foi contaminada, tornando-se *recuperadas*, não podendo ser contaminadas novamente ou infectar outras, e parte, que não foi contaminada, permanecerá indefinidamente no estado *suscetível*.

Este caso apresenta uma mudança do estado de equilíbrio, na qual a epidemia, que iria terminar com todas as máquinas contaminadas se não houvesse células *alertas* (ε_1=0), pode ser contida pelo modelo de alerta *SASIR*, preservando a integridade de parte das máquinas da rede.

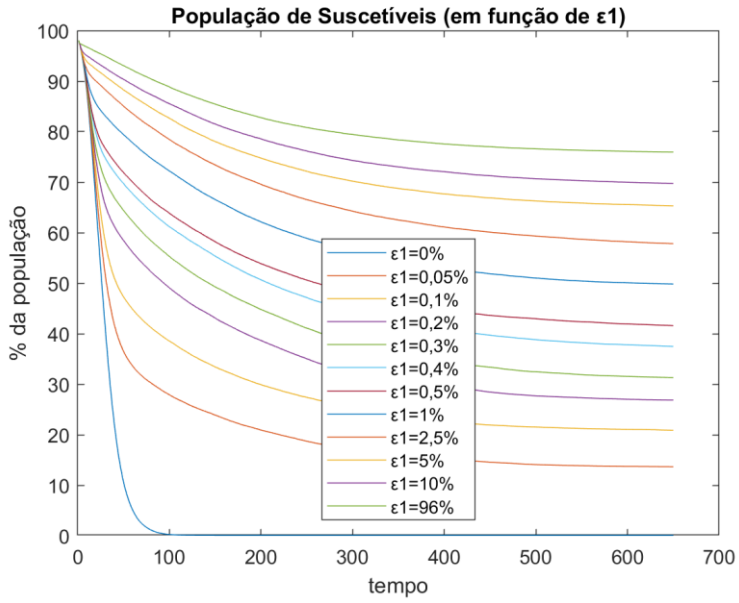


Gráfico 3 - População suscetível (células no estado *suscetível* e *alerta*) ao longo do tempo, em função de ε_1

Fazendo $\gamma = 0$ e mantendo os demais parâmetros constantes, a probabilidade da célula *infectada* ser *recuperada* é nula e, assim, as células, uma vez *infectadas* permanecerão neste estado indefinidamente. O Gráfico 4 apresenta os gráficos da proporção da população *infectada* ao longo do tempo, para diversos valores de ε_1. Os gráficos representam a proporção cumulativa de *infectados*, e neles é possível observar que o aumento de ε_1 retarda a propagação da infecção.

A situação na qual a taxa de recuperação (γ) é nula representa um possível cenário no qual o malware se espalha pela rede, contaminando todas as máquinas vulneráveis, sem que os sistemas tenham condições ou tempo hábil para serem restaurados.

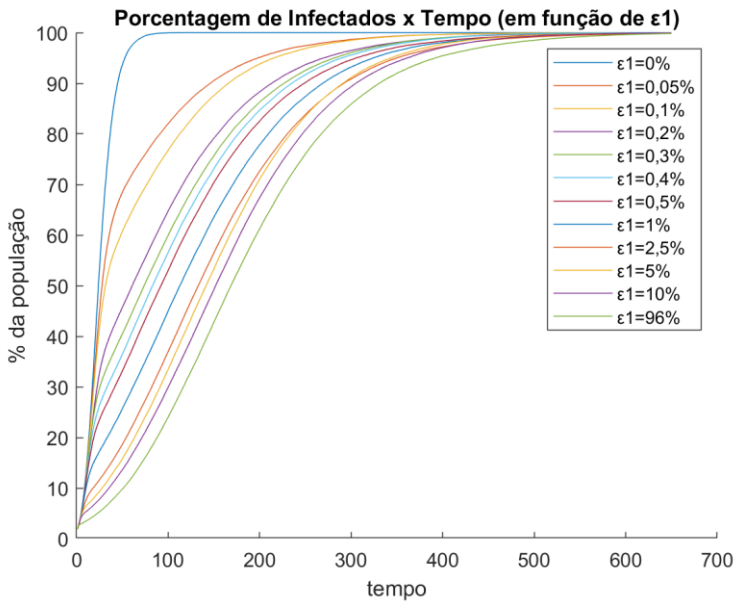


Gráfico 4 - Infectados ao longo do tempo, em função de ε_1, quando γ=0

Os gráficos 5 (a), (b), (c), (d), (e) e (f) apresentam os gráficos da eficiência relativa em função do tempo, para diversos valores de ε_1, e para η = 0, 0,1, 0,25, 0,5, 1 e 2, respectivamente. A eficiência relativa (Er), segundo a equação (3), diminui com o aumento de η, parâmetro que representa a razão entre os custos dos estados *alerta* e *infectado*. O aumento do valor deste parâmetro significa que operar no estado *alerta* fica relativamente mais oneroso.

Embora, na prática, definir a equação de custos exija conhecimentos sobre a natureza e a dinâmica dos sistemas envolvidos, a consideração sobre os custos enfatiza a necessidade de analisar a viabilidade operacional do modelo, e calcular os benefícios obtidos por esta estratégia de disparos de alerta.

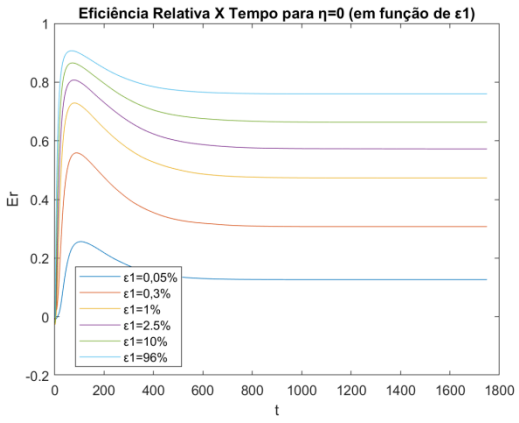
A eficiência relativa Er(t) determina a relação entre os custos da operação dos modelos *SASIR* e *SIR*. Assim, quando Er(t) é menor que zero em determinado instante, por exemplo, significa que os custos acarretados pelo modelo *SASIR*, do instante inicial até aquele momento, seriam maiores que os do modelo *SIR*, sob condições iguais e ao longo do mesmo intervalo de tempo.

Nos Gráficos 5 (b), (c), (d), (e) e (f), é possível observar que a eficiência relativa assume valores negativos para instantes de tempo t próximos a zero, e com amplitudes que aumentam com o valor de η. Em instantes de tempo próximos à origem, a eficiência relativa é menor que

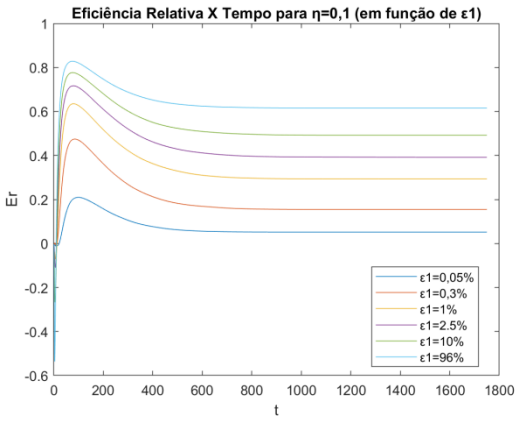
zero em função dos custos acarretados pelo surgimento das células em *alerta*, aliado à pequena redução do número de *infectados* até aquele instante.

Há curvas que atingiram valores abaixo de zero no início, mas que subiram para valores positivos ao longo do tempo, indicando a transição de uma condição desvantajosa para a viabilidade econômica. Observamos que as curvas sobem rapidamente até o valor máximo, para, em seguida, diminuir.

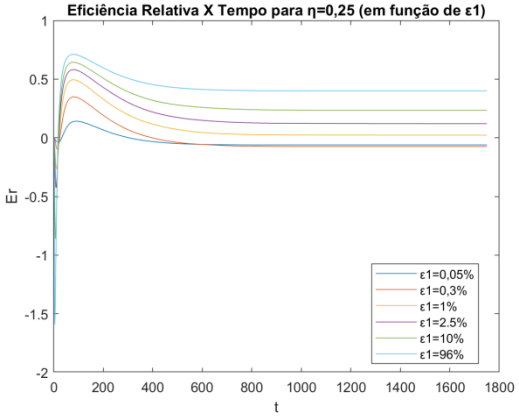
Conforme a equação (3), o valor da eficiência relativa (*Er*) maior que zero em regime permanente, isto é, quando $t \to \infty$, e para $\eta = 0$ (Gráfico 5(a)), significa que no equilíbrio, o modelo *SASIR* reduz o número de *infectados* comparado ao desempenho do *SIR*. Quanto maior o valor de *Er* no equilíbrio, mais eficiente terá sido o modelo em reduzir os custos operacionais do sistema. Observamos, conforme esperado, que a eficiência diminui quanto maior for a razão entre os custos operacionais das células *alerta* e *infectada*, representada por η, em virtude dos custos mais elevados incorridos na ativação das células *alerta*.



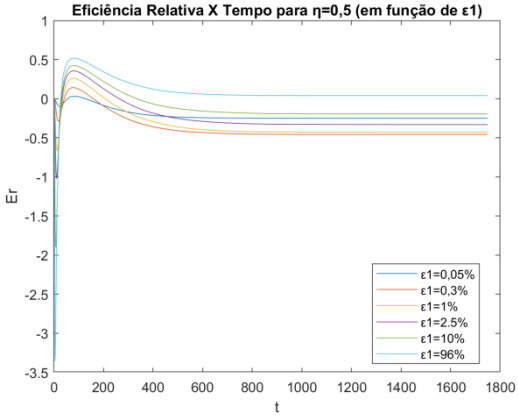
(a)



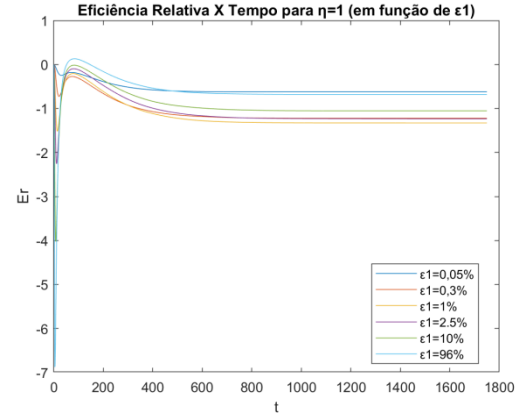
(b)



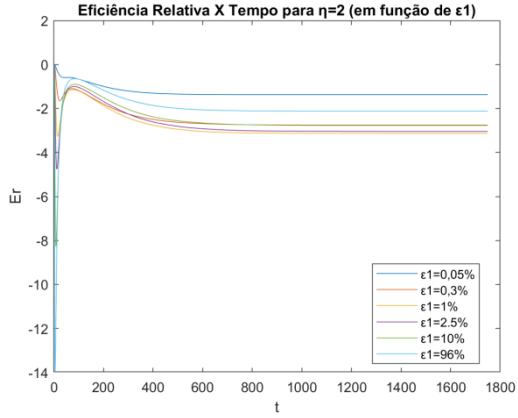
(c)



(d)



(e)



(f)

Gráfico 5 - Eficiência relativa do modelo *SASIR* em função do tempo, para diferentes valores de ε_1, para (a) η=0, (b) η=0,1, (c) η=0,25, (d) η=0,5, (e) η=1 e (f) η=2

Caso 2) Para $\beta_1 = 0{,}04$; $\beta_2 = 0{,}005$; $\gamma = 0{,}02$; $\varepsilon_2 = 0{,}48$

Este caso considera os parâmetros β_1, β_2 e γ iguais ao do anterior (*Caso 1*), mas com o valor de ε_2 igual à metade daquele. Esta diferença significa que a chance da célula em alerta permanecer neste estado quando na vizinhança de um *infectado* é igual à metade do anterior. O Gráfico 6 apresenta a porcentagem de *infectados* na população ao longo do tempo, para diferentes valores de ε_1. Observa-se pelos gráficos que, embora a redução da infecção seja menor que no caso anterior, da mesma forma que naquele, mostrado pelo Gráfico 2, as reduções são proporcionalmente mais significativas para valores menores de ε_1 e tendem a diminuir à medida que ε_1 aumenta. Além disso, o pico de *infectados* diminui de mais de 55% para cerca de 43,6% quando ε_1 aumenta de zero para 0,0005, mas reduz apenas para cerca de 36,4% quando ε_1 dobra de valor, e vale 0,001. Quando ε_1 assume o maior valor possível, isto é, 0,48, a redução do número de *infectados* é máxima e o seu pico é de aproximadamente 8%, que é quase o dobro daquele observado no caso anterior (4,2%) com $\varepsilon_1 = \varepsilon_2 = 0{,}96$.

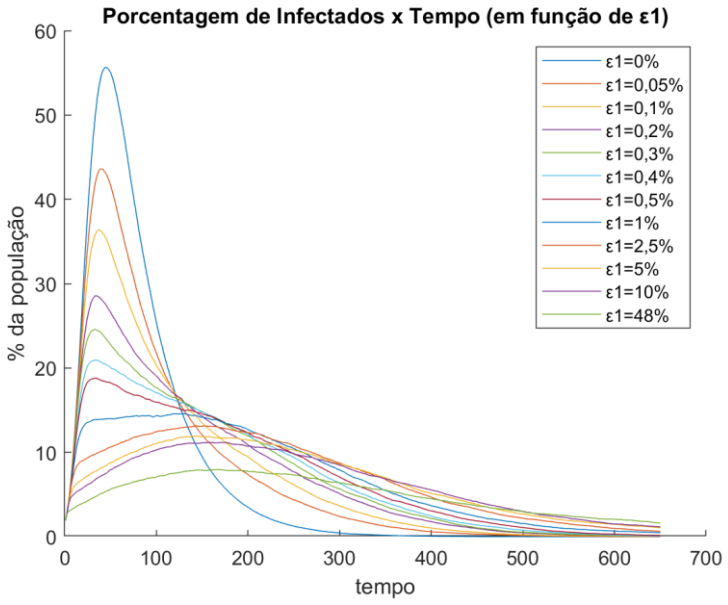


Gráfico 6 - Percentagem de infectados, para o caso 2, ao longo do tempo, em função de ε_1

O Gráfico 7 revela que, embora também neste caso, seja possível passar do estado de equilíbrio em que todas as máquinas são contaminadas (ε_1=0) para o equilíbrio onde parte das máquinas permanece *suscetível*, a proporção daquelas que não são contaminadas diminui consideravelmente, comparada com o caso anterior.

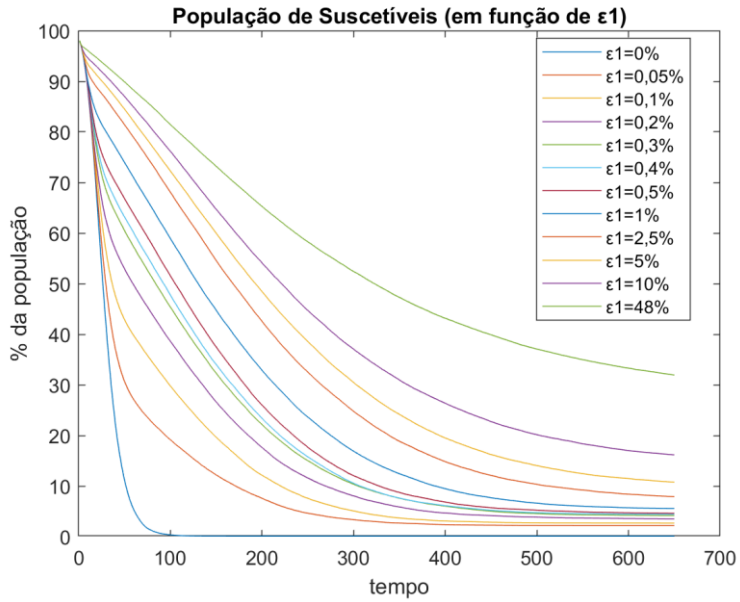


Gráfico 7 - População suscetível ao longo do tempo, em função de ε_1

O Gráfico 8 apresenta os gráficos da proporção da população *infectada* ao longo do tempo, para $\gamma = 0$ e para diversos valores de ε_1. Quando $\gamma = 0$ os *infectados* não passam para o estado *recuperado* e, por isso os gráficos representam a proporção cumulativa de *infectados*.

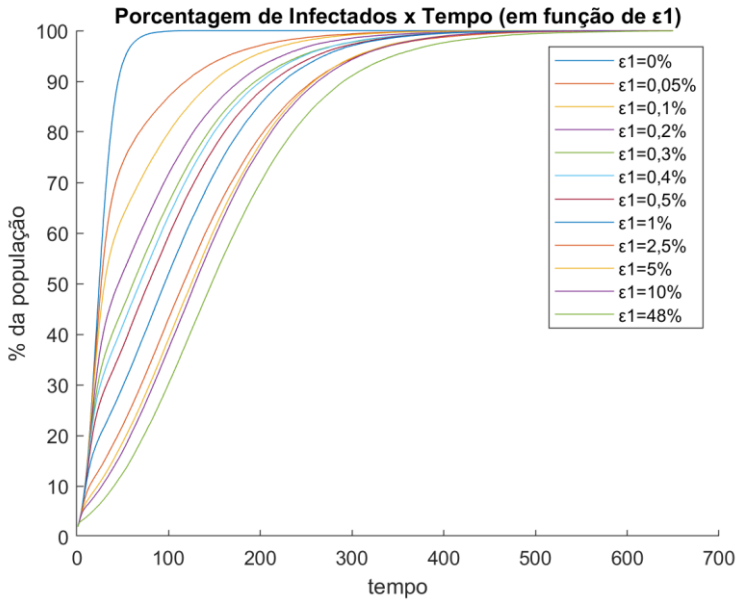
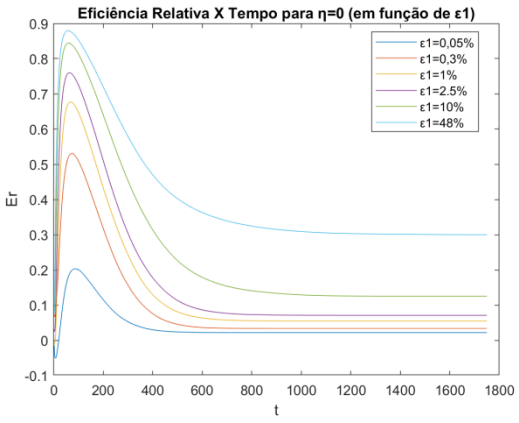
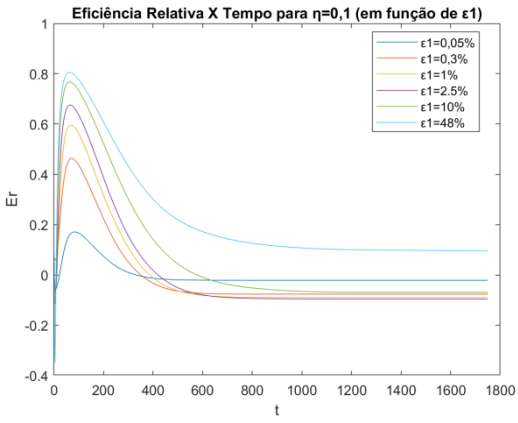


Gráfico 8 - Infectados ao longo do tempo, em função de ε_1, quando γ=0

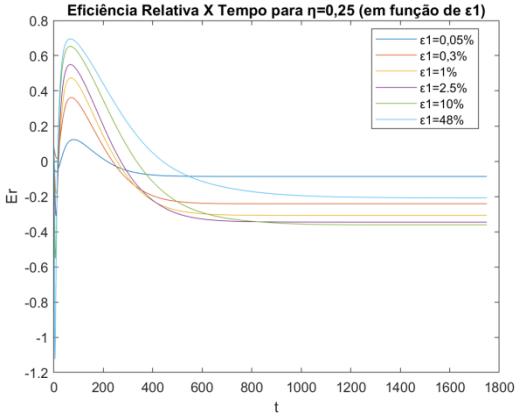
Os Gráficos 9 (a), (b), (c), (d), (e) e (f) apresentam os gráficos da eficiência relativa em função do tempo, para diversos valores de ε_1, e para η = 0, 0,1, 0,25, 0,5, 1 e 2, respectivamente. A equação (3) revela que a eficiência relativa (Er) diminui com o aumento de η, isto é, com o acréscimo do custo do estado *alerta* em relação ao *infectado*, o que acarreta custos mais altos para as células do sistema *SASIR* entrarem em *alerta*. Quando comparamos este *caso 2*, no qual ε_2 vale 0,48 com o anterior, o *caso 1*, em que ε_2 era 0,96, observa-se no segundo, para η igual a zero, que a eficiência relativa é consideravelmente maior em virtude do melhor desempenho daquele na redução do número de *infectados* e consequente preservação das células *suscetíveis*.



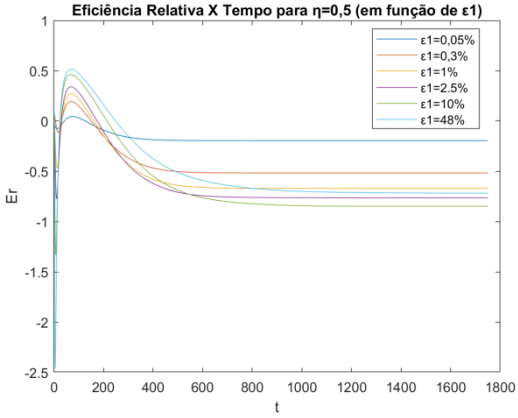
(a)



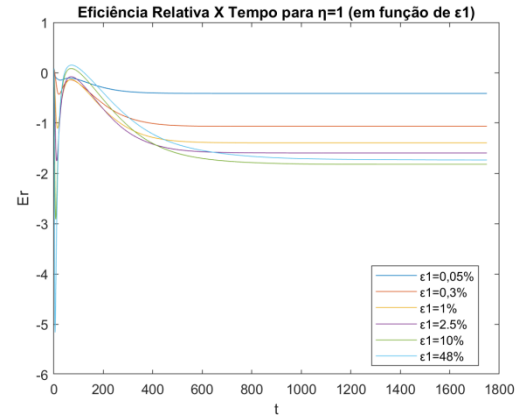
(b)



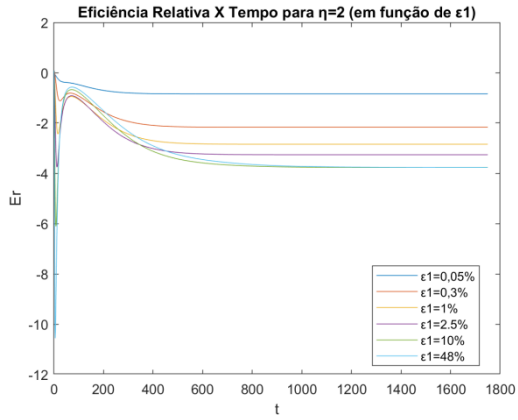
(c)



(d)



(e)



(f)

Gráfico 9 - Eficiência relativa do modelo *SASIR* em função do tempo, para diferentes valores de ε_1, para (a) η=0, (b) η=0,1, (c) η=0,25, (d) η=0,5, (e) η=1 e (f) η=2

Caso 3) Para $\beta_1 = 0{,}04$; $\beta_2 = 0{,}005$; $\gamma = 0{,}02$; $\varepsilon_2 = 0{,}1$

Neste caso, os parâmetros β_1, β_2 e γ são os mesmos usados nos dois casos anteriores, mas o valor de ε_2 é significativamente menor, igual a 0,1, o que significa que a probabilidade da célula *alerta* permanecer neste estado quando estiver na vizinhança de uma célula *infectada* é de 10%. Uma vez que o valor de ε_1 é definido como menor ou igual a ε_2, o parâmetro ε_1, que representa a probabilidade da célula entrar em *alerta*, também será menor ou igual a 10%. Desta forma, este caso ilustra uma situação na qual o sistema possui capacidade reduzida de detectar a presença de máquinas *infectadas*.

O Gráfico 10 mostra as curvas da população de *infectados* ao longo do tempo, para diferentes valores de ε_1. Comparado aos dois casos anteriores, nos quais os picos de *infectados* foram reduzidos a cerca de 4,2% e 8% da população, neste caso, a população de *infectados* foi reduzida a um pouco abaixo de 40%.

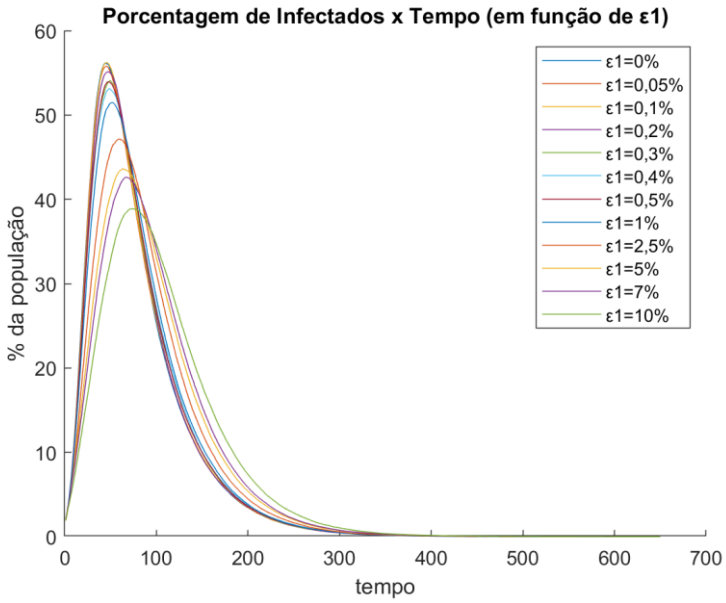


Gráfico 10 - Porcentagem de infectados para o caso 3 ao longo do tempo, em função de ε_1

Diferentemente dos dois casos anteriores, nos quais terminado o ataque cibernético, ao fim da propagação, parte da população *suscetível* permanecia preservada, enquanto neste caso, conforme ilustrado pelo Gráfico 11, a população de *suscetíveis* é praticamente eliminada ao longo do tempo.

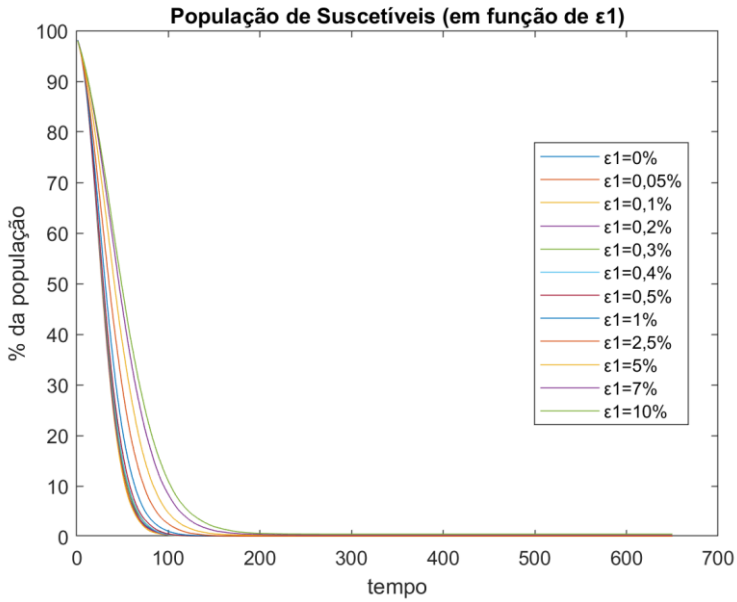


Gráfico 11 - População suscetível ao longo do tempo, em função de ε_1

O Gráfico 12 apresenta os gráficos da proporção da população *infectada* ao longo do tempo, para $\gamma = 0$ e para diversos valores de ε_1. Quando $\gamma = 0$ os *infectados* não passam para o estado *recuperado* e, por isso os gráficos representam a proporção cumulativa de *infectados*. Nos dois casos mostrados anteriormente, as curvas de *infectados*, para $\gamma = 0$, e para valores maiores de ε_1, descreviam um retardo mais significativo na propagação da epidemia, enquanto neste, conforme ilustrado no Gráfico 12, não se observa redução expressiva e as curvas estão mais próximas umas das outras.

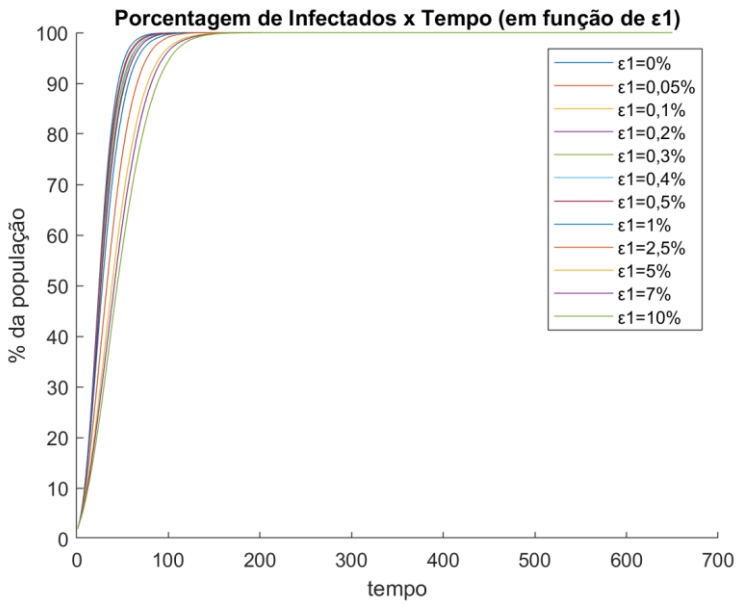
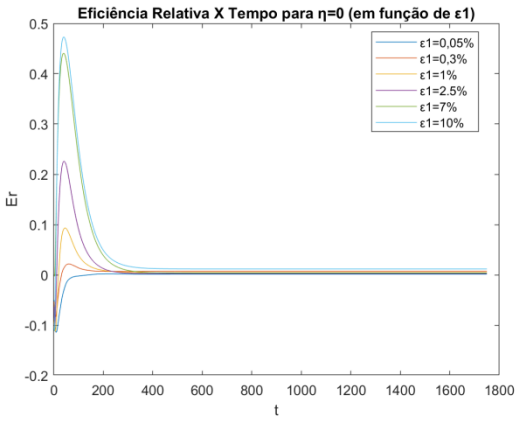
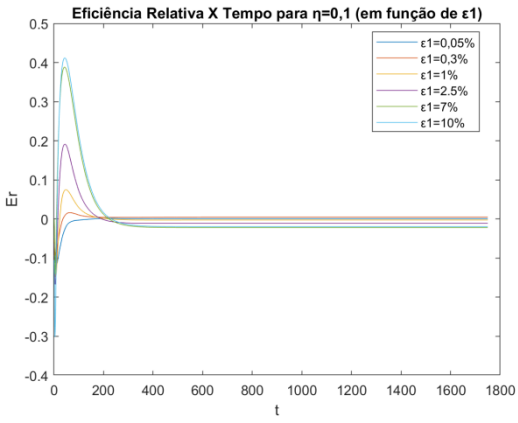


Gráfico 12 - Infectados ao longo do tempo, em função de ε_1, quando $\gamma=0$

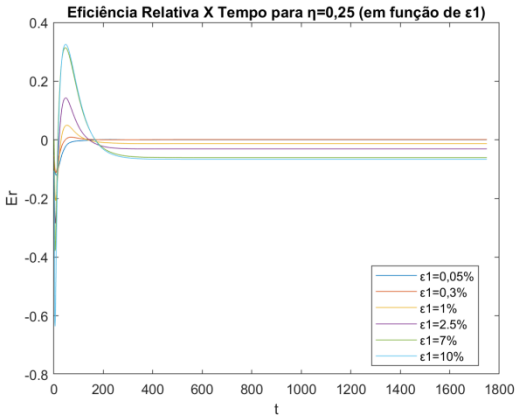
Conforme esperado, devido ao reduzido disparo de células de *alerta*, observa-se nos Gráficos 13 menor eficiência relativa em comparação com os dois casos anteriores. A diminuição da eficiência decorre da menor capacidade de mitigar a propagação e proteger as células *suscetíveis* contra o ataque.



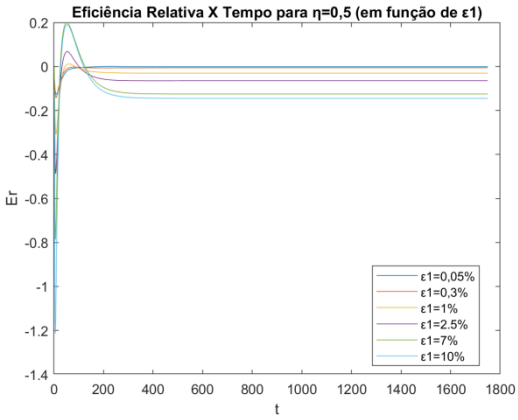
(a)



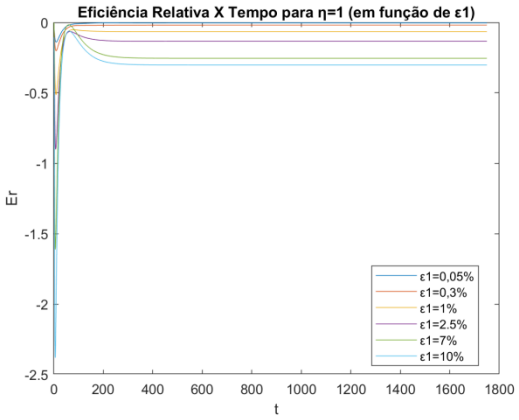
(b)



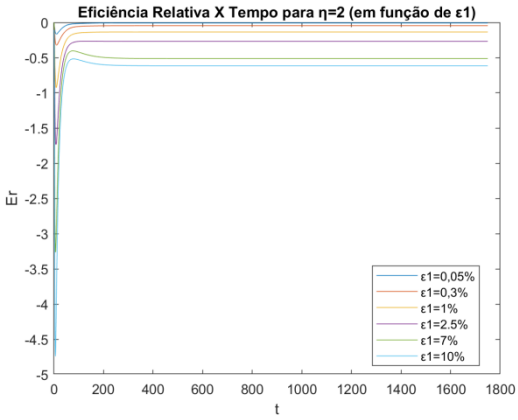
(c)



(d)



(e)



(f)

Gráfico 13 - Eficiência relativa do modelo *SASIR* em função do tempo, para diferentes valores de ε_1, para (a) η=0, (b) η=0,1, (c) η=0,25, (d) η=0,5, (e) η=1 e (f) η=2

Caso 4) Para $\beta_1 = 0{,}05$; $\beta_2 = 0{,}001$; $\gamma = 0{,}03$; $\varepsilon_2 = 0{,}95$

Este caso ilustra a situação na qual a propagação da epidemia é contida de maneira ideal, isto é, a partir do instante seguinte após as células entrarem no estado *alerta*, a curva de infectados inverte a sua tendência de subida e cai de maneira sustentada até a completa eliminação dos *infectados*.

A curva de proporção da população *infectada* ao longo do tempo, em função de ε_1 é apresentada no Gráfico 14. Com o aumento ε_1, que representa a probabilidade dos *suscetíveis* entrarem em *alerta* quando na presença de vizinhos *infectados*, o maior disparo de células em *alerta* fará com que diminua o número de *infectados* na rede. E para ε_1 igual a 65%, a redução do número de *infectados* é máxima, e o pico chega a cerca de 3% da população.

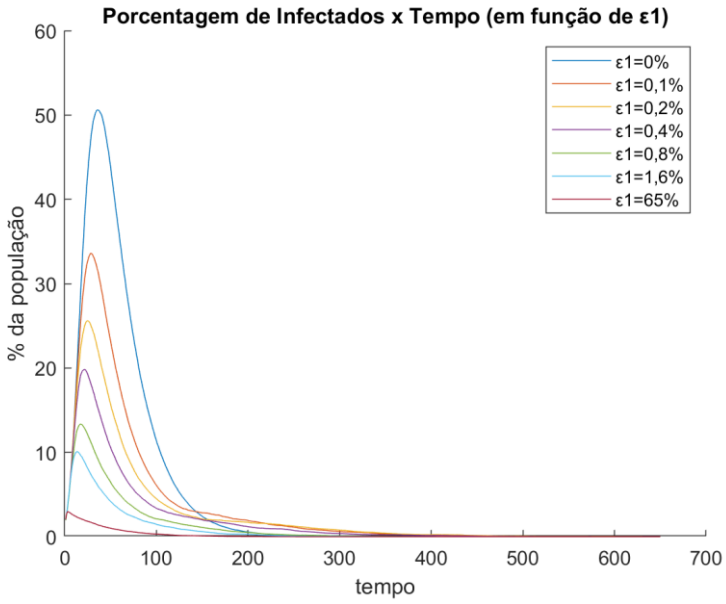


Gráfico 14 - Porcentagem de infectados ao longo do tempo para o caso 4, em função de ε_1

Calculando, $\frac{\gamma}{\beta_1} = \frac{3}{5} < 8$, sabemos que a epidemia tem condições de ser deflagrada, fato que é observado na Figura 24, sendo o aumento do número de *infectados* mais acentuado para ε_1=0, onde após apenas 35 passos de tempo, cerca de 50% da população está contaminada. Com o aumento do valor de ε_1, que representa a probabilidade de disparo das células de *alerta*, observa-se a redução da propagação e o achatamento da curva de *infectados*. A redução tem início com o aumento das células *alerta*, que aparecem no instante (t=2), e aumentam

significativamente em número no momento subsequente (t=3), quando estes fazem com que seus vizinhos *suscetíveis* também entrem em *alerta*.

Para melhor ilustrar a condição na qual o modelo é capaz de suprimir a propagação, o Gráfico 15 destaca os dez primeiros instantes de tempo da curva de *infectados*, para o caso em que ε_1=65% e a mitigação da propagação é máxima, sendo que o pico de *infectados* atinge cerca de 3% da população. Na figura é possível observar que a inclinação da curva diminui ligeiramente a partir do instante t=2, quando algumas células entram no estado *alerta*, e inverte completamente sua tendência, passando de surto de contaminados para queda sustentada, no instante t=3, quando estas células recrutam os seus vizinhos para o estado *alerta*.

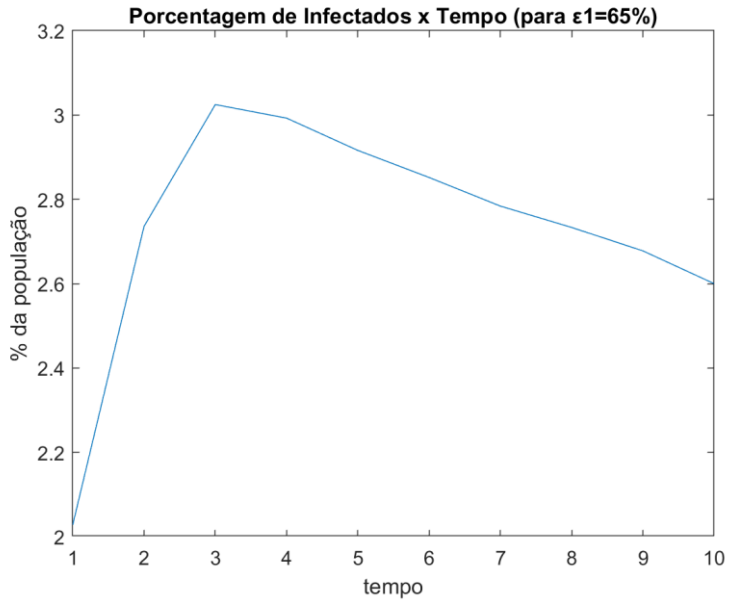


Gráfico 15 - Curva de infectados, para ε_1=65%, com destaque para a inversão da tendência de subida a partir do instante t=3, devido ao aumento significativo das células em *alerta*

Além disso, conforme ilustrado no Gráfico 16, com o aumento de ε_1, mais células são preservadas do ataque e maior é a população que permanece *suscetível* ao término da propagação. No caso em que ε_1=65%, por exemplo, mais de 96% da população vulnerável é protegida da infecção.

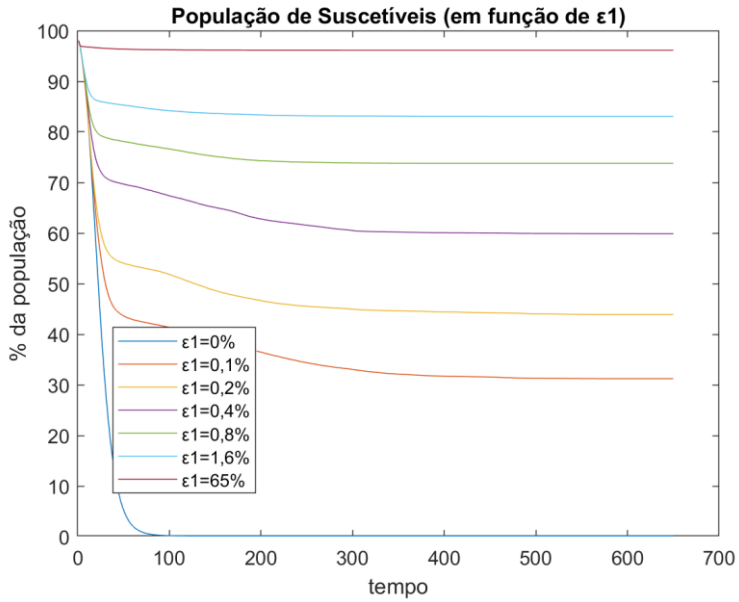


Gráfico 16 - População suscetível ao longo do tempo, em função de ε_1

O Gráfico 17 apresenta os gráficos da população de *infectados* ao longo do tempo, para $\gamma=0$ e para diversos valores de ε_1. Quando $\gamma=0$, os *infectados* não passam para o estado *recuperado* e, deste modo, os gráficos representam a proporção cumulativa de *infectados*. Nesta figura é possível observar que, sem o recrutamento das células de alerta, para $\varepsilon_1=0$, o número de *infectados* aumenta muito rapidamente, atingindo cerca de 100% da população após 70 passos de tempo. Quando $\varepsilon_1=65\%$, após um período dez vezes mais longo, de 700 passos de tempo, o número de *infectados* é de apenas cerca de 43% da população total.

A situação em que a taxa de recuperação (γ) é nula é interessante porque representa um possível cenário no qual o malware se espalha pela rede, contaminando todas as máquinas vulneráveis, sem que haja condições ou tempo hábil para os sistemas serem restabelecidos. Além disso, o presente caso é diferente dos três anteriores, conforme representado no Gráfico 17, porque neste as células *alertas* conseguem alterar significativamente e tornar mais linear a inclinação das curvas de *infectados*. As inclinações das curvas sofrem alterações mais pronunciadas quanto maior for a razão entre β_1 e β_2, uma vez que na passagem do estado *suscetível* para o *alerta* a tendência de aumento de *infectados* muda com a taxa de propagação que vai de β_1 para β_2.

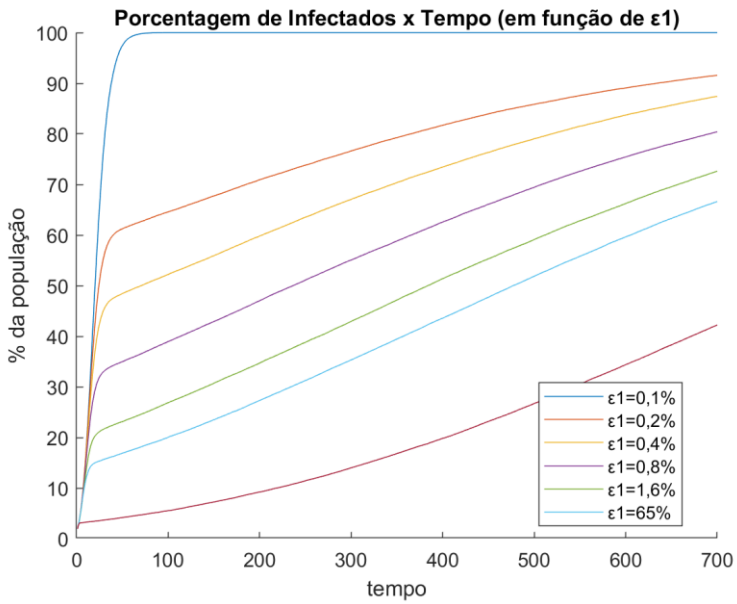
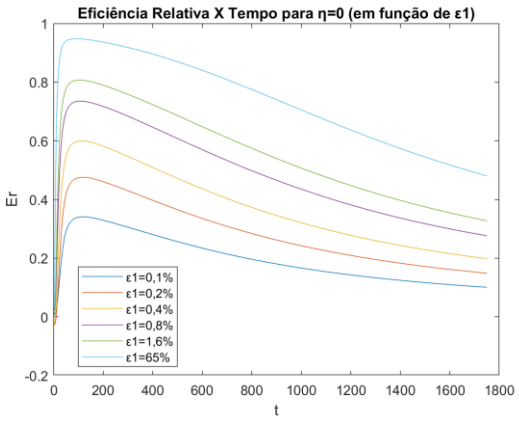


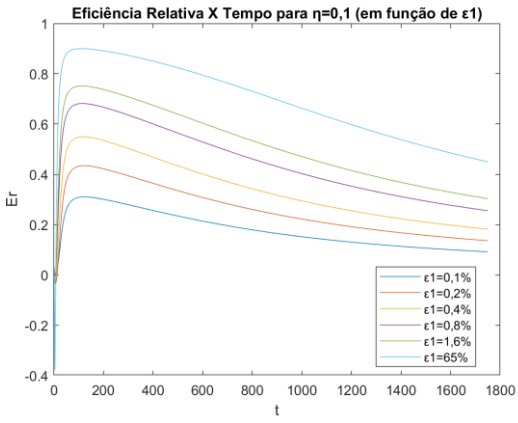
Gráfico 17 - Infectados ao longo do tempo, em função de ε_1, quando γ=0

Nos Gráficos 18 (b), (c), (d), (e) e (f), é possível observar que a eficiência relativa assume valores negativos para instantes de tempo *t* próximos a zero, e com amplitudes que aumentam com o valor de η. Nestes instantes próximos à origem, a eficiência relativa é menor que zero em função dos custos acarretados pelas células em *alerta*, aliados à pequena redução do número de *infectados* até aquele instante.

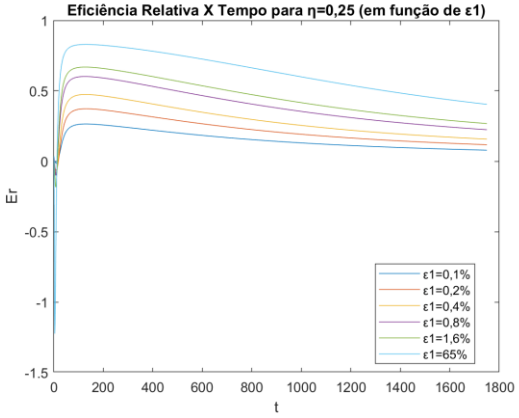
O Gráfico 18(f) mostra, por exemplo, que, embora seja possível mitigar significativamente a propagação, a eficiência relativa pode tornar-se menor que zero caso os custos operacionais do estado *alerta* sejam relativamente altos.



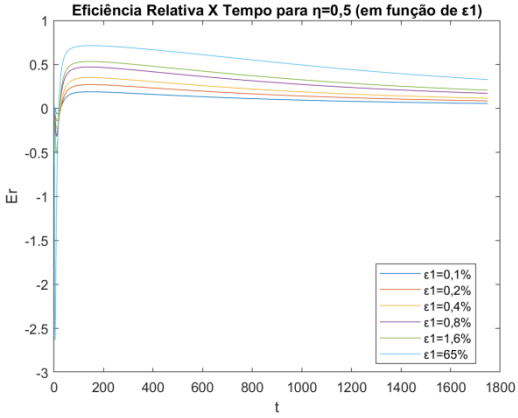
(a)



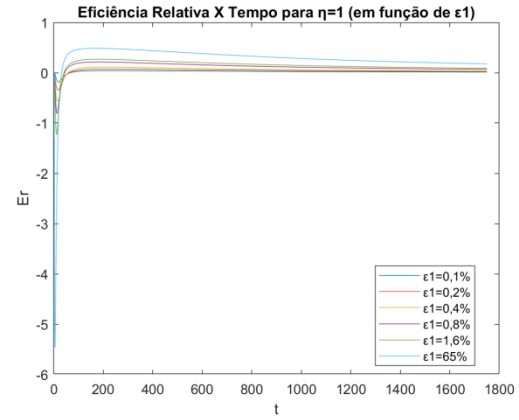
(b)



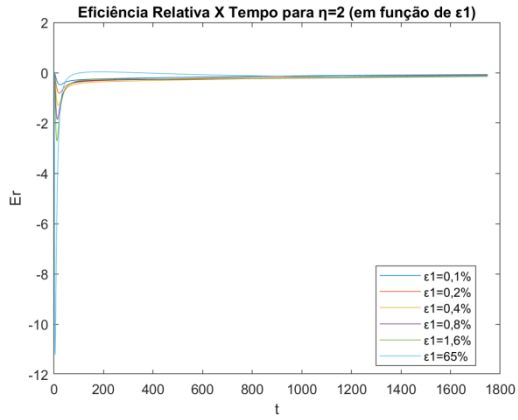
(c)



(d)



(e)



(f)

Gráfico 18 - Eficiência relativa do modelo *SASIR* em função do tempo, para diferentes valores de ε_1, para (a) η=0, (b) η=0,1, (c) η=0,25, (d) η=0,5, (e) η=1 e (f) η=2

5 CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS

Nos últimos anos, o amplo progresso tecnológico, ilustrado pelo aperfeiçoamento e amplo uso das redes de comunicação, da robótica, digitalização e Internet das coisas, lançou a indústria em direção ao novo estágio de evolução, onde os sistemas de tecnologia da informação são protagonistas, proporcionando redução de custos, melhorias de produtividade, desempenho e integração. Conforme o cenário evolui para a interconexão dos sistemas distribuídos, as vulnerabilidades e riscos de ataques cibernéticos se intensificam.

Para responder a estes desafios, a segurança da informação deve acompanhar o progresso tecnológico, proporcionando estratégias e inovações que harmonizem as necessidades dos usuários com padrões satisfatórios de confiabilidade e segurança. Desejando contribuir com o estado da arte sobre segurança cibernética, este trabalho apresenta o modelo epidemiológico espaço-temporal *SASIR* (Susceptível-Alerta-Susceptível-Infectado-Recuperado). A descrição deste modelo, através da plataforma espaço-temporal, é particularmente oportuna porque evidencia a natureza espacial envolvida na dinâmica do mecanismo de contenção e na estratégia de alerta do modelo.

Uma das vantagens dos modelos epidemiológicos espaço-temporais é conseguir descrever de forma concisa as dinâmicas de sistemas, tais como o *SASIR*, cujas representações matemáticas exigem considerável esforço algébrico, uma vez que envolvem cálculos de probabilidades para múltiplas combinações espaciais. Nestes casos, os seus desempenhos podem ser retratados através de simulações computacionais, para diversas condições iniciais e com diferentes parâmetros de operação.

Este trabalho, embora não tenha realizado simulações exaustivas, analisou diferentes parâmetros de funcionamento e distintos cenários de ataques. E demonstrou a capacidade do modelo para conter a propagação, particularmente quando as células no estado *alerta* exibem risco de contaminação significativamente menor que as *suscetíveis*, condição na qual a curva de *infectados*, logo após dois passos de tempo, inverte sua tendência de subida, passando de surto de contaminados para queda sustentada. Para o caso observado, por exemplo, mais de 96% da população vulnerável foi preservada do ataque.

A robustez do modelo foi evidenciada quando, sob situações menos favoráveis, com os parâmetros mais distantes da condição ideal, ainda foi possível achatar a curva de *infectados* e

preservar parte das células vulneráveis do ataque cibernético. As simulações também demonstraram que quando o risco de contaminação das células no estado *alerta* (β_2) não for significativamente menor que o das células *suscetíveis* (β_1), o achatamento da curva de *infectados* é moderado, mesmo quando ε_1 é máximo ($\varepsilon_1=\varepsilon_2$).

Adicionalmente, este trabalho estabelece, para $\varepsilon_1=0$, a configuração espacial na qual a derivada do número de *infectados* em função do tempo é máxima, e determina este valor. Por meio deste resultado é possível definir as condições nas quais a epidemia ocorre, isto é, o número de *infectados* tende a aumentar com o tempo.

A justificativa para o emprego do modelo epidemiológico com alerta, *SASIR*, reside no fato de que esta estratégia promove a redução dos danos causados pelo ataque cibernético. Para fazer alusão a esta redução, o texto também discorre sobre uma métrica que, sob o ponto de vista de eficiência, compara os custos operacionais acarretados pelo modelo *SASIR*, com aqueles do modelo clássico *SIR*. As curvas de eficiência também foram calculadas nas simulações e ilustram cenários nos quais os custos de operação do modelo com alerta foram mais elevados do que aqueles atingidos quando a propagação ocorria livremente, como no modelo *SIR*, revelando a importância de, no projeto do modelo, observar os custos operacionais para determinar a sua viabilidade econômica.

O modelo *SASIR*, implementado como autômato bidimensional, acomoda o comportamento de uma rede de comunicação em que a transmissão é direta entre vizinhos. Embora este paradigma represente adequadamente certas topologias, pode mostrar-se inadequado para distribuições heterogêneas. Como sugestão para trabalhos futuros, estudos mais avançados poderiam caracterizar o desempenho do modelo na contenção de ataques em redes mais complexas e que interligam extensas áreas, como as de smart cities, por exemplo.

Este trabalho apresentou um modelo de contenção, e demonstrou sua capacidade de reduzir a propagação e preservar os sistemas de um ataque cibernético. Os objetivos desta proposta atendem às necessidades contemporâneas de táticas de segurança, capazes de proteger contra ameaças que escapam dos recursos de proteção convencionais, e cujas velocidades de propagação exigem atuação imediata de sistemas automatizados. Assim, os resultados deste estudo encorajam o desenvolvimento de ferramentas, que incorporem a estratégia do modelo, como software ou hardware, para serem empregadas em sistemas computacionais reais.

REFERÊNCIAS

AHMAD, M. A.; WOODHEAD, S. Containment of fast scanning computer network worms. **Lecture Notes in Computer Science,** v. 9258, p. 235–247, 2015. doi:10.1007/978-3-319-23237-9_21

ALLEN, L. J. S. Some discrete-time si, sir, and sis epidemic models **Mathematical Biosciences,** v. 124, n. 1, p. 83–105, Nov. 1994

BARTHÉLEMY, M. et al. Velocity and hierarchical spread of epidemic outbreaks in scale-free networks **Physical review letters**. v. 92 , n. 17 , p. 178701-1 - 178701-4 2004. doi:10.1103/PhysRevLett.92.178701

BAJIYA, V. P. et al. Modeling the impacts of awareness and limited medical resources on the epidemic size of a multi-group SIR epidemic model **International Journal of Biomathematics** - v.0, n.0, p. 1-49, 12 Abril 2022 doi:10.1142/S1793524522500450

BENCSÁTH, B.; PÉK, G.; BUTTYÁN, L.; FELEGYHAZI, M. The cousins of stuxnet: Duqu, flame, and gauss. **Future Internet**, n. 4, p. 971–1003, 2012 doi:10.3390/fi4040971

CHEN, S.; TANG, Y. Slowing down internet worms. In: INTERNATIONAL CONFERENCE OF DISTRIBUTED COMPUTING SYSTEMS, IEEE, 24. **Proceedings…** Tokyo, Japan p. 312–319, 2004 doi:10.1109/ICDCS.2004.1281596

CISOTTO, F.; BADIA, L. Cyber security of smart grids modeled through epidemic models in CELLULAR AUTOMATA 2016. In: IEEE INTERNATIONAL SYMPOSIUM ON A WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS (WOWMOM), 17. **Proceedings…**, Coimbra, Portugal, p. 1-6, 2016. doi:10.1109/WoWMoM.2016.7523560

DANTU, J. C. R.; YELIMELI, A. Dynamic Control of Worm Propagation. In: CONFERENCE: INFORMATION TECHNOLOGY: CODING AND COMPUTING, 2004. v.1, 2004, **Proceedings…** doi:10.1109/ITCC.2004.1286491

ELLIS, D.R.; AIKEN, J.G.; ATTWOOD, K.S.; TENAGLIA, S.D. A Behavioral Approach to Worm Detection In: WORM '04:. ACM WORKSHOP ON RAPID MALCODE, **Proceedings…** Washington DC, USA, 2004 p. 43–53 doi:10.1145/1029618.1029625

FALLIERE, N.; MURCHU, L.O.; CHIEN, E. W32. stuxnet dossier. **White paper, Symantec Corp., Security Response**, 5, 2011.

FOSNOCK, C. **Computer worms:** past, present, and future. East Carolina University, v.8, p. 1-9, 2005

GOEL, KANICA et al. Nonlinear dynamics of a time-delayed epidemic model with two explicit aware classes, saturated incidences, and treatment **Nonlinear dynamics** v. 101, p. 1693-1715, 2020. doi:10.1007/s11071-020-05762-9

KABIR, K. M. A.; TANIMOTO, J. Vaccination strategies in a two-layer SIR/V–UA epidemic model with costly information and buzz effect **Communications in Nonlinear Science and Numerical Simulation**, v. 76, p. 92-108, 2019. doi:10.1016/j.cnsns.2019.04.007

KABIR, K. M. A.; KUGA, K.; TANIMOTO, J. Analysis of SIR epidemic model with information spreading of awareness Chaos, Solitons & Fractals, v. 119, p. 118-125, 2019 doi:10.1016/j.chaos.2018.12.017

KEPHART, J.O.; WHITE, S.R. Directed-graph epidemiological models of computer viruses In: IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, **Proceedings...** IEEE, Oakland, CA, USA, p. 343–359, 1991 doi:10.1109/RISP.1991.130801

KERMACK, W. O.; MCKENDRICK, A. G. Contributions to the mathematical theory of epidemics, part i. In: ROYAL SOCIETY OF EDINBURGH. **Proceedings...** Section A. Mathematics. p. 700–721, 1927

KERMACK, W. O.; MCKENDRICK, A. G. Contributions to the mathematical theory of epidemics, ii - the problem of endemicity. In: ROYAL SOCIETY OF EDINBURGH. **Proceedings...** Section A. Mathematics. p. 55–83, 1932

KERMACK, W. O.; MCKENDRICK, A. G. Contributions to the mathematical theory of epidemics, iii - further studies of the problem of endemicity. In: ROYAL SOCIETY OF EDINBURGH. **Proceedings...** Section A. Mathematics. p. 94–122, 1933

KIM, H.A.; KARP, B. Autograph: Toward Automated, Distributed Worm Signature Detection In: USENIX SECURITY SYMPOSIUM, 13, **Proceedings...** v. 13, San Diego,CA, 2004

KUMAR, A.; NILAM; KISHOR, R. A short study of an SIR model with inclusion of an alert class, two explicit nonlinear incidence rates and saturated treatment rate. **SeMA Journal**, v.76, p. 505–519, 2019 doi:10.1007/s40324-019-00189-8

LI, P.; SALOUR, M.; SU, X. A Survey of Internet Worm Detection and Containment. **IEEE Communications Surveys & Tutorials**, v. 10, n. 1, p. 20–35, 2008. doi:10.1109/COMST.2008.4483668

LOPEZ, M.; PEINADO, A.; ORTIZ, A. An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks **Computer Networks** v. 165 Dez, 2019 doi:10.1016/j.comnet.2019.106945

MAHBOUBI, A.; CAMTEPE, S.; MORARJI, H. A Study on Formal Methods to Generalize Heterogeneous Mobile Malware Propagation and Their Impacts **IEEE Access**, v. 5, p. 27740-27756, 2017. doi:10.1109/ACCESS.2017.2772787

MIEGHEM, P. V. The n-intertwined sis epidemic network model, **Computing**, p. 147–169, 2011. doi:10.1007/s00607-011-0155-y

MIEGHEM, P. V.; OMIC, J.; KOOIJ, R. Virus spread in networks, **IEEE/ACM Transactions on Networking**. v.17, p. 1–14, 2009

MISHRA, B. K.; PIQUEIRA, J. R. C. (org.) **Understanding Cyber Threats and Attacks** Nova Science Pub Inc, 2020

MISHRA, B. K.; PANDEY, S. K. Dynamic model of worms with vertical transmission in computer network **Applied Mathematics and Computation**, v. 217, n. 21, p. 8438-8446, 2011. doi:10.1016/j.amc.2011.03.041

MOORE, D. et al., Internet Quarantine: Requirements for Containing Self- Propagating Code In: IEEE INFOCOM 2003. TWENTY-SECOND ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES, **Proceedings...** v.3, p. 1901-1910, 2003. doi:10.1109/INFCOM.2003.1209212

MOORE, V.D. et al. Inside the Slammer Worm **IEEE Security & Privacy**, v. 1, n. 4, p. 33–39, 2003. doi:10.1109/MSECP.2003.1219056

PASTOR-SATORRAS, R.; VESPIGNANI, A. Epidemic spreading in scale-free networks, **Physical review letters**., v. 86, n. 14, p. 3200-3203, 2001. doi:10.1103/PhysRevLett.86.3200

PENG, S.; YU, S.; YANG, A. Smartphone Malware and Its Propagation Modeling: A Survey **IEEE Communications Surveys & Tutorials**, v. 16, n. 2, p. 925-941, 2014. doi:10.1109/SURV.2013.070813.00214

PIQUEIRA, J.R.C.; ARAUJO, V.O. A modified epidemiological model for computer viruses **Applied Mathematics and Compututation**. v. 213, n.2, p. 355–360, 2009. doi:10.1016/j.amc.2009.03.023

PORRAS, P.; BRIESEMEISTER, L.; SKINNER,K.; LEVITT, K.; ROWE, J.; TING, Y.C.A A Hybrid Quarantine Defense In: 2004 ACM WORKSHOP ON RAPID MALCODE, WORM 2004, **Proceedings...** Washington DC, USA, p. 73–82, 2004. doi:10.1145/1029618.1029630

PROVOS, N. A Virtual Honeypot Framework In: USENIX SECURITY SYMPOSIUM, 13, **Proceedings...** San Deigo, CA, USA, 2004

SAEED, I. A.; SELEMAT, A.; ABUAGOUB, A. M. A. A Survey on Malware and Malware Detection Systems **International Journal of Computer Aplications** v. 67, n. 16, p. 25-31, 2013

SAHNEH, F. D.; SCOGLIO, C.; MIEGHEM, P. V. Generalized Epidemic Mean-Field Model for Spreading Processes Over Multilayer Complex Networks **IEEE/ACM Transactions on Networking,** v. 21, n. 5, p. 1609-1620, 2013. doi:10.1109/TNET.2013.2239658

SINGH, S. et al. Automated Worm Fingerprinting In: CONFERENCE ON SYMPOSIUM ON OPERATING SYSTEMS DESIGN & IMPLEMENTATION (OSDI'04), 6, **Proceedings...** San Francisco, CA, USA, v. 6, p. 45–60, 2004

SONG, Y; JIANG, G-P; GU, Y Modeling malware propagation in complex networks based on cellular automata In: APCCAS 2008 - 2008 IEEE ASIA PACIFIC CONFERENCE ON CIRCUITS AND SYSTEMS, **Proceedings...** p. 259-263, 2008. doi:10.1109/APCCAS.2008.4746009

STANIFORD, S. et al. The top speed of flash worms in: PROCEEDINGS OF THE 2004 ACM WORKSHOP ON RAPID MALCODE, WORM 2004, Washington DC, USA, p. 33-42, Out 2004. doi: 10.1145/1029618.1029624

WANG, Z. et al. The impact of awareness diffusion on SIR-like epidemics in multiplex networks **Applied Mathematics and Computation**, v. 349, p. 134-147, 2019. doi:10.1016/j.amc.2018.12.045

WEAVER, D. E. N.; STANIFORD, S.; PAXSON, V. Worms vs. Perimeters — The Case for Hard-LANs In: ANNUAL IEEE SYMPOSIUM ON HIGH PERFORMANCE

INTERCONNECTS, 12, **Proceedings…**, Stanford, CA, USA, p. 70-77, 2004. doi: 10.1109/CONECT.2004.1375206

WEAVER, S. S. N.; PAXSON, V. Very Fast Containment of Scanning Worms In: USENIX SECURITY SYMPOSIUM, 13, **Proceedings...** San Diego, CA, USA p. 29-44, 2004.

WHYTE, D.; KRANAKIS, E.; OORSCHOTVAN, P.C. DNS based Detection of Scanning Worms in an Enterprise Network In: NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, NDSS 2005, **Proceedings...** San Diego, California, USA, 2005.

WHYTE, D.; OORSCHOTVAN, P.C.; KRANAKIS, E. Detecting Intra-Enterprise Scanning Worms based on Address Resolution In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC'05), 21, **Proceedings...** Tucson, AZ, USA, p. 371–380, 2005

WILLIAMSON, M.M. Throttling viruses: Restricting Propagation to Defeat Malicious Mobile Code In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 18, 2002. **Proceedings.**, Las Vegas, NV, USA, p. 61-68, doi: 10.1109/CSAC.2002.1176279

WONG, C. et al., Dynamic Quarantine of Internet Worms In: INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS, 2004, Florence, Italy, p. 73-82, doi: 10.1109/DSN.2004.1311878

YANG, M.; CHEN, G.; FU, X. A modified sis model with an infective medium on complex networks and its global stability **Physica A: Statistical Mechanics and its Applications** v. 390, n. 12, p. 2408–2413, 2011 doi: 10.1016/j.physa.2011.02.007

ZHENG, C. et al. Interplay between SIR-based disease spreading and awareness diffusion on multiplex networks **Journal of Parallel and Distributed Computing**, v. 115, p. 20-28, 2018. doi: 10.1016/j.jpdc.2018.01.001