Controle com Acionamento por Eventos Resiliente a Ataques de Negação de Serviço ⋆

Pedro H. S. Coutinho * **Iury Bessa** *,** **Márcia L. C. Peixoto** *
Paulo S. P. Pessim * **Pedro O. F. Pires** * **Reinaldo M. Palhares** ***

* *Programa de Pós-graduação em Engenharia Elétrica, Universidade Federal de Minas Gerais, Belo Horizonte, Brasil (e-mails:{phcoutinho, marciapeixoto, ppessim}@ufmg.br, pedropires.petee@gmail.com)*
** *Departamento de Eletricidade, Universidade Federal do Amazonas, Manaus, Brasil (e-mail:iurybessa@ufam.edu.br)*
*** *Departamento de Engenharia Eletrônica, Universidade Federal de Minas Gerais, Belo Horizonte, Brasil (e-mail:rpalhares@ufmg.br)*

Abstract: This paper presents an emulation-based design condition for event-triggered control systems under denial-of-service (DoS) attacks. Considering a deterministic model that constrains the duration of DoS attacks only in an average sense, the proposed condition ensures the exponential stability of the closed-loop system and provides a maximal percentage of time at which information can be lost without leading to instability. A multi-objective optimization problem is proposed to establish the relation between the reduction of transmission attempts and the tolerance to DoS attacks. The commitment between these two objectives is illustrated by means of numerical simulations, as well as the effectiveness of the proposed ETC scheme in reducing the network resources usage even in the presence of DoS attacks.

Resumo: Este trabalho apresenta uma condição de projeto baseado em emulação para sistemas de controle com acionamento por eventos sujeitos a ataques de negação de serviço (DoS). Considerando um modelo determinístico que restringe a duração de ataques DoS somente em um sentido médio, a condição proposta garante a estabilidade exponencial do sistema em malha fechada e fornece um percentual máximo de tempo que a informação pode ser perdida sem resultar em instabilidade. Um problema convexo de otimização multiobjetivo é proposto para estabelecer a relação entre a redução do número de tentativas de transmissões e a tolerância aos ataques DoS. A relação de compromisso entre esses dois objetivos é ilustrada por meio de simulações numéricas, assim como a efetividade do esquema de acionamento proposto em reduzir o uso dos recursos da rede, mesmo com a ocorrência de ataques DoS.

Keywords: Event-based control; Cyber-physical systems; Denial-of-service attacks; Convex optimization; Control under communication constraints

Palavras-chaves: Controle baseado em eventos; Sistemas ciberfísicos; Ataques de negação de serviço; Otimização convexa; Controle sujeito a restrições de comunicação

1. INTRODUÇÃO

Sistemas ciberfísicos são caracterizados pela integração e cooperação de componentes físicos e virtuais com forte presença de redes de comunicação. Nesse contexto, é usual o emprego de sistemas de controle em rede, onde as plantas, seus atuadores e sensores, e os controladores são interconectados via rede de comunicação. Existem duas questões principais a serem tratadas em sistemas de controle em rede: o gerenciamento dos recursos da rede, que são normalmente limitados e compartilhados, e a segurança, pois esses sistemas podem ser vulneráveis a ciberataques (Teixeira et al., 2015).

Em relação ao gerenciamento dos recursos da rede, destacam-se as técnicas de controle com acionamento por eventos (ETC, do inglês *Event-Triggered Control*). Em técnicas de ETC, mecanismos de acionamento por eventos (ETM, do inglês *Event-Triggered Mechanism*) são introduzidos na malha de controle para gerar uma sequência de instantes de transmissão (normalmente aperiódica) em que os dados devem ser transmitidos pela rede a fim de assegurar a estabilidade do sistema em malha fechada (Ban et al., 2020). Utilizando uma função de acionamento adequada, as transmissões são efetuadas somente quando a saída da planta diverge suficientemente do último sinal transmitido. Com isso, o ETC é capaz de reduzir o uso dos recursos da rede evitando transmissões desnecessárias, comuns em estratégias de acionamento periódico no tempo.

⋆ Este trabalho foi financiado pelo CNPq (307933/2018-0; 164692/2020-7; 141252/2021-9; 148769/2021-7), CAPES (Código de financiamento 001), pelo programa de bolsas de estudos PROPG-CAPES/FAPEAM (88887.199399/2018-00) e pelo Programa de Educação Tutorial da Engenharia Elétrica (PETEE UFMG), através do Ministério da Educação (MEC) e da Escola de Engenharia da UFMG.

Já em relação às questões de cibersegurança, há duas classes principais de ciberataques: ataques deceptivos (Ding et al., 2018) e de negação de serviço (DoS, do inglês *Denial-of-Service*) (De Persis e Tesi, 2016). A primeira é caracterizada por corromper os dados transmitidos a partir da injeção de dados falsos, enquanto que os ataques DoS são caracterizados pela interrupção/bloqueio da transmissão dos dados em certos períodos de tempo. No contexto de cibersegurança, soluções para diferentes problemas são apresentadas na literatura, tais como detecção e mitigação de ciberataques, e controle resiliente ou robusto a ciberataques. Este trabalho se concentra no ETC resiliente para sistemas de controle em rede sujeitos a ataques DoS.

Para lidar com o problema de controle sob ataques DoS, diferentes modelos são adotados para caracterizar esses ataques. De forma geral, os modelos desses ataques podem ser estocásticos ou determinísticos. Modelos estocásticos consideram que cada transmissão tem alguma probabilidade de estar sujeita a ataques. Nesses casos, o sucesso da transmissão considera que a ocorrência de ataques DoS são variáveis aleatórias cujos modelos podem ser simplesmente distribuições de Bernoulli (Cetinkaya et al., 2015; Niemoczynski et al., 2016; Guo et al., 2020; Mahmoud et al., 2020; Li et al., 2021), ou podem ser mais complexos e detalhados levando em conta parâmetros da rede, tais como potência do sinal transmitido e de ruídos (Zhang et al., 2022). De outro modo, modelos determinísticos usualmente consideram que a ocorrência dos ataques DoS se dá em pulsos de comprimentos variáveis. Nesse sentido, esses modelos impõem restrições à largura desses pulsos. A forma mais simples de fazer isso é assumir que cada pulso de ataque é limitado em comprimento (De Persis e Tesi, 2018) ou em energia (Lai et al., 2018; Rotondo et al., 2019; Wang et al., 2019) com limite conhecido, ou seja, existe um número finito de transmissões consecutivas que podem ser mal-sucedidas por conta de um ataque DoS. Além disso, é comum o uso de modelos que assumem que os ataques DoS são periódicos, cujos ciclos se dividem em fase com ataque e sem ataque (Wang et al., 2021). No entanto, modelos determinísticos mais genéricos são também propostos (De Persis e Tesi, 2016), onde o ataque DoS tem sua frequência limitada e a restrição ao comprimento DoS se aplica a todas as sequências ao invés de limitar o número de amostras consecutivas.

Com base nesses modelos, diversas abordagens de ETC resilientes a ataques DoS são propostas na literatura. Além do uso eficiente dos recursos da rede, no contexto de ataques DoS, o uso de ETC apresenta obstáculos adicionais ao atacante, visto que a predição dos instantes de transmissão se torna mais difícil (De Persis e Tesi, 2021). Dessa forma, com o uso de ETC, a taxa de transmissões perdidas devido a um ataque DoS se torna menor. Para sistemas discretos no tempo sujeitos a ataques DoS, abordagens de ETC com diferentes estruturas são propostas, tais como: estáticas (Yan et al., 2020), adaptativas (Zhao et al., 2022), e dinâmicas (Zhang et al., 2020).

O efeito da quantização em sistemas de controle em rede a tempo discreto sujeitos a ataques DoS aperiódicos com duração limitada é investigado em van Dinther et al. (2020). Para isso, uma condição de análise é apresentada para verificar a estabilidade do sistema com controlador quantizado e caracterizar a máxima duração de ataques DoS para qual a estabilidade é garantida. O mesmo problema considerando sistemas com incertezas paramétricas foi estudado por Kang e Ishii (2021). O presente trabalho também investiga a estabilidade de sistemas de controle em rede a tempo discreto sujeitos a ataques DoS aperiódicos com duração limitada, no entanto, aqui é analisado o efeito da inserção de um ETM na estabilidade e resiliência. Em particular, este trabalho apresenta uma condição baseada em emulação para o projeto de ETMs que garantam a resiliência de sistemas a tempo discreto em relação a ataques DoS. Além disso, um problema de otimização multiobjetivo é proposto para obter os parâmetros do ETM de forma a avaliar os critérios de economia da largura de banda e resiliência do sistema de ETC. Em particular, esses critérios são formulados em termos do número de transmissões e máxima duração de ataques DoS suportada pelo sistema.

O restante deste trabalho é organizado da seguinte forma: o sistema de controle em rede sujeito a ataques DoS e a formulação do problema de controle são apresentados na Seção 2; as condições de projeto por emulação do sistema de controle com acionamento por eventos que garantem a estabilidade exponencial considerando a ocorrência de ataques DoS são apresentadas na Seção 3; a Seção 4 apresenta simulações numéricas e a Seção 5 apresenta as conclusões do trabalho.

Notação: $\mathbb{Z}$ é o conjunto de números inteiros, $\mathbb{Z}^+$ é o conjunto de números inteiros não-negativos e $\mathbb{N}$ é o conjunto de números naturais. $\mathbb{R}^n$ denota o espaço Euclideano n-dimensional e $\mathbb{R}^{m\times n}$ o conjunto de matrizes reais $m \times n$. $X > 0$ ($X < 0$) denota que X é uma matriz simétrica definida positiva (negativa). A matriz identidade é denotada por I e a matriz nula por 0. A função piso é definida como $\lfloor x \rfloor \triangleq \max\{m \in \mathbb{Z} : m \leq x\}$. $\underline{\lambda}(P)$ ($\overline{\lambda}(P)$) denota o menor (maior) autovalor de P.

2. FORMULAÇÃO DO PROBLEMA

Considere a configuração do sistema de controle em rede sujeito a ataques DoS apresentada na Figura 1.

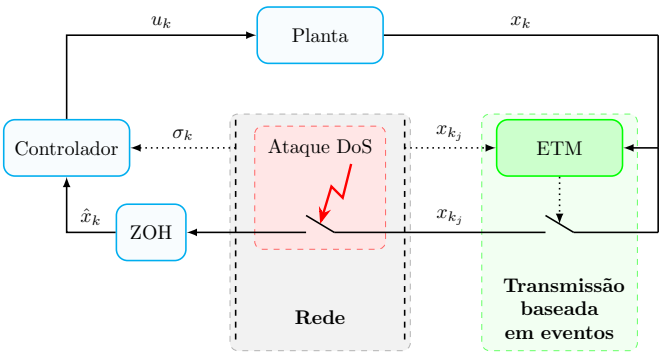

Figura 1. Configuração do sistema de controle em rede sujeito a ataques DoS.

A dinâmica da planta é descrita por:

$$x_{k+1} = Ax_k + Bu_k, \tag{1}$$

em que $x_k \in \mathbb{R}^n$ é o vetor de estados e $u_k \in \mathbb{R}^m$ é o vetor de entradas de controle. Além disso, na configuração

considerada, o controlador produz o sinal de controle de acordo com a lei

$$v_k = K\hat{x}_k, \tag{2}$$

sendo $K \in \mathbb{R}^{m\times n}$ o ganho do controlador e $\hat{x}_k$ a informação mais recente de x_k disponível para o controlador. Considera-se a implementação de um segurador de ordem zero (ZOH, do inglês *zero-order hold*).

Hipótese 1. Para a planta (1) e a lei de controle (2), a matriz K é tal que os valores absolutos dos autovalores de $A + BK$ são menores que 1.

Na presença de ataques DoS, a informação do estado não é atualizada para o cômputo correto de v_k. Para tratar esse efeito, similar aos trabalhos de van Dinther et al. (2020) e Kang e Ishii (2021), considera-se que a rede possui um mecanismo de reconhecimento de ataques que envia o sinal de defesa para o controlador, tal que o sinal de controle efetivamente aplicado à planta seja

$$u_k = \sigma_k v_k, \tag{3}$$

em que σ_k indica a ocorrência de um ataque DoS nos instantes de tentativas de transmissão k_j, ou seja, $\sigma_k = 0$ quando a transmissão é malsucedida e $\sigma_k = 1$ quando a transmissão é bem sucedida.

2.1 Ataques DoS com restrição de duração

Considere a sequência de ataques DoS $\{H_n\}_{n\in\mathbb{Z}^+}$, em que o n-ésimo ataque é definido por $H_n \triangleq \{h_n, \ldots, h_n+\tau_n-1\}$, sendo $h_n \in \mathbb{Z}^+$ o instante de início e $\tau_n \in \mathbb{Z}^+$ a duração.

Seja $\mathcal{I}_{DoS}$ a coleção de todas as sequências de ataques sem sobreposição, ou seja, $h_n \leq h_n + \tau_n - 1 < h_{n+1}$, para todo $n \in \mathbb{Z}^+$ com $h_0 \geq 0$. Para uma dada sequência $\{H_n\}_{n\in\mathbb{Z}^+} \in \mathcal{I}_{DoS}$, o conjunto de todos os instantes de tempo em que ataques DoS estão ativos é dado por

$$\mathcal{T} \triangleq \bigcup_{n\in\mathbb{Z}^+} H_n. \tag{4}$$

Pela definição em (4), pode-se descrever a atualização de $\hat{x}_k$ em (2) na presença de ataques DoS da seguinte forma

$$\hat{x}_k = \begin{cases} x_{k_j}, & k_j \notin \mathcal{T} \\ \hat{x}_{k-1}, & k_j \in \mathcal{T}. \end{cases} \tag{5}$$

Por consistência de notação, assume-se que $\hat{x}_{-1}{=}x_{-1}{=}x_0$.

Como os ataques DoS bloqueiam a transmissão de dados para o controlador, o sistema não pode ser estabilizado se ataques ocorrerem em todos os instantes de tempo. Por este motivo, considera-se a seguinte hipótese sobre a ocorrência dos ataques.

Hipótese 2. Seja $\Xi(k) = \bigcup_{n\in\mathbb{Z}^+} H_n \bigcap \{0,\ldots,k\}$ o intervalo total de ataques DoS lançados em $\{0,\ldots,k\}$. Existem $\eta \geq 0$ e $\nu \in [0,1]$ tal que, para $k \in \mathbb{Z}^+$, a duração dos ataques DoS satisfazem a condição:

$$\Phi(k) \leq \eta + \nu k, \tag{6}$$

sendo que $\Phi(k) = |\Xi(k)|$ denota o número total de ataques DoS lançados em $\{0,\ldots,k\}$.

O termo η pode ser interpretado como um termo de regularização, enquanto ν está relacionado com o percentual de amostras potencialmente perdidas devido aos ataques DoS lançados até o instante k.

Nota 3. O modelo de ataques DoS em (6) se baseia no modelo proposto por De Persis e Tesi (2016) que restringe a frequência e a duração de ataques que afetam sistemas a tempo contínuo. Como discutido em van Dinther et al. (2020), somente a restrição de duração é necessária no contexto discreto, uma vez que a restrição de frequência está relacionada com a possibilidade de ocorrência de ataques do tipo pulso, que não é possível no domínio discreto. Nota-se que (6) impõe somente uma restrição num sentido médio sobre a duração, portanto, esse modelo é capaz de capturar diferentes cenários de ataques DoS sem impor limitações sobre a sua estrutura, tais como os periódicos (Deng et al., 2021; Zhu e Zheng, 2019), aleatórios (Cetinkaya et al., 2015; Niemoczynski et al., 2016; Guo et al., 2020; Li et al., 2021) e de energia limitada (Lai et al., 2018; Wang et al., 2019), previamente estudados na literatura relacionada.

2.2 Controle com acionamento por eventos resiliente

Considera-se o ETM a seguir para gerar a sequência de instantes de tentativas de transmissão com o objetivo de reduzir o uso dos recursos da rede de comunicação:

$$k_{j+1} = \min\{k > k_j : \Gamma(\sigma_{k-1}, z_k) < 0\}, \tag{7}$$

em que $k_0 = 0$, $z_k = \left[x_k^\top \; e_k^\top\right]^\top$, $e_k = \hat{x}_{k_j} - x_k$, $\forall k \in \mathcal{K}_j$, é o erro de transmissão, $\mathcal{K}_j \triangleq \{k_j, \ldots, k_{j+1} - 1\}$ é o j-ésimo intervalo entre tentativas de transmissão, e a função de acionamento é dada por

$$\Gamma(\sigma_{k-1}, z_k) = \sigma_{k-1}\left(1 + z_k^\top \Psi z_k\right) - 1 \tag{8}$$

sendo

$$\Psi \triangleq \begin{bmatrix} \Psi_x & \Psi_{xe} \\ \star & -\Psi_e \end{bmatrix}$$

uma matriz simétrica a ser projetada com $\Psi_x, \Psi_e \in \mathbb{R}^{n\times n}$ sendo definidas positivas. A informação de σ_{k-1} indica ao ETM se houve ou não uma tentativa bem-sucedida de transmissão no instante anterior. Se em $k-1$ houve uma transmissão bem-sucedida, então $\Gamma(1, z_k) = z_k^\top \Psi z_k$ e o ETM opera normalmente. Por outro lado, se a transmissão foi malsucedida em $k-1$, então $\Gamma(0, z_k) = -1$, fazendo com que o ETM tente transmitir novamente em k. Essa estratégia de acionamento aumenta a frequência de tentativas de transmissão nos períodos em que o sistema detecta a ocorrência de ataques.

A partir da descrição da lei de controle em (3) e do efeito da transmissão aperiódica induzida pelo ETM em (7), é possível escrever o sistema em malha fechada da seguinte forma:

$$x_{k+1} = F_{\sigma_k} x_k + G_{\sigma_k} e_k, \tag{9}$$

em que $F_{\sigma_k} \triangleq A + \sigma_k BK$ e $G_{\sigma_k} \triangleq \sigma_k BK$. O sistema em (9) pode ser visto como um sistema dinâmico chaveado que comuta entre dois modos determinados pelo sinal dado por σ_k. No primeiro modo, quando $\sigma_k = 0$, o sistema (9) opera em malha aberta, enquanto que no segundo modo, quando $\sigma_k = 1$, o sistema (9) opera em malha fechada sujeito à perturbação induzida pelo erro de transmissão do acionamento por eventos.

2.3 Declaração do problema

Seja o sistema de controle em malha fechada (9) equipado com o ETM em (7) sujeito a sequências de ataques DoS

$\{H_n\}_{n\in\mathbb{Z}^+} \in \mathcal{I}_{DoS}$. Considerando que as Hipóteses 1 e 2 sejam atendidas, determine a função de acionamento (8) tal que a origem de (9) seja exponencialmente estável para $\nu < \bar{\nu} \in [0{,}1]$.

3. RESULTADOS PRINCIPAIS

3.1 Condição de projeto

Teorema 4. Considere o sistema de controle em rede sujeito a ataques DoS $\{H_n\}_{n\in\mathbb{Z}^+} \in \mathcal{I}_{DoS}$ composto pela planta em (1), lei de controle em (3) e ETM em (7). Considere que as Hipóteses 1 e 2 sejam satisfeitas. Se existirem $\alpha > 1$, $\beta \in (0{,}1)$, matrizes simétricas definidas positivas $P \in \mathbb{R}^{n\times n}$, $\tilde{\Psi}_x \in \mathbb{R}^{n\times n}$ e $\Psi_e \in \mathbb{R}^{n\times n}$, e uma matriz $\Psi_{xe} \in \mathbb{R}^{n\times n}$, tais que

$$F_0^\top P F_0 - \alpha P < 0, \tag{10}$$

$$\begin{bmatrix} F_1^\top P F_1 - \beta P & F_1^\top P G_1 + \Psi_{xe} & \mathrm{I} \\ \star & G_1^\top P G_1 - \Psi_e & 0 \\ \star & \star & -\tilde{\Psi}_x \end{bmatrix} < 0, \tag{11}$$

e o parâmetro ν satisfaz a restrição

$$\nu < \frac{-\ln\beta}{\ln\alpha - \ln\beta} \triangleq \bar{\nu}, \tag{12}$$

então o sistema de controle em rede em malha fechada (9) é exponencialmente estável.

Demonstração. Assuma que as condições (10)–(12) são satisfeitas. Seja $\Lambda(k)$ o conjunto das amostras efetivamente perdidas devido aos ataques DoS, dado por

$$\Lambda(k) \triangleq \left\{ k \in \mathbb{Z}^+ : k \in \bigcup_{j\in\mathbb{Z}^+} \mathcal{K}_j \wedge k_j \in \mathcal{T} \right\}.$$

Note que $\sigma_k = 0$, $\forall k \in \Lambda(k)$, e $|\Lambda(k)| = \sum_{p=0}^{k}(1-\sigma_p)$. A condição em (10) implica diretamente que

$$x_k^\top F_0^\top P F_0 x_k - \alpha x_k^\top P x_k < 0.$$

Definindo a função $V(x) = x^\top P x$, verifica-se que $V(x) > 0$ para todo $x \neq 0 \in \mathbb{R}^n$, uma vez que $P > 0$. Além disso, pela equação do sistema em malha fechada (9) operando com $\sigma_k = 0$, tem-se que

$$V(x_{k+1}) < \alpha V(x_k), \quad \forall k \in \Lambda(k). \tag{13}$$

Por complemento de Schur, a condição (11) implica que

$$\begin{bmatrix} F_1^\top P F_1 - \beta P + \Psi_x & F_1^\top P G_1 + \Psi_{xe} \\ \star & G_1^\top P G_1 - \Psi_e \end{bmatrix} < 0, \tag{14}$$

onde $\Psi_x \triangleq \tilde{\Psi}_x^{-1}$. Assumindo que o sistema não está sob ataque em um dado $k = k_j$, o sistema em malha fechada (9) opera no modo $\sigma_k = 1$. Assim, multiplicando (14) por $z_k^\top$ à esquerda e z_k à direita, tem-se que

$$V(x_{k+1}) < \beta V(x_k) - z_k^\top \Psi z_k. \tag{15}$$

Como o ETM (7) garante que $z_k^\top \Psi z_k \geq 0$, $\forall k \in \mathcal{K}_j$ (pois, caso contrário, haveria uma nova transmissão), (15) implica que

$$V(x_{k+1}) < \beta V(x_k), \quad \forall k \in \overline{\Lambda}(k), \tag{16}$$

sendo $\overline{\Lambda}(k) \triangleq \{0,\ldots,k\} \setminus \Lambda(k)$.

Segue de (13) e (16) que $V(x_k) \leq \alpha^{|\Lambda(k)|}\beta^{|\overline{\Lambda}(k)|}V(x_0)$, $\forall k \in \mathbb{N}$. Como $|\Lambda(k)| \leq \Phi(k)$, $|\overline{\Lambda}(k)| = k - |\Lambda(k)|$ e $\ln\alpha > \ln\beta$, é possível verificar que

$$V(x_k) \leq e^{[k\ln\beta + \Phi(k)(\ln\alpha - \ln\beta)]}V(x_0), \quad \forall k \in \mathbb{N}.$$

A condição em (6) implica que

$$V(x_k) \leq \rho e^{-\gamma k} V(x_0), \quad \forall k \in \mathbb{N}, \tag{17}$$

sendo $\rho = (\alpha/\beta)^\eta$ e $\gamma = -\ln\beta - \nu(\ln\alpha - \ln\beta)$. Sabendo que $\underline{\lambda}(P)\|x\|^2 \leq V(x) \leq \overline{\lambda}(P)\|x\|^2$, segue de (17) que $\|x_k\| \leq r e^{-\theta k}\|x_0\|$, onde $r = \sqrt{\rho\overline{\lambda}(P)/\underline{\lambda}(P)}$ e $\theta = \gamma/2$. Se ν satisfaz a condição em (12), é possível verificar que $\theta > 0$ e, portanto, o sistema é exponencialmente estável. Isso conclui a demonstração. ■

3.2 Problema de otimização multiobjetivo

O problema abordado neste trabalho possui dois objetivos principais relacionados à economia de largura de banda (redução do número de transmissões) e tolerância aos ataques DoS. O Teorema 4 garante que se as desigualdades (10) e (11) são satisfeitas para algumas matrizes $P > 0$, $\tilde{\Psi}_x > 0$ e $\Psi_e > 0$, então a estabilidade é garantida para qualquer $\nu < \bar{\nu}(\alpha,\beta)$. Portanto, maximizando $\bar{\nu}(\alpha,\beta)$, a estabilidade é garantida para uma maior gama de ataques DoS. Por outro lado, dada a política de transmissão do ETM descrita em (7), a minimização do traço de $\tilde{\Psi}_x + \Psi_e$ leva a redução do número de transmissões (Coutinho e Palhares, 2022). Dessa forma, define-se dois objetivos:

$$f_1 = \bar{\nu}(\alpha,\beta), \quad f_2 = \mathrm{tr}\left(\tilde{\Psi}_x + \Psi_e\right),$$

sendo que f_1 está relacionado à tolerância a ataques e f_2 à economia de largura de banda.

Para lidar com esse problema de otimização multiobjetivo, este trabalho propõe o uso do método ε-restrito (Mavrotas, 2009). Nesse sentido, o objetivo f_1 é otimizado sob a restrição do objetivo f_2 pelo escalar $\varepsilon \in \mathbb{R}_{>0}$. Portanto, o problema de otimização a seguir é resolvido nesse trabalho:

$$\begin{aligned} \text{maximizar} \quad & \bar{\nu}(\alpha,\beta) \\ \text{sujeito a} \quad & \mathrm{tr}\left(\tilde{\Psi}_x + \Psi_e\right) \leq \varepsilon, \\ & P > 0,\ \tilde{\Psi}_x > 0,\ \Psi_e > 0, \\ & (10),\ (11),\ 0 < \beta < 1,\ \alpha > 1. \end{aligned} \tag{18}$$

Para diferentes valores de ε, duas buscas em grade [1] são realizadas para obter as taxas de crescimento e decaimento, α e β, que maximizam $\bar{\nu}$. Para cada valor de ε, α e β, o problema de otimização (18) se torna um problema de programação semidefinida [2].

4. SIMULAÇÕES NUMÉRICAS

Considere o sistema a tempo discreto da forma:

$$x_{k+1} = \begin{bmatrix} 1{,}0050 & 0{,}0501 \\ 0{,}2003 & 1{,}0050 \end{bmatrix} x_k + \begin{bmatrix} 0{,}0501 \\ 0{,}0050 \end{bmatrix} u_k$$

obtido a partir da discretização do sistema a tempo contínuo em (Sbarbaro et al., 2014, Exemplo 2) com tempo de

[1] As buscas em grade foram realizadas utilizando o método da bisseção.

[2] Neste trabalho, o problema de programação semidefinida foi resolvido no ambiente do MATLAB utilizando o *solver* MOSEK e o *parser* YALMIP.

amostragem de 0,05 s. Considerando o ganho de realimentação de estados $K = [-6\ -3]$, a Hipótese 1 é satisfeita, uma vez que os autovalores de $A+BK$ são 0,7897 e 0,9048.

Inicialmente, avalia-se a relação entre a economia de largura de banda e tolerância aos ataques DoS a partir da solução do problema de otimização em (18). Para isso, são considerados valores de ε em uma grade de 20 pontos espaçados em uma escala logarítmica entre as décadas 10^1 e 10^5. Os pares (α^*, β^*) que maximizam a função objetivo $f_1 = \bar{\nu}$ para cada valor de ε são obtidos por meio de buscas em grade sobre os parâmetros α e β. Os valores de $\bar{\nu}$ obtidos com esse procedimento são apresentados na Figura 2. É possível verificar a relação de compromisso existente entre as duas funções objetivo f_1 e f_2, de modo que com menos tentativas de transmissões (valores menores de f_2), é possível garantir a estabilidade exponencial para ataques DoS com durações menores (valores menores de f_1). Para valores maiores de ε, $\bar{\nu}$ tende ao valor 0,5, que corresponde à garantia de estabilidade com a transmissão periódica.

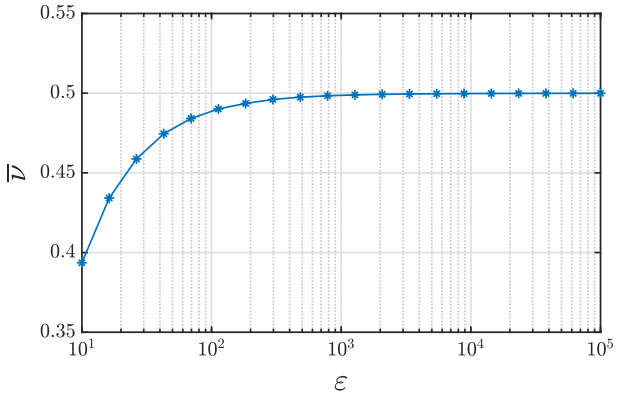

Figura 2. Valores de $\bar{\nu}$ obtidos via o problema de otimização em (18) para diversos valores de ε.

Para ilustrar a aplicação da estratégia de ETC resiliente proposta, o problema de otimização (18) é resolvido para $\varepsilon = 69{,}5193$, resultando em $(\alpha^*, \beta^*) = (1{,}2241, 0{,}8271)$, $\bar{\nu} = 0{,}4841$ e no ETM (7)–(8) com a seguinte matriz Ψ:

$$\Psi = \left[\begin{array}{cc|cc} 45{,}6631 & 21{,}9157 & 70{,}7199 & 35{,}3600 \\ 21{,}9157 & 10{,}5543 & 35{,}4320 & 17{,}7160 \\ \hline 70{,}7199 & 35{,}4320 & -28{,}2575 & -14{,}1259 \\ 35{,}3600 & 17{,}7160 & -14{,}1259 & -7{,}0686 \end{array}\right]$$

Assumindo $\eta = 0$ em (6), define-se $\Theta = \lfloor k\bar{\nu} \rfloor$ como o número total de amostras que podem ser perdidas pelos ataques DoS no intervalo $\{0, \ldots, k\}$. Note que assumir $\eta = 0$ não é restritivo pois este parâmetro não afeta a estabilidade, especialmente quando $k \to \infty$. Duas sequências de ataques foram consideradas para a avaliação da estratégia de ETC resiliente em simulações de duração de 10 s, ou seja, $k = 201$ amostras, e com condição inicial $x_0 = [-1{,}125\ -2{,}75]^\top$. Na primeira, Sequência 1, considerou-se um cenário com menos intervalos de ataques DoS com durações maiores, enquanto na segunda, Sequência 2, foi avaliada uma sequência com mais intervalos de ataques com durações menores, ambas gerando o mesmo $\Theta = 97$. Os resultados para as Sequências 1 e 2 são apresentados nas Figuras 3 e 4, respectivamente. Os números de transmissões bem-sucedidas e malsucedidas para as duas sequências de ataques são apresentados na Tabela 1.

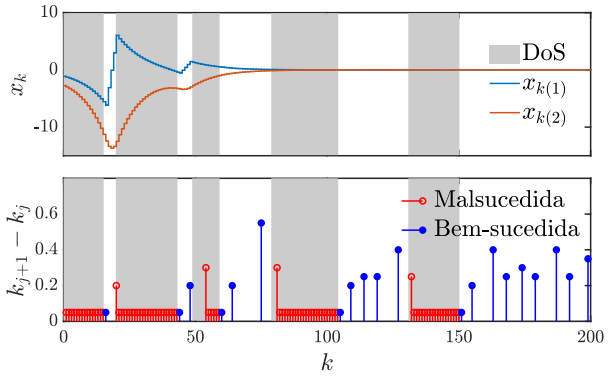

Figura 3. Resultados de simulação para a Sequência 1. As trajetórias dos estados x_k são apresentadas no painel superior e os tempos entre tentativas de transmissões no inferior. As listras verticais cinzas representam os intervalos de tempo nos quais o DoS está ativo.

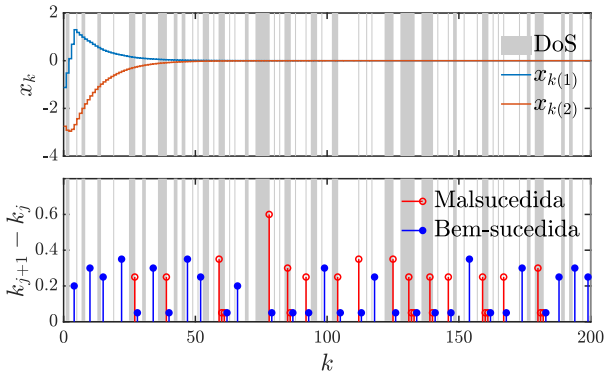

Figura 4. Resultados de simulação para a Sequência 2. As trajetórias dos estados x_k são apresentadas no painel superior e os tempos entre tentativas de transmissões no inferior. As listras verticais cinzas representam os intervalos de tempo nos quais o DoS está ativo.

Tabela 1. Número de transmissões para as diferentes sequências de ataque e políticas de transmissão.

ETC			
Sequência de ataque	**Transmissões**		
	Bem-sucedidas	Malsucedidas	Total
1	20	89	109
2	31	25	56
Transmissão periódica			
Sequência de ataque	**Transmissões**		
	Bem-sucedidas	Malsucedidas	Total
1 e 2	104	97	201

É possível notar que, apesar dos ataques DoS, a estabilidade foi garantida em ambos os cenários. Além disso, o número de transmissões malsucedidas foi maior no caso da Sequência 1 do que no da Sequência 2 devido à maior duração dos ataques. Em contrapartida, com o maior número de ataques na Sequência 2, o sistema de ETC se apresentou mais reativo, levando a um maior número de transmissões bem-sucedidas. Finalmente, em comparação com a amostragem periódica, o esquema de ETC proposto

foi efetivo na redução da largura de banda em ambos os cenários, já que reduziu significativamente o número de tentativas de transmissão.

5. CONCLUSÕES

Este trabalho abordou o problema de ETC resiliente para sistemas discretos no tempo sujeitos a ataques DoS aperiódicos com duração limitada. Para isso, este trabalho apresentou um problema convexo de otimização multiobjetivo baseado em emulação para o projeto de um ETM estático, a fim de minimizar o consumo de banda e maximizar a tolerância à ataques DoS. Tal problema de otimização baseou-se em restrições LMI, que permitiu o projeto do ETM com o uso de programação semidefinda. Simulações numéricas mostraram que o sistema de ETC foi capaz de garantir a estabilidade exponencial do sistema frente a ataques DoS, além de possibilitar uma redução significativa no número de transmissões. Em trabalhos futuros, a abordagem pode ser aprimorada para projetar ETMs dinâmicos para sistemas não-lineares.

REFERÊNCIAS

Ban, J., Seo, M., Goh, T., Jeong, H., e Kim, S.W. (2020). Improved co-design of event-triggered dynamic output feedback controllers for linear systems. *Automatica*, 111, 108600.

Cetinkaya, A., Ishii, H., e Hayakawa, T. (2015). Event-triggered output feedback control resilient against jamming attacks and random packet losses. *IFAC-PapersOnLine*, 48(22), 270–275.

Coutinho, P.H.S. e Palhares, R.M. (2022). Codesign of dynamic event-triggered gain-scheduling control for a class of nonlinear systems. *IEEE Trans. Automat. Contr.*, 67(8), 4186–4193. 10.1109/TAC.2021.3108498.

De Persis, C. e Tesi, P. (2016). Networked control of nonlinear systems under Denial-of-Service. *Syst. Control Lett.*, 96, 124–131.

De Persis, C. e Tesi, P. (2018). A comparison among deterministic packet-dropouts models in networked control systems. *IEEE Control Syst.*, 2, 109–114.

De Persis, C. e Tesi, P. (2021). Resilient control under denial-of-service: Results and research directions. In *Lect. Notes Control Inf. Sci.*, 41–60. Springer.

Deng, Y., Yin, X., e Hu, S. (2021). Event-triggered predictive control for networked control systems with DoS attacks. *Inf. Sci.*, 542, 71–91.

Ding, D., Wang, Z., Han, Q.L., e Wei, G. (2018). Security control for discrete-time stochastic nonlinear systems subject to deception attacks. *IEEE Trans. Syst. Man, Cybern. Syst.*, 48(5), 779–789.

Guo, L., Yu, H., e Hao, F. (2020). Event-triggered control for stochastic networked control systems against denial-of-service attacks. *Inf. Sci.*, 527, 51–69.

Kang, X. e Ishii, H. (2021). Resilient control of uncertain networked systems under DoS attacks. In *CDC'2021*, 6952–6957. Austin, TX, USA.

Lai, S., Chen, B., Li, T., e Yu, L. (2018). Packet-based state feedback control under DoS attacks in cyber-physical systems. *IEEE Trans. Circuits Syst. II: Express Br.*, 66(8), 1421–1425.

Li, X., Wei, G., e Wang, L. (2021). Distributed set-membership filtering for discrete-time systems subject to denial-of-service attacks and fading measurements: A zonotopic approach. *Inf. Sci.*, 547, 49–67.

Mahmoud, M.S., Hamdan, M.M., e Baroudi, U.A. (2020). Secure control of cyber physical systems subject to stochastic distributed DoS and deception attacks. *Int. J. Syst. Sci.*, 51(9), 1653–1668.

Mavrotas, G. (2009). Effective implementation of the ε-constraint method in multi-objective mathematical programming problems. *Appl. Math. Ccomput.*, 213(2), 455–465.

Niemoczynski, B., Biswas, S., e Kollmer, J. (2016). Stability of discrete-time networked control systems under denial of service attacks. In *Resilience Week (RWS)*, 119–124.

Rotondo, D., Sánchez, H.S., Puig, V., Escobet, T., e Quevedo, J. (2019). A virtual actuator approach for the secure control of networked LPV systems under pulse-width modulated DoS attacks. *Neurocomputing*, 365, 21–30.

Sbarbaro, D., Tarbouriech, S., e Gomes da Silva Jr, J. (2014). An event-triggered observer based control strategy for SISO systems. In *CDC'2014*, 2789–2794. IEEE.

Teixeira, A., Shames, I., Sandberg, H., e Johansson, K.H. (2015). A secure control framework for resource-limited adversaries. *Automatica*, 51, 135–148.

van Dinther, D., Feng, S., Ishii, H., e Heemels, W.M. (2020). Towards the coarsest quantized controller under denial-of-service attacks. *IFAC-PapersOnLine*, 53(2), 3496–3501.

Wang, J., Gao, J., e Wu, P. (2021). Attack-resilient event-triggered formation control of multi-agent systems under periodic dos attacks using complex laplacian. *ISA Trans.* doi:10.1016/j.isatra.2021.10.030.

Wang, Z., Li, L., Sun, H., Zhu, C., e Xu, X. (2019). Dynamic output feedback control of cyber-physical systems under DoS attacks. *IEEE Access*, 7, 181032–181040.

Yan, H., Wang, J., Zhang, H., Shen, H., e Zhan, X. (2020). Event-based security control for stochastic networked systems subject to attacks. *IEEE Trans. Syst. Man Cybern.: Syst.*, 50, 4643–4654.

Zhang, H., Hu, J., Liu, G.P., e Yu, X. (2022). Event-triggered secure control of discrete systems under cyber-attacks using an observer-based sliding mode strategy. *Inf. Sci.*, 587, 587–606.

Zhang, Z.H., Liu, D., Deng, C., e Fan, Q.Y. (2020). A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous DoS attacks. *Inf. Sci.*, 519, 260–272.

Zhao, N., Shi, P., Xing, W., e Lim, C.P. (2022). Event-triggered control for networked systems under denial of service attacks and applications. *IEEE Trans. Circuits Syst. I, Reg. Papers*, 69, 811–820.

Zhu, Y. e Zheng, W.X. (2019). Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy. *IEEE Trans. Automat. Contr.*, 65(8), 3714–3721.