

Research Article

Open Access



# Importance-driven denial of service attack strategy design against remote state estimation in multi-agent intelligent power systems

Xia Zhao<sup>1</sup>, Guowei Liu<sup>2</sup>, Lei Li<sup>3</sup>

<sup>1</sup>College of Science, University of Shanghai for Science and Technology, Shanghai 200093, China.

<sup>2</sup>School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China.

<sup>3</sup>Human Resources and Social Security Bureau of Jimo District, Qingdao 266200, Shandong, China.

**Correspondence to:** Dr. Guowei Liu, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, 516 Jungong Road, Yangpu District, Shanghai 200093, China. E-mail: zwliuguowei@163.com

**How to cite this article:** Zhao X, Liu G, Li L. Importance-driven denial of service attack strategy design against remote state estimation in multi-agent intelligent power systems. *Intell Robot* 2024;4(3):244-55. <http://dx.doi.org/10.20517/ir.2024.16>

**Received:** 14 May 2024 **First Decision:** 3 Jul 2024 **Revised:** 16 Jul 2024 **Accepted:** 25 Jul 2024 **Published:** 31 Jul 2024

**Academic Editor:** Simon X. Yang **Copy Editor:** Pei-Yun Wang **Production Editor:** Pei-Yun Wang

## Abstract

This paper introduces a novel importance-driven denial of service (IDoS) attack strategy aimed at impairing the quality of remote estimators for target agents within multi-agent intelligent power systems. The strategy features two key aspects. Firstly, the IDoS attack strategy concentrates on target agents, enabling attackers to determine the voltage sensitivity of each agent based on limited information. By utilizing these sensitivities, the proposed strategy selectively targets agents with high sensitivity to amplify disruption on the target agent. Secondly, unlike most existing denial of service attack strategies that adhere to predefined attack sequences, IDoS attacks can selectively target important packets on highly sensitive agents, causing further disruption to the target agent. Simulation results on the IEEE 39-Bus system demonstrate that, compared to existing denial of service attack strategies, the proposed IDoS attack strategy significantly diminishes the estimation quality of the target agent, confirming its effectiveness from an attacker's perspective.

**Keywords:** Multi-agent power systems, remote state estimation, DoS attacks, cyber attacks



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose, even commercially, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.



## 1. INTRODUCTION

The power system is the backbone of society, directly impacting people's lives and a nation's economy<sup>[1]</sup>. However, as digitalization advances, interconnected power systems present more opportunities for attackers<sup>[2]</sup>. Among the various types of attacks, denial of service (DoS) attacks and deception attacks are predominant<sup>[3]</sup>. Unlike deception attacks, DoS attacks aim to exhaust network resources, cause congestion, and disrupt user access by flooding the system with a large volume of meaningless packets<sup>[4]</sup>. Despite the apparent simplicity of DoS attacks, their destructive potential poses a significant threat to the stability of the power system, warranting heightened attention<sup>[5,6]</sup>.

In the field of power system security literature, there are generally two main perspectives: the defender's perspective and the attacker's perspective. The defender's perspective focuses on developing various methods to counter increasingly severe cyber attacks, including techniques such as proportional-integral observers<sup>[7]</sup>, consensus control<sup>[8]</sup>, bandwidth-conscious event-based control<sup>[9]</sup>, and collision-free multi-platoon control<sup>[10]</sup>. In contrast, the attacker's perspective predominantly explores more destructive attack strategies or seeks to enhance stealthiness. For instance,<sup>[11]</sup> optimizes attack scheduling to maximize destructive impact and proposes that continuous attacks can significantly amplify the potency of DoS attacks. Building upon this,<sup>[12]</sup> addresses attack scheduling under energy constraints. To counteract remote estimators, studies such as<sup>[13–15]</sup> respectively delve into stochastic DoS attack allocation, adaptive dynamic programming approach, and attack energy management. Furthermore, studies such as<sup>[16–18]</sup> explore the complexity of attack scheduling, encompassing aspects such as sensors, communication protocols, and cooperation strategies.

In this context, most DoS attacks are typically indiscriminate, meaning the attacker lacks specific knowledge about the target system and employs random or preset patterns of attack<sup>[11]</sup>. On the other hand, deception attacks are based on the attacker having an in-depth understanding of the system<sup>[19]</sup>, including detailed knowledge of its structure, parameters, controller gains, and estimator gains. These two types of attackers represent two extremes: one is completely unaware of the system and relies on random or preset attack strategies, while the other is well-informed about the system and can leverage detailed information to execute precise attacks. Typically, certain information about power systems, such as topology and system output, is relatively easy for attackers to obtain, while other critical details, such as estimator gains, are harder to access. Therefore, from the attacker's perspective, devising an attack strategy based on readily accessible system information is crucial, which is a key motivation for this paper.

Although the aforementioned literature endeavors to increase the destructiveness of attacks, two critical issues deserve attention. Firstly, most current DoS attack strategies indiscriminately target the entire system in a predetermined sequence. However, in real-world power systems, certain agents hold greater significance, such as those serving airports, hospitals, financial centers, and control centers<sup>[20]</sup>. Designing a DoS attack strategy to inflict greater damage on specific agents is one of the primary motivations of this paper. Secondly, certain information in power systems is easily accessible to attackers, such as packet importance<sup>[21]</sup>, system topology, and rated parameters. Effectively leveraging this information to amplify the destructiveness of DoS attacks serves as another motivation for this paper.

To tackle the challenges outlined above, this paper first proposes a method for calculating the sensitivity of target agent voltages. Secondly, we utilize these sensitivities to develop a novel importance-driven DoS (IDoS) attack strategy, which integrates agent voltage sensitivity with packet importance. To achieve these objectives, we pose two questions:

- (1) How to design a method to calculate voltage sensitivity using limited information?
- (2) How to design the IDoS attack strategy by integrating sensitivity information with packet importance?

The primary focus of this paper is to address these two inquiries. The key innovations of this paper are summarized as follows:

- (1) A new method for computing voltage sensitivity is proposed. Unlike existing sensitivity calculation approaches<sup>[22–24]</sup>, this method reduces reliance on system information, including current state values and their respective rates of change, thereby enabling attackers to implement attacks more practically.
- (2) A novel IDoS attack strategy is designed, which integrates both voltage sensitivity and packet importance. Unlike most DoS attack strategies that target indiscriminately<sup>[11,12]</sup>, our approach allocates more attack energy to important packets on sensitive agents, thus resulting in a greater potential for disruption on the target agent compared to other attack strategies.

The structure of the subsequent sections of this paper is as follows: Section 2 discusses the calculation of voltage sensitivity. Section 3 presents the design process of the IDoS attack strategy. Section 4 conducts simulations to assess the destructive capability of the attack strategy. Finally, Section 5 provides a summary of the study.

**Notation** Let the superscript  $\Re$  indicate the real part of a parameter, the superscript  $\Im$  denote the imaginary part, and the superscript  $T$  represent the transpose of a matrix. The notation  $\|\cdot\|$  denotes the Euclidean norm,  $\Delta$  signifies a change in a parameter, and  $\exp(\cdot)$  refers to the exponential function with base  $e$ .

## 2. SYSTEM AND STATE ESTIMATION

In a multi-agent power system with  $n$  agents, the measured values obtained from devices such as phasor measurement units (PMUs) can be represented as  $z(k) = [z_1(k) \cdots z_n(k)]^T$ , where  $k$  indicates the discrete time step,  $z_i(k) = V_i(k)$  and  $V_i$  is the voltage of the  $i$  ( $i = 1, \dots, n$ )th agent. The system state can be denoted as  $x(k) = [x_1(k) \cdots x_n(k)]^T$ , where  $x_i(k) = [V_i(k) I_i(k) \theta_i(k)]^T$ , in which  $I_i$  signifies the injected current at the  $i$ th agent and  $\theta_i$  is the phase angle. Therefore, the system model can be expressed as:

$$z(k) = h(x(k)) + \epsilon(k), \quad (1)$$

where  $\epsilon(k)$  denotes the measurement noise.

Various methods are proposed to estimate the system's state, with weighted least squares (WLS) being widely favored, defined as follows:

$$\hat{x}(k) = \arg \min_{x(k)} [z(k) - h(x(k))]^T Y^{-1} [z(k) - h(x(k))], \quad (2)$$

where  $Y$  denotes the covariance matrix of measurement errors.

After completing the state estimation process, the detection of faulty data is typically performed to identify potential measurement errors. Among various methods for detection, the maximum normalized residual test is the most commonly used. In this method, the residual is defined as:

$$\gamma(k) = \left\| z(k) - h(x(\hat{k})) \right\|_2. \quad (3)$$

The parameter  $\gamma(k)$  serves as a crucial metric for assessing estimation quality. A lower  $\gamma(k)$  value indicates superior estimation performance. Therefore, our study focuses on designing a DoS attack strategy from the attacker's perspective to maximize  $\gamma(k)$ .

### 3. IDOS ATTACK STRATEGY DESIGN

In this section, a novel IDoS attack strategy from the attacker's perspective is introduced. This strategy leverages the voltage sensitivity of agents and the importance of packets. By allocating more attack energy to the critical data packets of highly sensitive agents, it maximizes the estimation error of the remote estimator. The design comprises two main steps: firstly, analyzing the voltage-current relationships of all agents in the system to determine the voltage sensitivity of the target agent to each agent; secondly, allocating more attack energy to important packets on highly sensitive agents, thereby inflicting more severe damage on the target agent.

#### 3.1 Voltage sensitivity to powers

To enhance the feasibility and practicality of the proposed IDoS attack, this subsection introduces a new method for calculating voltage sensitivity. This method minimizes the attacker's need for extensive system information, requiring only the power system's topology and rated parameters to accurately compute the voltage sensitivity of each agent. The calculation process is as follows: First, the relationship between system voltage and current is established through power flow analysis. Next, the active and reactive voltage sensitivities of the target agent are determined from this relationship. Finally, the voltage sensitivity of the target to all other agents is obtained using an improved entropy method.

In the multi-agent power system, the first agent is designated as the reference agent with its voltage set as the reference voltage. The relationship between the voltage of each agent and the injected current can be expressed as follows:

$$\begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ \varphi_2 & \Phi_{22} & \cdots & \Phi_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_n & \Phi_{n2} & \cdots & \Phi_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix}, \quad (4)$$

where

$$\begin{aligned} \Phi_{2n} &= R_{2n} + jX_{2n}, \quad \Phi_{n2} = R_{n2} + jX_{n2}, \\ \Phi_{22} &= - \sum_{i=1, i \neq 2}^n (R_{2i} + jX_{2i}), \quad \Phi_{nn} = - \sum_{i=1}^{n-1} (R_{ni} + jX_{ni}), \end{aligned}$$

in which  $R_{ni} + jX_{ni}$  ( $i = 1, \dots, n$ ) represents the impedance of the line between the  $i$ th agent and the  $n$ th agent,  $\varphi$  denotes the scaling constant, and  $V_i$  and  $I_i$  refer to the rated voltage and rated injected current of the  $i$ th agent, respectively.

Without loss of generality, we define the  $\xi$  ( $\xi = 1, \dots, n$ )th agent as the target agent. For simplicity, let us assume that all agents except the  $i$ th one have zero injected currents. Based on Equation (4), we obtain the following outcomes:

$$(V_\xi^{\Re} + jV_\xi^{\Im})(V_i^{\Re} - jV_i^{\Im}) - (V_{\varphi\xi}^{\Re} + jV_{\varphi\xi}^{\Im})(V_i^{\Re} - jV_i^{\Im}) = (R_i + jX_i)(P_i - jQ_i), \quad (5)$$

where  $V_{\varphi\xi} = \varphi_\xi V_1$ ,  $P_i$  and  $Q_i$  represent the rated active power and rated reactive power of the  $i$ th agent, while  $\Re$  and  $\Im$  denote the real and imaginary parts of the parameters, respectively.

To understand how changes in active power  $P_i$  affect the voltage  $V_\xi$  of the target agent, we take the partial derivative of the active power with respect to Equation (5). This operation gives us the voltage-active sensitivity, which measures the change in voltage at agent  $\xi$  due to a change in active power at agent  $i$ . The voltage-active sensitivity of the  $\xi$ th agent to the  $i$ th agent can be expressed as:

$$\varepsilon_{Pi} = \frac{\partial V_\xi}{\partial P_i} = \frac{1}{V_\xi} (V_\xi^{\Re} \frac{\partial V_\xi^{\Re}}{\partial P_i} + V_\xi^{\Im} \frac{\partial V_\xi^{\Im}}{\partial P_i}). \quad (6)$$

Specifically, when  $i = \xi$ , Equation (5) can be updated to:

$$(V_{\varphi\xi}^{\mathcal{R}} + jV_{\varphi\xi}^{\mathcal{I}})(V_{\xi}^{\mathcal{R}} - jV_{\xi}^{\mathcal{I}}) - V_{\xi}^2 = \left( \sum_{i=1, i \neq \xi}^n R_{\xi i} + j \sum_{i=1, i \neq \xi}^n X_{\xi i} \right) (P_{\xi} - jQ_{\xi}). \quad (7)$$

In this case, by taking the partial derivative of the active power with respect to Equation (7), the self-voltage sensitivity of the  $\xi$ th agent is:

$$\varepsilon_{P_{\xi}} = \frac{\partial V_{\xi}}{\partial P_{\xi}} = \frac{1}{V_{\xi}} (V_{\xi}^{\mathcal{R}} \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial P_{\xi}} + V_{\xi}^{\mathcal{I}} \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial P_{\xi}}). \quad (8)$$

This self-sensitivity reflects how changes in the active power of the target agent itself affect its own voltage. Parameters  $\frac{\partial V_{\xi}^{\mathcal{R}}}{\partial P_i}$ ,  $\frac{\partial V_{\xi}^{\mathcal{I}}}{\partial P_i}$ ,  $\frac{\partial V_{\xi}^{\mathcal{R}}}{\partial P_{\xi}}$  and  $\frac{\partial V_{\xi}^{\mathcal{I}}}{\partial P_{\xi}}$  in Equations (6) and (8) are determined by solving the following system of equations:

$$\begin{cases} \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial P_i} = \frac{1}{V_i} (V_i^{\mathcal{R}} (R_i + V_{\varphi\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{R}}}{\partial P_i} + V_{\varphi\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{I}}}{\partial P_i} - V_{\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{R}}}{\partial P_i} - V_{\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{I}}}{\partial P_i}) \\ \quad - V_i^{\mathcal{I}} (V_{\varphi\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{R}}}{\partial P_i} - V_{\varphi\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{I}}}{\partial P_i} - V_{\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{R}}}{\partial P_i} + V_{\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{I}}}{\partial P_i} + X_i), \\ \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial P_i} = \frac{1}{V_i} ((V_{\varphi\xi}^{\mathcal{I}} - V_{\xi}^{\mathcal{I}}) \frac{\partial V_i^{\mathcal{R}}}{\partial P_i} - (V_{\varphi\xi}^{\mathcal{R}} - V_{\xi}^{\mathcal{R}}) \frac{\partial V_i^{\mathcal{I}}}{\partial P_i} + V_i^{\mathcal{I}} \frac{\partial V_i^{\mathcal{R}}}{\partial P_i} + X_i), \\ \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial P_{\xi}} = \frac{2V_{\xi}^{\mathcal{I}} \Phi_{\xi\xi}^{\mathcal{I}} - V_{\varphi\xi}^{\mathcal{I}} \Phi_{\xi\xi}^{\mathcal{I}} - V_{\varphi\xi}^{\mathcal{R}} \Phi_{\xi\xi}^{\mathcal{R}}}{(V_{\varphi\xi}^{\mathcal{R}})^2 + (V_{\varphi\xi}^{\mathcal{I}})^2 - 2V_{\varphi\xi}^{\mathcal{R}} V_{\xi}^{\mathcal{R}} - 2V_{\varphi\xi}^{\mathcal{I}} V_{\xi}^{\mathcal{I}}}, \\ \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial P_{\xi}} = \frac{\Phi_{\xi\xi}^{\mathcal{I}}}{V_{\varphi\xi}^{\mathcal{R}}} + \frac{V_{\varphi\xi}^{\mathcal{R}} \partial V_{\xi}^{\mathcal{R}}}{V_{\varphi\xi}^{\mathcal{I}} \partial P_{\xi}}. \end{cases} \quad (9)$$

Through the aforementioned steps, the voltage-active power sensitivity vector  $\varepsilon_P = [\varepsilon_{P_1} \cdots \varepsilon_{P_n}]$  can be obtained.

Similarly, from Equation (5), we can obtain the voltage-reactive sensitivity of the  $\xi$ th agent to the  $i$ th agent as:

$$\begin{aligned} \varepsilon_{Q_i} &= \frac{\partial V_{\xi}}{\partial Q_i} = \frac{1}{V_{\xi}} (V_{\xi}^{\mathcal{R}} \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial Q_i} + V_{\xi}^{\mathcal{I}} \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial Q_i}), \\ \varepsilon_{Q_{\xi}} &= \frac{\partial V_{\xi}}{\partial Q_{\xi}} = \frac{1}{V_{\xi}} (V_{\xi}^{\mathcal{R}} \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial Q_{\xi}} + V_{\xi}^{\mathcal{I}} \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial Q_{\xi}}), \end{aligned} \quad (10)$$

where the unknown parameters  $\frac{\partial V_{\xi}^{\mathcal{R}}}{\partial Q_i}$ ,  $\frac{\partial V_{\xi}^{\mathcal{I}}}{\partial Q_i}$ ,  $\frac{\partial V_{\xi}^{\mathcal{R}}}{\partial Q_{\xi}}$  and  $\frac{\partial V_{\xi}^{\mathcal{I}}}{\partial Q_{\xi}}$  can be solved by the following system of equations:

$$\begin{cases} \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial Q_i} = \frac{1}{V_i} (V_i^{\mathcal{R}} (X_i + V_{\varphi\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{R}}}{\partial Q_i} + V_{\varphi\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{I}}}{\partial Q_i} - V_{\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{R}}}{\partial Q_i} - V_{\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{I}}}{\partial Q_i}) \\ \quad - V_i^{\mathcal{I}} (V_{\varphi\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{R}}}{\partial Q_i} - V_{\varphi\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{I}}}{\partial Q_i} - V_{\xi}^{\mathcal{I}} \frac{\partial V_i^{\mathcal{R}}}{\partial Q_i} + V_{\xi}^{\mathcal{R}} \frac{\partial V_i^{\mathcal{I}}}{\partial Q_i} - R_i), \\ \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial Q_i} = \frac{1}{V_i} ((V_{\varphi\xi}^{\mathcal{I}} - V_{\xi}^{\mathcal{I}}) \frac{\partial V_i^{\mathcal{R}}}{\partial Q_i} - (V_{\varphi\xi}^{\mathcal{R}} - V_{\xi}^{\mathcal{R}}) \frac{\partial V_i^{\mathcal{I}}}{\partial Q_i} + V_i^{\mathcal{I}} \frac{\partial V_i^{\mathcal{R}}}{\partial Q_i} - R_i), \\ \frac{\partial V_{\xi}^{\mathcal{R}}}{\partial Q_{\xi}} = \frac{V_{\varphi\xi}^{\mathcal{I}} \Phi_{\xi\xi}^{\mathcal{R}} - 2V_{\xi}^{\mathcal{I}} \Phi_{\xi\xi}^{\mathcal{R}} - V_{\varphi\xi}^{\mathcal{R}} \Phi_{\xi\xi}^{\mathcal{I}}}{(V_{\varphi\xi}^{\mathcal{R}})^2 + (V_{\varphi\xi}^{\mathcal{I}})^2 - 2V_{\varphi\xi}^{\mathcal{R}} V_{\xi}^{\mathcal{R}} - 2V_{\varphi\xi}^{\mathcal{I}} V_{\xi}^{\mathcal{I}}}, \\ \frac{\partial V_{\xi}^{\mathcal{I}}}{\partial Q_{\xi}} = \frac{V_{\varphi\xi}^{\mathcal{R}} \partial V_{\xi}^{\mathcal{R}}}{V_{\varphi\xi}^{\mathcal{I}} \partial Q_{\xi}} - \frac{\Phi_{\xi\xi}^{\mathcal{R}}}{V_{\varphi\xi}^{\mathcal{I}}}. \end{cases} \quad (11)$$

Therefore, the voltage-reactive power sensitivity vector  $\varepsilon_Q = [\varepsilon_{Q_1} \cdots \varepsilon_{Q_n}]$  can be derived.

After normalizing these vectors, the Pearson correlation coefficient is introduced. The sliding window for the  $i$ th agent is defined as:

$$\varpi_i = \begin{cases} [i, i + \psi], & \text{if } i \leq n - \psi; \\ [i, n] \cup [1, \psi - n + i], & \text{otherwise,} \end{cases} \quad (12)$$

where the window length is  $\psi + 1$  and  $\psi \leq n - 1$ . A shorter window can promptly respond to short-term data changes but may be susceptible to noise interference. Conversely, a longer window can effectively smooth out data, reducing the impact of noise, yet it may not be as sensitive to short-term fluctuations. Attackers can tailor their choice of window length based on the specific characteristics of the data.

As the window moves, the correlation coefficient can be calculated by:

$$r_i(\varepsilon'_P, \varepsilon'_Q) = \frac{\sum_{l \in \varpi_i} [(\varepsilon'_{P_l} - \bar{\varepsilon}'_P)(\varepsilon'_{Q_l} - \bar{\varepsilon}'_Q)]}{\sqrt{\sum_{l \in \varpi_i} (\varepsilon'_{P_l} - \bar{\varepsilon}'_P)^2} \sqrt{\sum_{l \in \varpi_i} (\varepsilon'_{Q_l} - \bar{\varepsilon}'_Q)^2}}, \quad (13)$$

where

$$\begin{aligned} \varepsilon'_{P_i} &= \frac{\varepsilon_{P_i} - \min(\varepsilon_P)}{\max(\varepsilon_P) - \min(\varepsilon_P)}, \quad \bar{\varepsilon}'_P = \frac{1}{n} \sum_{i=1}^n \varepsilon'_{P_i}, \\ \varepsilon'_{Q_i} &= \frac{\varepsilon_{Q_i} - \min(\varepsilon_Q)}{\max(\varepsilon_Q) - \min(\varepsilon_Q)}, \quad \bar{\varepsilon}'_Q = \frac{1}{n} \sum_{i=1}^n \varepsilon'_{Q_i}. \end{aligned}$$

To capture the interrelationships among the elements in the sensitivity vector, we introduce exponential information entropy. Therefore, the voltage sensitivity of the target agent to the  $i$ th agent is represented as:

$$\varepsilon_i = \frac{\omega_P \varepsilon_{P_i} + \omega_Q \varepsilon_{Q_i}}{\omega_P + \omega_Q}, \quad (14)$$

where

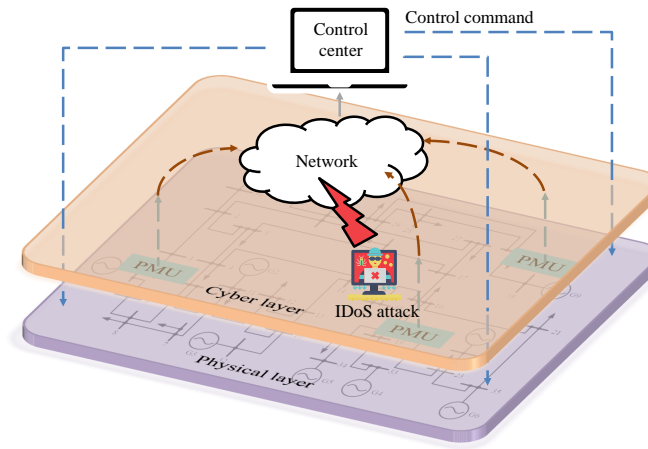
$$\begin{aligned} \omega_P &= \left( \sum_{i=1}^n e^{-\varepsilon'_{P_i}} \log e^{-\varepsilon'_{P_i}} \right) \sum_{m=1}^n \frac{\varepsilon'_{P_m} r_m(\varepsilon'_P, \varepsilon'_Q)}{\sum_{l=1}^n \varepsilon'_{P_l}}, \\ \omega_Q &= \left( \sum_{i=1}^n e^{-\varepsilon'_{Q_i}} \log e^{-\varepsilon'_{Q_i}} \right) \sum_{m=1}^n \frac{\varepsilon'_{Q_m} r_m(\varepsilon'_P, \varepsilon'_Q)}{\sum_{l=1}^n \varepsilon'_{Q_l}}. \end{aligned} \quad (15)$$

**Remark 1** Current methods for calculating voltage sensitivity necessitate power system topology, parameters, voltage, and power outputs to derive variations<sup>[22–24]</sup>, as demonstrated by:

$$\Delta V_\xi = \Delta Q_i \varepsilon_{Q_i} + \Delta P_i \varepsilon_{P_i},$$

where  $\Delta V_\xi$  denotes the voltage change at the  $\xi$ th agent, and  $\Delta Q_i$  and  $\Delta P_i$  represent changes in reactive and active power at the  $i$ th agent, respectively. However, from an attacker's viewpoint, obtaining the system state information requires prolonged eavesdropping on the control center, posing significant challenges. Conversely, our proposed voltage sensitivity calculation method only requires obtaining the power system's topology and rated parameters, enhancing practicality and feasibility.

**Remark 2** To obtain the sensitive information, an enhanced entropy-based weighting method is employed. Traditional entropy-based approaches<sup>[25,26]</sup> primarily address data uncertainty while disregarding inter-data



**Figure 1.** IDoS attack scheme. IDoS: Importance-driven denial of service.

relationships, which can lead to inaccuracies in weighting calculations. To overcome this limitation, this paper introduces exponential entropy and the Pearson correlation coefficient to respectively capture relationships among data and between active and reactive power, thereby enhancing the efficiency of comprehensive information utilization.

### 3.2 IDoS attack strategy design

By leveraging the sensitivity of each agent obtained previously, this section proposes a novel IDoS attack that allocates more attack energy to the important packets transmitted by highly sensitive agents, potentially causing greater disruption.

An experienced attacker targets the network channels between PMUs and control centers [Figure 1]; we can make the following assumptions about the capabilities of the attacker:

**Assumption 1** (1) The attacker can access the topology of the power system to calculate the voltage sensitivity of the  $\xi$ th agent to each agent, forming a subset  $\mathcal{S} = \{\varepsilon_{\xi_1}, \dots, \varepsilon_{\xi_\eta}\}$ , where  $\varepsilon_{\xi_1} > \dots > \varepsilon_{\xi_\eta}$  and  $1 \leq \eta \leq n$ . It is evident that the  $\xi$ th agent exhibits the highest sensitivity to the  $\xi_1$ th agent; (2) The attacker can eavesdrop on output packets and retain the latest non-attack packets.

**Remark 1** In contrast to [27–29], the attack strategy proposed in this paper does not require attackers to obtain hard-to-access information, such as real-time state values or control gains. This enhances the feasibility of Assumption 1.

Based on the aforementioned assumptions, attackers operate according to the following attack mechanism:

$$\varsigma_i(k) = \begin{cases} 1, & \text{if } \vartheta_i(k) > 0; \\ 0, & \text{otherwise,} \end{cases} \quad (16)$$

where

$$\vartheta_i(k) = \|z_i(k) - z_i(k)\|^2 - \frac{\rho}{\varepsilon_{\xi_i}} \|z_i(k)\|^2, \quad \varepsilon_{\xi_i} \in \mathcal{S}, \quad (17)$$

in which  $\rho > 0$  represents the attack parameter, determined by the attacker to adjust the attack frequency.  $z_i(k)$  stands for the output data of the  $i$ th agent, and  $z_i(k)$  denotes the most recently received non-attack packet.

When  $\varsigma_i(k) = 1$ , it indicates that the attacker initiates an attack on the  $i$ th agent at time  $k$ . As a result, the



packet  $z_i(k)$  is attacked, rendering it inaccessible to the estimator. Conversely, when  $\varsigma_i(k) = 0$ , it signifies the absence of attacks, leading to the update of the most recent non-attack packet as  $z_i(k_t) = z_i(k)$ .

**Remark 2** The IDoS attack model Equation (16) distinctly illustrates the correlation between attack behavior and the output packets  $z_i(k)$ ,  $z_i(k_t)$ , voltage sensitivity  $\varepsilon_{\xi_i}$ , and attack parameter  $\rho$ . However, the variables  $z_i(k)$ ,  $z_i(k_t)$ , and  $\varepsilon_{\xi_i}$  are beyond the attacker's control. The attacker can adjust the attack frequency by manipulating the attack parameter  $\rho$ . When faced with energy constraints, increasing the attack parameter  $\rho$  enables the attacker to reduce attack instances, thus lowering energy consumption. Fundamentally, the proposed IDoS attack model effectively integrates voltage sensitivity, packet importance, and energy constraints.

**Remark 3** The proposed IDoS attack strategy is inspired by the event-triggered mechanism, where only significant data packets are transmitted. Similarly, the attack model Equation (16) targets only important data packets. A higher value of  $\vartheta_i(k)$  indicates that the data packet  $z_i(k)$  is more important, and attacking this packet can cause greater harm. Despite these similarities, there are notable differences between the two. The widely used event-triggered mechanism<sup>[30]</sup> is defined as:

$$\bar{\vartheta}(\cdot) = (z(k_t) - z(k))^T \Psi(y(k_z) - y(k)) - \bar{\rho} z^T(k) \Psi z(k),$$

where  $\bar{\rho}$  is the trigger threshold parameter, and  $\Psi$  is the weighting matrix to be designed. In contrast, the IDoS attack model Equation (16) only requires the attacker to determine the attack parameter  $\rho$ .

**Remark 4** In reality, power systems typically encompass numerous agents. When attack energy remains constant, evenly distributing it across each agent leads to energy dispersion, thereby diminishing the attack's impact. Hence, the attack strategy proposed in this paper concentrates the attack energy on the most sensitive subset of agents, denoted as  $\mathcal{S}$ . The size of this subset, denoted by  $\eta$  ( $1 < \eta < n$ ), is determined by the attacker based on their attack resources and technical proficiency. Specifically, when  $\eta = 1$ , the attacker targets important packets solely on the most sensitive agent, whereas with  $\eta = n$ , the attacker simultaneously targets important packets across all agents.

#### 4. EXPERIMENTAL SIMULATION RESULTS

To validate the disruptive potential of the proposed IDoS attack strategy, this section conducts simulation experiments on the IEEE 39-Bus system [Figure 2]. Firstly, the experiment explores the relationship between the attack parameter  $\rho$  and the number of attacks, enabling attackers to set appropriate attack parameters based on the available attack energy. Secondly, the proposed IDoS attack strategy is compared with two traditional DoS attack strategies and DoS attack strategies that consider only partial importance information, thereby verifying the effectiveness of the proposed IDoS attack.

Without loss of generality, Bus 16 is designated as the target agent. Using Equation (14), we obtain the voltage sensitivity of each agent as shown in Table 1. Setting  $\eta = 4$ ,  $\epsilon(k) = 3 \exp(-k) \sin(k)$ , the four agents with the highest sensitivity are Bus 16, Bus 19, Bus 21, and Bus 17, i.e.,  $\mathcal{S} = \{0.4432, 0.1413, 0.1248, 0.1179\}$ . To better reflect the destructiveness of the attack, we define the cumulative error as  $J = \sum_k \gamma(k)$ .

According to the attack model Equation (16), the relationship between the attack parameter  $\rho$  and the number of attacks on each sensitive agent can be observed as depicted in Figure 3. It can be inferred that as  $\rho$  increases, the number of attacks on each sensitive agent decreases. Thus, attackers can adjust  $\rho$  based on the allowable attack times determined by attack energy. Additionally, agents with higher sensitivity are allocated more attack energy/times. For the sake of generality, in this experiment,  $\rho$  is set to 0.8. Within the sampling time period  $[0, 40]$ , the attack instances and intervals for these four agents are illustrated in Figure 4. From this, the total number of attacks is calculated to be 95.



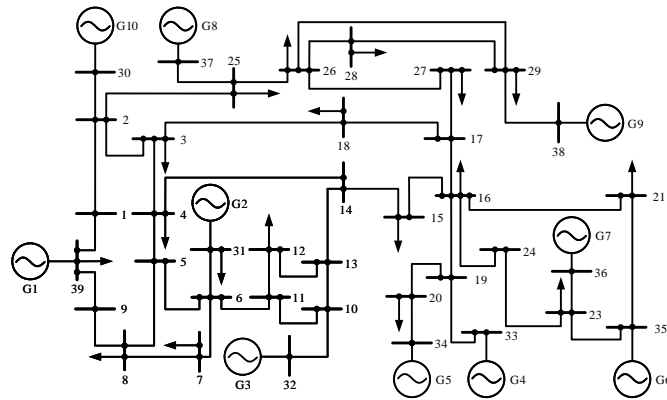
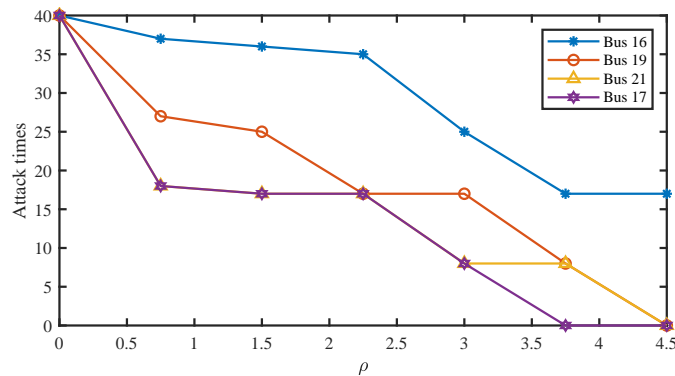


Figure 2. IEEE 39-Bus system.

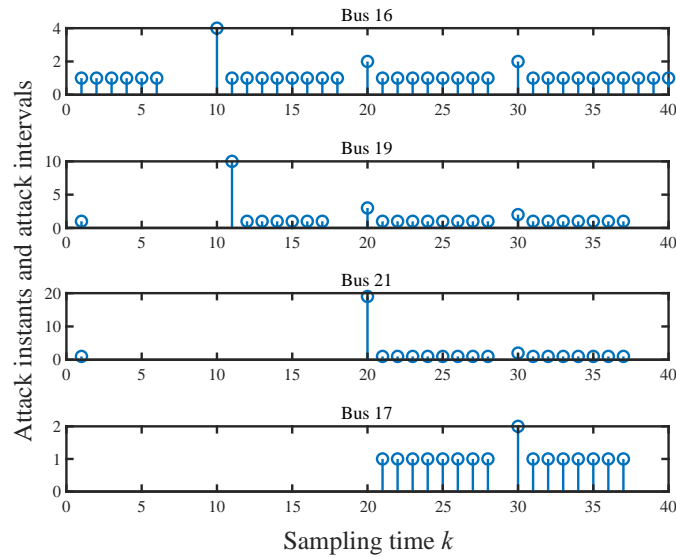
Table 1. Sensitivity for each Bus

Bus 1 0.0017	Bus 2 0.0008	Bus 3 0.0012	Bus 4 0.0006	Bus 5 0.0008	Bus 6 0.0008	Bus 7 0.0052	Bus 8 0.0005	Bus 9 0.0013	Bus 10 0.0009	Bus 11 0.0009	Bus 12 0.0069	Bus 13 0.0009
Bus 14 0.0008	Bus 15 0.0589	Bus 16 0.4432	Bus 17 0.1179	Bus 18 0.0037	Bus 19 0.1413	Bus 20 0.0004	Bus 21 0.1248	Bus 22 0.0009	Bus 23 0.0032	Bus 24 0.0437	Bus 25 0.0035	Bus 26 0.0027
Bus 27 0.0020	Bus 28 0.0208	Bus 29 0.0018	Bus 30 0.0003	Bus 31 0.0002	Bus 32 0.0002	Bus 33 0.0002	Bus 34 0.0002	Bus 35 0.0002	Bus 36 0.0002	Bus 37 0.0002	Bus 38 0.0002	Bus 39 0.0060

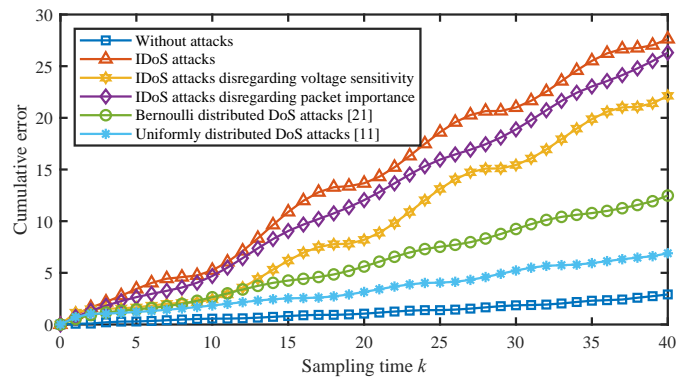
Figure 3. The relationship between  $\rho$  and attack times.

To ensure the effectiveness of the comparative experiments, we maintain an equal total number of attacks launched by different attack models within the same time frame. The attack models being compared are as follows:

- (1) Model 1: The attacker launches IDoS attacks, with the timing of the attacks determined by the proposed model Equation (16).
- (2) Model 2: The attacker employs IDoS attacks without considering voltage sensitivity, with the timing determined by the proposed model Equation (16), where  $\varepsilon_{\xi_1} = \varepsilon_{\xi_2} = \varepsilon_{\xi_3} = \varepsilon_{\xi_4} = 0.25$ .
- (3) Model 3: The attacker executes IDoS attacks without considering packet importance. The attack probabilities for Bus 16, Bus 19, Bus 21, and Bus 17 are set to 0.875, 0.625, 0.45, and 0.425, respectively.
- (4) Model 4: The attacker initiates Bernoulli distributed DoS attacks<sup>[21]</sup>, with the timing of attacks adhering to the Bernoulli parameter. The attack probability within the time range  $[0, 40]$  is set to 0.5938.
- (5) Model 5: The attacker employs uniformly distributed DoS attacks<sup>[11]</sup>, with the timing of attacks evenly



**Figure 4.** IDoS attack instants and attack intervals. IDoS: Importance-driven denial of service.



**Figure 5.** Cumulative error under various attack models.

distributed.

Due to the stochastic nature of the aforementioned attack models, this study conducts 500 experiments for each model. The average results from these experiments serve as the evaluation standard, ensuring that the conclusions drawn are statistically significant and reliable.

Under different attack models, the cumulative error of Bus 16 is illustrated in Figure 5. Upon observation, several trends become apparent: Firstly, the first three IDoS models noticeably outperform the others. This indicates that even without the full sophistication of considering both voltage sensitivity and packet importance, IDoS models are more effective at disrupting the system than traditional DoS attacks. Secondly, IDoS attacks that simultaneously consider voltage sensitivity and packet importance are markedly superior to those that neglect either voltage sensitivity or packet importance. This superior performance can be attributed to its comprehensive approach; this dual consideration allows the attacker to maximize the impact by focusing on the most critical points in the system, thereby causing more substantial disruptions. In contrast, Model 2, which uses IDoS attacks but disregards voltage sensitivity, and Model 3, which considers voltage sensitivity but neglects packet importance, both show lower cumulative errors compared to Model 1. This indicates that while considering voltage sensitivity or packet importance individually can improve attack effectiveness,

combining both importance yields the most significant impact. Based on [Figure 5](#), we can conclude that the proposed IDoS attacks comprehensively consider voltage sensitivity and packet importance, allocating more attack energy to important packets on sensitive agents, thus causing greater disruption.

## 5. CONCLUSION

The paper has first introduced a new method for calculating voltage sensitivity, which only requires attackers to have access to the power system's topology and relevant parameters, thereby enhancing its feasibility. Secondly, a novel IDoS attack strategy has been proposed, which simultaneously considers the voltage sensitivity of the target agent to each agent and the importance of packets. This strategy allocates more attack energy to critical packets on sensitive agents. Finally, simulation results have validated that the proposed IDoS attack strategy is more destructive to the target agent compared to other DoS attack strategies.

It should be noted that traditional estimators are no longer effective in providing accurate estimates against the IDoS attack strategy proposed in this paper. Therefore, designing specialized estimators or controllers that can effectively address IDoS attacks will be a key focus of our future research. Additionally, for defenders, attack isolation is an effective method to prevent the spread of disruptions, and this will also be a major area of our future investigation.

## DECLARATIONS

### Authors' contributions

Made substantial contributions to conception and design of the study and performed data analysis and interpretation: Zhao X, Liu G, Li L

Performed data acquisition and provided administrative, technical, and material support: Zhao X, Liu G

### Availability of data and materials

Not applicable.

### Financial support and sponsorship

This work was supported by the National Natural Science Foundation of China (No. 62173231).

### Conflicts of interest

All authors declared that there are no conflicts of interest.

### Ethical approval and consent to participate

Not applicable.

### Consent for publication

Not applicable.

### Copyright

© The Author(s) 2024.

## REFERENCES

1. Qu B, Wang Z, Shen B, Dong H, Zhang X. Secure particle filtering with paillier encryption-decryption scheme: application to multi-machine power grids. *IEEE T Smart Grid* 2024;15:863–73. [DOI](#)
2. Huang R, Li Y. Adversarial attack mitigation strategy for machine learning-based network attack detection model in power system. *IEEE T Smart Grid* 2023;14:2367–76. [DOI](#)

3. Zhou T, Xiahou K, Zhang LL, Wu QH. Real-time detection of cyber-physical false data injection attacks on power systems. *IEEE Trans Ind Inf* 2021;17:6810–9. [DOI](#)
4. Cheng Z, Yue D, Shen S, Hu S, Chen L. Secure frequency control of hybrid power system under DoS attacks via lie algebra. *IEEE T Inf Foren Sec* 2022;17:1172–84. [DOI](#)
5. Hu Z, Liu S, Luo W, Wu L. Resilient distributed fuzzy load frequency regulation for power systems under cross-layer random denial-of-service attacks. *IEEE Trans Cybern* 2022;52:2396–406. [DOI](#)
6. Zhang Y, Peng C, Xie S, Du X. Deterministic network calculus-based  $H_\infty$  load frequency control of multiarea power systems under malicious DoS attacks. *IEEE T Smart Grid* 2022;13:1542–54. [DOI](#)
7. Yan S, Gu Z, Park JH, Xie X, Sun W. Distributed cooperative voltage control of networked islanded microgrid via proportional-integral observer. *IEEE T Smart Grid* 2024. [DOI](#)
8. Wang X, Guang W, Huang T, Kurths J. Optimized adaptive finite-time consensus control for stochastic nonlinear multiagent systems with non-affine nonlinear faults. *IEEE Trans Autom Sci Eng* 2023;1-12. [DOI](#)
9. Xiao S, Ge X, Ding L, Yue D. A bandwidth-conscious event-based control approach to secondary frequency regulation under vehicle-to-grid service. *IEEE T Smart Grid* 2024;15:3739–50. [DOI](#)
10. Xiao S, Ge X, Han QL, Zhang Y. Secure and collision-free multi-platoon control of automated vehicles under data falsification attacks. *Automatica* 2022;145:110531. [DOI](#)
11. Zhang H, Cheng P, Shi L, Chen J. Optimal denial-of-service attack scheduling with energy constraint. *IEEE T Automat Contr* 2015;60:3023–8. [DOI](#)
12. Qin J, Li M, Shi L, Yu X. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. *IEEE T Automat Contr* 2018;63:1648–63. [DOI](#)
13. Zhang Y, Du L, Lewis FL. Stochastic DoS attack allocation against collaborative estimation in sensor networks. *IEEE/CAA J Autom Sin* 2020;7:1225–34. [DOI](#)
14. Liu R, Hao F, Yu H. Optimal SINR-based DoS attack scheduling for remote state estimation via adaptive dynamic programming approach. *IEEE Trans Syst Man Cybern* 2021;51:7622–32. [DOI](#)
15. Zhang H, Qi Y, Wu J, Fu L, He L. DoS attack energy management against remote state estimation. *IEEE Trans Control Network Syst* 2018;5:383–94. [DOI](#)
16. Zhang XG, Yang GH. Optimal sensor attacks in cyber-physical systems with round-robin protocol. *Inf Sci* 2021;548:85–100. [DOI](#)
17. Zhang J, Sun J, Lin H. Optimal DoS attack schedules on remote state estimation under multi-sensor round-robin protocol. *Automatica* 2021;127:109517. [DOI](#)
18. Zhang J, Sun J. Optimal cooperative multiple-attackers scheduling against remote state estimation of cyber-physical systems. *Syst Control Lett* 2020;144:104771. [DOI](#)
19. Tian E, Chen H, Wang C, Wang L. Security-ensured state of charge estimation of lithium-ion batteries subject to malicious attacks. *IEEE T Smart Grid* 2023;14:2250–61. [DOI](#)
20. Zhu D, Wang H, Wang R, Duan J, Bai J. Identification of key nodes in a power grid based on modified PageRank algorithm. *Energies* 2022;15:797. [DOI](#)
21. Wang X, Tian E, Zheng WX, Xie X. Important-data-based DoS attack mechanism and resilient  $H_\infty$  filter design for networked T-S fuzzy systems. *IEEE Trans Cybern* 2024;54:3352-62. [DOI](#)
22. Kumar R JR, Natarajan B, Pahwa A. Neumann series based voltage sensitivity analysis for three phase distribution system. *IEEE Trans Power Syst* 2022;37:3145–8. [DOI](#)
23. Chang JW, Kang M, Oh S. Data-driven estimation of voltage-to-power sensitivities considering their mutual dependency in medium voltage distribution networks. *IEEE Trans Power Syst* 2022;37:3173–6. [DOI](#)
24. Liu JH, Li ZH. Distributed voltage security enhancement using measurement-based voltage sensitivities. *IEEE Trans Power Syst* 2024;39:836–49. [DOI](#)
25. Xie B, Chen W, Zhou Q, Du J, Cui L. Partition of the development stage of air-gap discharge in oil-paper insulation based on wavelet packet energy entropy. *IEEE T Dielect El In* 2016;23:866–72. [DOI](#)
26. Bian Q, Qiu Y, Wu W, Xin H, Fu X. Generation dispatch method based on maximum entropy principle for power systems with high penetration of wind power. *J Mod Power Syst Clean Energy* 2018;6:1213–22. [DOI](#)
27. Zhao Z, Huang Y, Zhen Z, Li Y. Data-driven false data-injection attack design and detection in cyber-physical systems. *IEEE Trans Cybern* 2021;51:6179–87. [DOI](#)
28. Liu C, He W, Deng R, Tian YC, Du W. False-data-injection-enabled network parameter modifications in power systems: attack and detection. *IEEE Trans Ind Inf* 2023;19:177–88. [DOI](#)
29. Liu C, Liang H, Chen T. Network parameter coordinated false data injection attacks against power system AC state estimation. *IEEE T Smart Grid* 2021;12:1626–39. [DOI](#)
30. Yue D, Tian E, Han QL. A delay system method for designing event-triggered controllers of networked control systems. *IEEE Trans Automat Contr* 2013;58:475–81. [DOI](#)