Chinese Journal of Information Fusion
http://dx.doi.org/10.62762/CJIF.2025.922221

RESEARCH ARTICLE

Sequential Information Fusion for Resilient Estimation: Dynamic Observation Scheduling against Intermittent DoS Attacks

Jie Lu[1,2], **Wenhao Lin**[1,2] **and Chao Yang**[1,2,*]

[1] Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, Shanghai 200237, China
[2] Department of Automation, School of Information Science and Engineering, East China University of Science and Technology, Shanghai 200237, China

Abstract

In this paper, we consider the state estimation problem in a cyber-physical system (CPS) against intermittent denial-of-service (DoS) attacks, which are usually difficult to defend due to their concealment and unpredictability. To address this issue, this paper proposes a dynamic observation scheduling method based on Fisher information to achieve efficient and resilient state estimation. Specifically, a sliding window mechanism is first employed to predict the successful transmission probability for each time window. Subsequently, the method constructs a scheduling sequence by aligning these predicted probabilities with the Fisher information of the observation's components. This strategy effectively achieves the co-optimization of message quality and transmission risk. Theoretical analysis shows that the scheduling method can be viewed as a risk-avoidance weighted maximization problem, which can achieve single-step optimality through same-direction matching. Simulations compare the proposed approach with fixed-order and random scheduling strategies. The results show that the proposed algorithm significantly improves the estimation accuracy under standard attacks and maintains effective estimation even under extreme attacks.

Keywords: dynamic observation scheduling, fisher information, information fusion, intermittent DoS attacks.

1 Introduction

In modern cyber-physical systems, state estimation serves as a core component for enabling closed-loop control based on sensing and decision-making. It is widely applied in autonomous driving, the Industrial Internet of Things (IIoT), robotic systems, smart grids, and other domains [1–3]. With the advancement of multi-sensor integration and information fusion technologies, state estimators often depend on heterogeneous observations from multiple sensors [4,

Academic Editor:
Jiayi Ma

Submitted: 06 November 2025
Accepted: 09 January 2026
Published: 06 March 2026

Vol. 3, **No.** 1, 2026.
10.62762/CJIF.2025.922221

***Corresponding author:**
✉Chao Yang
yangchao@ecust.edu.cn

Citation
Lu, J., Lin, W., & Yang, C. (2026). Sequential Information Fusion for Resilient Estimation: Dynamic Observation Scheduling against Intermittent DoS Attacks. *Chinese Journal of Information Fusion*, 3(1), 46–61.

5]. They enhance estimation accuracy and system robustness through fusion algorithms, such as Kalman filters and their variants [6, 7]. However, such fusion processes critically depend on reliable communication to transmit high-frequency sensor data from the sensing side to the estimation side [8, 9].

However, in modern applications, networks have become a critical vulnerability in the state estimation process, making them particularly susceptible to cyberattacks [10–13]. DoS attacks are a common type of network attack that primarily blocks the network communication channel between an estimator and an observer, thereby disrupting the estimator's performance [14–17]. DoS attacks primarily take the form of flooding and intermittent attacks. Compared to flooding attacks, intermittent DoS attacks are more stealthy and deceptive, as they selectively and unpredictably block portions of observation data [18, 19]. Intermittent DoS attacks make anomaly detection challenging because they operate in seemingly normal conditions but gradually degrade estimation accuracy or even cause the system to diverge. The unpredictability and concealment of such attacks pose greater challenges to existing estimation algorithms.

In recent years, extensive research efforts have been devoted to defending against DoS attacks in CPSs. Existing defense strategies can be broadly categorized into three main classes: static observation scheduling, encrypted communication, and event-triggered control. In the first category, static observation scheduling methods aim to enhance estimation resilience by predefining sensor–controller communication patterns [20–22]. However, their fixed structure makes them unable to adapt to dynamically varying attack conditions. The second line of defense, encrypted communication, focuses on improving data integrity and confidentiality [23–25]. Yet, its high computational cost severely limits real-time applicability. For example, Lesjak et al. [26] found significant authentication and handshake delays in their experiments with MQTT/TLS, which were higher than the latency requirements of typical real-time control loops on resource-constrained platforms. The third category, event-triggered control mechanisms, attempts to reduce vulnerability by transmitting only essential data updates [27, 28]. For example, resilient event-triggered schemes based on static thresholds or fixed-priority scheduling can tolerate occasional packet losses, as explored in event-triggered control under DoS attacks [29] and in switched systems under multiple attacks [30]. However, most existing event-triggered controls still have limited adaptability to time-varying attack intensity or distribution because they are based on static thresholds or fixed priorities. Moreover, some studies have explored secure cooperative control frameworks. For instance, Wang et al. [31] proposed a distributed output-feedback approach based on local observers and resilient controllers, ensuring uniform ultimate boundedness under switching topologies and intermittent DoS attacks . In summary, although these defense strategies have achieved notable progress, their effectiveness remains limited due to high computational overhead, excessive latency, and insufficient adaptability to dynamic and irregular attack patterns.

Critically, most existing solutions overlook the varying informativeness of observations, meaning that not all sensor data contribute equally to estimation accuracy. In fusion-based architectures, particularly those involving asynchronous transmission of split sub-observations, interference with critical packets can significantly amplify system uncertainty [32]. This highlights the need for a dynamic scheduling mechanism that accounts for both attack modeling and observation informativeness. Such a mechanism can significantly improve the robustness of state estimation in resource-constrained and adversarial environments.

To address the above challenges, we propose a dynamic observation scheduling method that proactively adapts to intermittent DoS attacks while ensuring low-latency performance. The core idea of this work is to dynamically schedule observation transmissions by mapping the most informative sub-packets to time windows with lower attack risk. The informativeness of each observation is quantified using Fisher information, and the scheduling strategy adapts in real time to changes in the estimated communication reliability. This lightweight approach enhances estimation robustness under intermittent DoS attacks while remaining fully compatible with standard Kalman filtering frameworks.

The main contributions of this work are summarized as follows:

1. **A novel single-step optimality criterion for resilient estimation.** Unlike heuristic approaches, we theoretically establish that minimizing the lower bound of estimation error covariance is equivalent to solving a risk-averse weighted maximization problem. We

demonstrate that monotonically aligning the Fisher information weights with the predicted probability of successful transmission guarantees this single-step optimality.

2. **A lightweight scheduling algorithm suitable for edge devices.** We designed a resource-efficient algorithm suitable for edge deployments. By combining a sliding window predictor with a Fisher information-based security threshold, this method achieves resilient estimation performance using only local statistics, making it ideal for resource-constrained edge devices lacking global network state.

3. **A novel layered attack model and sub-packet transmission mechanism.** We design an asynchronous transmission mechanism that splits observations into sub-packets to mitigate complete data loss. This strategy is rigorously evaluated against a novel hierarchical attack model—which combines Markov state transitions with window-level distributions—capturing the temporal correlation and bursty nature of "stealthy" intermittent DoS attacks, providing a rigorous benchmark for defense in dynamic adversarial environments.

The remainder of this paper is organized as follows. Section 2 introduces the system model and formulates the problem. Section 3 details the proposed dynamic observation scheduling algorithm and presents the theoretical analysis. In Section 4, we conducted simulation experiments to test the effectiveness and robustness of the proposed method. Finally, Section 5 concludes the paper and discusses potential directions for future work.

Notations: $\mathbb{Z}_+$ is the set of non-negative integers and $k \in \mathbb{Z}_+$ is the time index. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is the n-dimensional Euclidean space. $\mathbb{S}^n_+$ (and $\mathbb{S}^n_{++}$) is the set of n by n positive semi-definite matrices (and positive definite matrices); when $X \in \mathbb{S}^n_+$ (and $\mathbb{S}^n_{++}$), it is written as $X \geq 0$ (and $X > 0$). $X \geq Y$ if $X - Y \in \mathbb{S}^n_+$. $\boldsymbol{E}(\cdot)$ or $\boldsymbol{E}[\cdot]$ is the expectation of a random variable and $\boldsymbol{E}(\cdot|\cdot)$ or $\boldsymbol{E}[\cdot|\cdot]$ is the conditional expectation. $\mathrm{tr}(\cdot)$ is the trace of a matrix. $X^\top$ is the transpose of the matrix X.

2 Problem Setup

In this section, we propose an asynchronous fusion estimation framework based on heterogeneous sensors under intermittent DoS attacks. At the end of this section, we formally define the problem to be addressed.

2.1 System Model

The system model is illustrated in Figure 1.

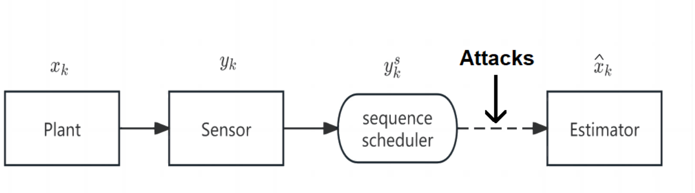


Figure 1. The model structure.

Consider a discrete-time LTI process with the following plant state equation and sensor observation equation:

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

$$y_k = Cx_k + v_k, \tag{2}$$

where $x_k \in \mathbb{R}^n$ is the state of the process, $A \in \mathbb{R}^{n\times n}$ is the state of the process, $w_k \in \mathbb{R}^n$ is the Gaussian white noise with distribution $\mathcal{N}(0, Q)(Q \geq 0)$, $y_k \in \mathbb{R}^p$ is the observation of the current state, $C \in \mathbb{R}^{p\times n}$ is the observation matrix, and $v_k \in \mathbb{R}^p$ is the Gaussian white noise with distribution $\mathcal{N}(0, R)(R > 0)$. The initial condition of the state is assumed as that x_0 is Gaussian with $\mathcal{N}(\bar{x}_0, \Sigma_0)(\Sigma_0 \geq 0)$.

According to the algorithm requirements, the observation $y_k \in \mathbb{R}^p$ is first decomposed into p sub-vectors $y_{k,1}, y_{k,2}, \dots y_{k,p}$, where $y_k = (y_{k,1}^\top \ y_{k,2}^\top \ \dots \ y_{k,p}^\top)^\top$, and then their order is rearranged as $y^s_{k,1}, y^s_{k,2}, \dots y^s_{k,p}$. These sub-vectors $y^s_{k,1}, y^s_{k,2}, \dots y^s_{k,p}$ are then transmitted to the remote estimator sequentially via a communication channel that may be intermittently disrupted by DoS attacks.

The decomposition is taken as follows. Assume that the observation noise components v_i are mutually statistically independent, i.e.,

$$\mathbb{E}\Big[v_i \, v_j^\top\Big] = 0, \quad \forall\, i \neq j, \tag{3}$$

which implies that the overall observation noise covariance matrix is block-diagonal:

$$R = \mathrm{diag}(R_1, R_2, \dots, R_p), \tag{4}$$

where $R_i = \mathbb{E}[v_i \, v_i^\top]$. The sensor observation equation after decomposition can be expressed as

$$\begin{bmatrix} y_{k,1} \\ y_{k,2} \\ \vdots \\ y_{k,p} \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_p \end{bmatrix} x_k + \begin{bmatrix} v_{k,1} \\ v_{k,2} \\ \vdots \\ v_{k,p} \end{bmatrix}.$$

Therefore, the i-th sub-components $y_{k,i}$ can be written as

$$y_{k,i} \quad = \quad C_i x_k + v_{k,i}. \tag{5}$$

The specific reason for decomposing the observation $y_k \in \mathbb{R}^p$ into p sub-vectors $y_{k,i}$ will be explained in detail in the subsequent subsections.

Remark 1. *It is worth noting that the proposed model does not assume identical noise characteristics across different sub-packets. Each observation $y_{k,i}$ is associated with its own noise covariance R_i, i.e.,*

$$v_{k,i} \sim \mathcal{N}(0, R_i),$$

which naturally allows heterogeneous noise levels among sensors.

2.2 Transmission and Estimation Models

In order to enhance the robustness and reconfigurability of state estimation under unreliable communication conditions, the proposed method adopts an asynchronous sub-observation transmission architecture. Specifically, the time interval between steps $k-1$ and k is divided into p time windows, and the sensor observation data is split according to the equation (5) and transmitted independently in these time windows in the form of separate observation data packets. This architecture can not only capture the segmented communication modes commonly seen in practical systems, but also achieve directional scheduling under intermittent DoS attacks or bandwidth limitations.

The binary variable $\gamma_k(j) \in \{0,1\}$ characterizes the transmission status of the j-th time window at time k, defined as:

$$\gamma_k(j) = \begin{cases} 1, & \text{If the transmission succeeds,} \\ 0, & \text{If the transmission fails.} \end{cases} \tag{6}$$

Because the communication outcome of each time window is independent, the overall transmission outcome at time k can be represented as a one-dimensional row vector with p elements, as follows:

$$\gamma_k = [\gamma_k(1),\ \gamma_k(2),\ \ldots\ \gamma_k(p)]. \tag{7}$$

To characterize the stochastic nature of the channel, we define $p_k(j)$ as the success probability of the j-th time window at time k, expressed as:

$$p_k(j) = \Pr(\gamma_k(j) = 1) = \mathbb{E}[\gamma_k(j)]. \tag{8}$$

Assume that in a transmission, there are f elements in the transmission results $\gamma_k(j)$ that equal 1 due to the intermittent DoS attack. This means the estimator successfully receives f packets, denoted as $y^s_{k,1}$, $y^s_{k,2}$, …, $y^s_{k,f}$. Using these available observations, it constructs the observation matrix H_k, the observation vector $\tilde{y}_k$, and the noise covariance matrix $\tilde{R}_k$ for the estimation process, which are defined as follows:

$$H_k = \left(C_1^\top\ C_2^\top\ \ldots,\ C_f^\top\ \right)^\top, \tag{9}$$

$$\tilde{y}_k = \left(y_{k,1}^\top,\ y_{k,2}^\top,\ \ldots,\ y_{k,f}^\top\right)^\top, \tag{10}$$

$$\tilde{R} = \mathrm{diag}(R_1,\ R_2,\ \ldots,\ R_f). \tag{11}$$

After reconstructing the above data H_k, $\tilde{y}_k$, and $\tilde{R}_k$, the estimator will perform Kalman filtering to update the state estimate according to the following steps.

The Kalman filter consists of a prediction step and an update (correction) step.

The estimator first predicts the state based on the information at the previous sub-observation packages, using the formula

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1|k-1}, \tag{12}$$

$$P_{k|k-1} = AP_{k-1|k-1}A^\top + Q, \tag{13}$$

where Q is the process noise covariance matrix defined in equation (1), $\hat{x}_{k|k-1}$ and $P_{k|k-1}$ are the predicted state and error covariance at time k.

After receiving the available sub-observation $\tilde{y}_k$, the estimation is corrected using the formula

$$K_k = P_{k|k-1}H_k^\top(H_k P_{k|k-1}H_k^\top + \tilde{R})^{-1}, \tag{14}$$

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k(\tilde{y}_k - H_k\hat{x}_{k|k-1}), \tag{15}$$

$$P_{k|k} = (I - K_k H_k)P_{k|k-1}, \tag{16}$$

where I is the identity matrix of appropriate dimension, K_k is the Kalman gain, H_k is the observation matrix dynamically constructed based on the sub-observation packets C_i received at time k, and $\tilde{R}$ is the associated observation noise covariance.

2.3 Intermittent DoS Attack Model

Intermittent DoS attacks are time-selective jamming strategies that disrupt communication links during specific intervals, rendering critical observations unavailable [33]. Unlike continuous flooding, these attacks are bursty and deceptive. By aligning brief jamming pulses with critical data transmission windows, attackers can significantly degrade estimator performance while remaining difficult to detect.

To capture the stochastic blocking and dynamic correlation of such attacks, we propose a model that combines the Markov state transition matrix with the Bernoulli attack probability distribution. Let $\mathcal{M} = \{1, \ldots, n\}$ denote a finite set of attack patterns. Each pattern $i \in \mathcal{M}$ represents a distinct attack strategy (e.g., targeting early vs. late windows) and is associated with a vector of window-level attack probabilities:

$$q_{attack}^{(i)} = [q_1^{(i)},\, q_2^{(i)},\, \ldots,\, q_p^{(i)}], \tag{17}$$

Where $q_j^{(i)} \in [0, 1]$ represents the probability of being attacked in the j-th time window under attack pattern i. Therefore, the probability of successful transmission $p_k(j)$ is actually determined by the attack probability $q_j^{(i)}$:

$$p_k(j) = \Pr(\gamma_k(j) = 1) = 1 - q_j^{(i)}. \tag{18}$$

To describe the dynamics of attack strategies, we employ a Markov state transition matrix $P_{\text{trans}} \in \mathbb{R}^{n\times n}$:

$$P_{\text{trans}} = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ P_{n1} & P_{n2} & \cdots & P_{nn} \end{bmatrix}, \tag{19}$$

where P_{ij} represents the transition probability from pattern i to pattern j. The diagonal entries reflect the short-term stability of an attack pattern, while the off-diagonal entries capture the stochastic nature of pattern switching. This design introduces controlled randomness while preserving temporal continuity, providing a more realistic representation of channel reliability than independent Bernoulli models.

Assumption 1. *To facilitate the theoretical analysis, the proposed intermittent DoS attack model relies on the following assumptions:*

1. ***Conditional Bernoulli losses.*** *Under any attack pattern $i \in \mathcal{M}$, the transmission outcomes $\gamma_k(j)$ are independent Bernoulli variables:*

$$\gamma_k(j) \sim \text{Bernoulli}\big(1 - q_j^{(i)}\big), \quad j = 1, \ldots, p.$$

2. ***Measurement independence.*** *As indicated in equation (3), the noise components of the sub-packets are mutually independent.*

3. ***Loss-only attacks.*** *The DoS attack only affects the arrival of data (packet loss) and does not tamper with the data content (integrity is preserved).*

Remark 2. ***Limitations of the Attack Model:*** *The proposed model provides a trade-off between mathematical tractability and practical realism. It effectively captures scripted or semi-intelligent strategies where attackers cyclically use pre-defined interference patterns. However, its representational capability is limited against fully adaptive adversaries employing learning algorithms or historical interactions, as such behaviors violate the Markov property, which we plan to address in future work.*

Remark 3. ***Other applicable scopes of model :*** *It is worth emphasizing that, although the proposed model is primarily formulated to characterize intermittent DoS attacks, it is not restricted to adversarial scenarios. In particular, the model is equally applicable to non-malicious and regularly occurring packet loss phenomena commonly observed in practical engineering systems [34]. For instance, rotating mechanical interfaces (e.g., slip rings in radar systems) and mobile robotic platforms operating in environments with structural occlusions may induce communication channels with quasi-periodic yet stochastic interruption patterns [35]. Such communication behaviors can be effectively captured by the model presented in this section.*

2.4 Problem Statement

In networked estimation systems, sensor measurements contribute unequally to the final accuracy. We decompose the observation data into p sub-packets, where d_j represents the importance weight of the j-th sub-packet (formally defined later in equation (26) as the scalarized Fisher information).These packets are transmitted sequentially over p time windows. Due to intermittent DoS attacks, packet loss may occur. And $\gamma_k(j) \in \{0, 1\}$ represents whether the j-th sub-packet was successfully transmitted at time k.

Therefore, we define the objective optimization function $\mathcal{W}_{k,received}$ as the expectation of the importance of the packets received by the estimator:

$$\mathcal{W}_{k,received} = \sum_{j=1}^{p} \mathbb{E}[\gamma_k(j)] \cdot d_j. \tag{20}$$

Our goal is to maximize $\mathcal{W}_{k,received}$, which means to make the estimator receive the most important data packets as much as possible, thereby improving estimation performance.

3 Dynamic Observation Scheduling

This section introduces the theoretical foundations and core mechanisms of the proposed dynamic observation scheduling algorithm. Firstly, we present the theoretical basis of the algorithm. Then, the detailed form of the algorithm and corresponding pseudocode are described. Finally, we discuss the algorithm's engineering applicability.

3.1 Theoretical Analysis

3.1.1 Fisher Information

To achieve effective scheduling, a metric quantifying the importance of sub-observation packets is essential. We select Fisher Information (FI) as this metric, as it inherently characterizes the contribution of observations to reducing state uncertainty [36, 37].

Fisher information measures the sensitivity of the likelihood function $p(y_k|x_k)$ to the state parameter x_k. Generally, it is defined as:

$$\mathcal{I}(x_k) = \mathbb{E}\left[\left(\frac{\partial \ln p(y_k|x_k)}{\partial x_k}\right)\left(\frac{\partial \ln p(y_k|x_k)}{\partial x_k}\right)^\top\right]. \tag{21}$$

Proposition 1 (Fisher Information for Linear Gaussian Observations)**.** *Consider the linear Gaussian observation model in equation* (2)*:*

$$y_k = Cx_k + v_k, \quad v_k \sim \mathcal{N}(0, R).$$

The Fisher information matrix (FIM) for the state x_k is given by:

$$\mathcal{I}(x_k) = C^\top R^{-1} C. \tag{22}$$

Proof. In the linear Gaussian model, the log-likelihood function implies

$$\frac{\partial \ln p(y_k|x_k)}{\partial x_k} = C^\top R^{-1}(y_k - Cx_k).$$

Substituting this into definition (21) and taking the expectation yields the result directly. □

Equation (22) shows that the Fisher information is proportional to the measurement matrix C and inversely proportional to the noise covariance R.

Remark 4. *According to the Cramér–Rao Lower Bound (CRLB) theorem, the estimation error covariance $P_{k|k} = \mathbb{E}[(\hat{x}_k - x_k)(\hat{x}_k - x_k)^\top]$ is lower-bounded by the inverse of the FIM* [38]*:*

$$P_{k|k} \succeq \mathcal{I}^{-1}(x_k) = (C^\top R^{-1} C)^{-1}, \tag{23}$$

provided that the FIM is invertible. Consequently, maximizing the Fisher information is mathematically equivalent to tightening the lower bound of the estimation error, thereby improving the potential estimation accuracy.

In this paper, the original observation matrix C is decomposed into p submatrices $C_1, C_2, \ldots, C_p$. Similarly, the observation noise covariance matrix R is partitioned into $R_1, R_2, \ldots, R_p$. According to equation (22), the Fisher information contributed by the j-th sub-observation package can be calculated as

$$\mathcal{I}_j = C_j^\top R_j^{-1} C_j. \tag{24}$$

When attacks occur, the *effective* Fisher information of estimator contributed by the j-th sub-packet at time k is defined as

$$\mathcal{I}_k^{\text{eff}}(j) \;=\; \gamma_k(j)\mathcal{I}_j, \tag{25}$$

where $\gamma_k(j)$ is defined in equation (6).

By using the following boundary, we can correlate the expected posterior covariance with the expected Fisher information received by the estimator.

Lemma 1 (Expected CRLB under missing observations)**.** *$P_{k|k-1}$ is the predicted error covariance matrix. We define the predicted information matrix as*

$$Y_{k|k-1} = P_{k|k-1}^{-1}.$$

Under the assumptions above and assuming the matrix $\sum_{j=1}^{p} p_k(j)\mathcal{I}_j$ is invertible ($p_k(j)$ *has already been defined by the equation* (8)*), the mean posterior covariance at time k satisfies*

$$\mathbb{E}[P_{k|k}] \succeq \left(Y_{k|k-1} + \sum_{j=1}^{p} p_k(j)\mathcal{I}_j\right)^{-1}.$$

Proof. Using the information-form Kalman filter, the posterior information matrix can be written as

$$Y_{k|k} = Y_{k|k-1} + \sum_{j=1}^{p} \mathcal{I}_k^{\text{eff}}(j).$$

For *a posterior* update step, the prior information $Y_{k|k-1}$ is known. Taking expectation yields

$$\begin{aligned}\mathbb{E}[Y_{k|k}] &= Y_{k|k-1} + \sum_{j=1}^{p} \mathbb{E}[\mathcal{I}_k^{\text{eff}}(j)] \\ &= Y_{k|k-1} + \sum_{j=1}^{p} \mathbb{E}[\gamma_k(j)]\mathcal{I}_j \\ &= Y_{k|k-1} + \sum_{j=1}^{p} p_k(j)\,\mathcal{I}_j.\end{aligned}$$

By the operator convexity of the matrix inverse (matrix inversion inequality), we have

$$\mathbb{E}[P_{k|k}] = \mathbb{E}[Y_{k|k}^{-1}] \succeq \left(\mathbb{E}[Y_{k|k}]\right)^{-1}$$

Note that $P_{k|k} = Y_{k|k}^{-1}$ and combining the above gives the stated inequality. □

Remark 5. *Observations with higher Fisher information contribute more substantially to reducing the uncertainty of the system state, thereby playing a more important role in the final estimation.*

Based on the FIM, we define the scalar importance weight d_j in equation (20) as:

$$d_j = \operatorname{tr}(C_j^\top R_j^{-1} C_j). \tag{26}$$

It is worth mentioning that this metric naturally accounts for sensor heterogeneity; sensors with larger noise covariance R_j yields a smaller d_j.

3.1.2 *Estimator Acceptance Threshold*

From a long-term statistical perspective, the variation in equation (20) can be analyzed to determine whether the highest-quality sub-observation packets have been subject to intermittent DoS attacks.

Specifically, we introduce an indicator, denoted as $\mathcal{W}_{threshold}$, defined in equation

$$\mathcal{W}_{threshold} = \alpha \cdot \sum_{j=1}^{p} d_j, \tag{27}$$

to evaluate whether the amount of information received by the estimator is insufficient. In equation (27), the parameter $\alpha \in (0,1)$ serves as a tunable factor balancing computational complexity and estimation performance.

To determine whether the most informative sub-observations are being targeted by an intermittent DoS attack, we examine whether the received Fisher information $\mathcal{W}_{k,\text{received}}$, computed via equation (20), satisfies the condition $\mathcal{W}_{k,\text{received}} < \mathcal{W}_{\text{threshold}}$. A sudden drop indicates a potential change in the attacker's strategy, suggesting that the most informative sub-observation packets have been attacked. In such cases, the transmission schedule should be reconfigured promptly.

3.1.3 *Successful Transmission Probability Estimation*

When the total Fisher information received by the estimator falls below a predetermined threshold $\mathcal{W}_{threshold}$, the transmission order must be rescheduled based on the intermittent DoS attack that may occur at the next moment.

Directly predicting intermittent DoS attacks is difficult due to their time-varying and sudden nature. In this paper, to successfully estimate the probability of successful transmission at time $k+1$, we employ a weighted sliding-window method with a length L.

Different from the general average-based method, which assigns equal weights to all L past observations, we introduce a discount factor $r \in (0,1)$ to emphasize more recent attack outcomes. Specifically, the estimated successful transmission probability of the j-th time window at time $k+1$ is computed as

$$\hat{p}_{k+1}(j) = \sum_{i=0}^{L-1} \beta(i) \cdot \gamma_{k-i}(j)\;,\; \beta(i) = \frac{r^i}{\sum\limits_{l=0}^{L-1} r^l}\;, \tag{28}$$

where $\gamma_{k-i}(j) \in \{0,1\}$ denotes the transmission outcome of the j-th time window at time $k-i$ and $\beta(i)$ is the normalized weight. The window length L controls the number of past attack outcomes to consider, while the exponential weights r^i ensure that more recent attack outcomes contribute more significantly to the probability prediction.

Since the estimator primarily focuses on the outcomes of recent attacks while preserving only limited historical attack information, it is reasonable to assume in the algorithm that the predicted transmission success probability $\hat{p}_{k+1}(j)$ approximates the actual transmission success probability $p_{k+1}(j)$ with high accuracy, i.e.,

$$\hat{p}_{k+1}(j) \approx p_{k+1}(j) = \Pr(\gamma_{k+1}(j) = 1). \tag{29}$$

Combining the above equation, the objective expressed by equation (20) becomes

$$\mathcal{W}_{k,received} = \sum_{j=1}^{p} p_k(j) \cdot d_j \approx \sum_{j=1}^{p} \hat{p}_k(j) \cdot d_j. \tag{30}$$

In addition, the two parameters of the estimator, namely the window length L and the discount factor r, have a direct impact on the prediction accuracy. L determines the memory horizon, while r controls the weight decay of past outcomes. Functionally, smaller L and r can enhance the estimator's responsiveness to rapid changes in attack patterns, while larger L and r can produce smoother estimation results during the stable phase of the attack pattern. In practical implementation, these parameters should be tuned to match the expected attack dynamics; for instance, moderate values (e.g., $L = 5, r = 0.5$) offer a balanced trade-off between sensitivity and robustness against typical intermittent patterns.

3.1.4 *Approximate Optimality of Algorithms*

In specific practical scheduling, achieving the globally optimal transmission schedule is not only computationally prohibitive, since the combinatorial search space grows factorially with the number of sub-packets, but also fundamentally intractable due to the uncertainty of future DoS attack patterns.

To address this, the proposed approach formulates a tractable single-step optimization problem based on the Fisher information metric. Specifically, the scheduler prioritizes sub-observation packets according to their Fisher information weights d_j and assigns them to transmission windows with corresponding success probabilities $\hat{p}_k(j)$. The optimization problem is expressed as

$$\max_{\pi_k \in \mathcal{P}} J(\pi_k) = \sum_{j=1}^{p} \hat{p}_k(\pi_k(j)) \ \cdot d_j, \tag{31}$$

where π_k is one permutation of the index sequence $\{$1-2-3-...-$p\}$, which indicates the permuted order from $y_{k,1}$, $y_{k,2}$, $\ldots$, $y_{k,p}$ to $y^s_{k,1}$, $y^s_{k,2}$, $\ldots$, $y^s_{k,p}$, and $\mathcal{P}$ represents the set of all feasible transmission orders. π_k is our optimization variable because different scheduling orders π_k determine different pairing relationships between $\hat{p}_k(j)$ and $\mathcal{P}$.

Theorem 1 (Single-step optimality via exchanging argument). *Consider π to be one permutation of the index sequence, and define the single-step objective as*

$$J(\pi) = \sum_{j=1}^{p} \hat{p}(\pi(j)) \cdot d_j,$$

*where $d_1, \ldots, d_p \geq 0$ are the Fisher information weights of the p sub-packets and $\hat{p}(\pi(1)), \ldots, \hat{p}(\pi(p))$ are the success probabilities of the p transmission windows under the transmission order π. Assume that each $\hat{p}(\pi(j))$ depends only on the time-window index j (i.e., it is independent of which sub-packet is assigned to that window). Then, the optimal order $\pi^* \in P$ is the one that arranges the sequences d_j and $\hat{p}_k(\pi^*(j))$ in the same order which we called **same-direction matching**, i.e.,*

$$\forall u, v \in \{1, \ldots, p\},$$
$$d_u \geq d_v \iff \hat{p}(\pi^*(u)) \geq \hat{p}(\pi^*(v)).$$

Proof. Suppose that there exists an optimal order π^*, which is *not* a same-order matching of the sorted sequences. Without loss of generality, reorder the sub-packet indices so that

$$d_{(1)} \geq d_{(2)} \geq \cdots \geq d_{(p)},$$

and denote the success probabilities sorted in the order by

$$\hat{p}(\pi(1)) \geq \hat{p}(\pi(2)) \geq \cdots \geq \hat{p}(\pi(p)).$$

Since π^* is not a same-order matching, there exist indices $u < v$ such that a larger weight $d_{(u)}$ is assigned (under π^*) to a window with strictly smaller success probability than that of $d_{(v)}$, i.e.

$$d_{(u)} > d_{(v)} \quad \text{but} \quad \hat{p}(\pi^*(u)) < \hat{p}(\pi^*(v)).$$

Construct a new order $\tilde{\pi}$ by swapping the assignments of positions u and v in π^* (leave all other assignments unchanged). The change in objective equals

$$\begin{aligned} J(\tilde{\pi}) - J(\pi^*) &= \big(d_{(u)} \cdot \hat{p}(\pi^*(v)) + d_{(v)} \cdot \hat{p}(\pi^*(u))\big) \\ &\quad - \big(d_{(u)} \cdot \hat{p}(\pi^*(u)) + d_{(v)} \cdot \hat{p}(\pi^*(v))\big) \\ &= \big(\hat{p}(\pi^*(v)) - \hat{p}(\pi^*(u))\big)\big(d_{(u)} - d_{(v)}\big) > 0, \end{aligned}$$

which contradicts the optimality of π^*. Therefore, the same-order matching is optimal. □

These results demonstrate that the proposed scheduling method has a solid theoretical foundation and is not based on purely heuristic or empirical strategies. It is optimal for single-step estimation and ensures the best possible estimator performance even under intermittent DoS attacks.

3.2 Algorithm

We call the method proposed in this paper the Dynamic Observation Scheduling Algorithm, or **DOS** algorithm for short. For clarity, we use bold text to refer to our proposed algorithm as **DOS**, which should be distinguished from "DoS attack" as used in this article to refer to "denial-of-service attack".

Remark 6. *Although the proposed* ***DOS*** *algorithm is primarily designed to address intermittent DoS attacks, it is also applicable to the non-malicious periodic and irregular packet loss scenarios described in Remark 3.*

3.2.1 Core Steps of Algorithm

The core idea of the algorithm is to estimate the transmission success rate based on a sliding window and dynamically configure the mapping between observation sub-packets and transmission time windows, thereby mitigating the loss of key observation data caused by intermittent DoS attacks.

The core of the algorithm consists of three main components:

1. Fisher information weight calculation and threshold judgment;
2. sliding window successful transmission probability estimation;
3. observation redistribution based on information volume and security.

During the initialization phase, the observation is partitioned into p sub-packets as required, and the corresponding Fisher information values d_j for each sub-packet are computed using formula (26). The symbol $\{\pi_k\}$ denotes the transmission order, and the initial transmission order $\{\pi_0\}$ is set to $\{1\text{-}2\text{-}3\text{-}\ldots\text{-}p\}$.

Then the main loop of the algorithm includes the following stages:

Step 1: By monitoring the DoS attack outcomes, the estimator continuously evaluates whether the received Fisher information $\mathcal{W}_{received}$ falls below a predefined threshold $\mathcal{W}_{threshold}$. A significant drop in the received information indicates that one or more high-value observation sub-packets may have been compromised by intermittent DoS attacks.

Step 2: Record the transmission result vector γ_k and update the sliding window. Then, combined with formula (28), estimate the transmission success probability of each time window in the next time $k+1$, expressed as

$$\hat{p}_{k+1} = [\hat{p}_{k+1}(1), \hat{p}_{k+1}(2), \quad \ldots \quad \hat{p}_{k+1}(p)]. \tag{32}$$

Step 3: When the received Fisher information $\mathcal{W}_{k,\text{received}}$ is lower than the predefined threshold $\mathcal{W}_{\text{threshold}}$, the system initiates the remapping strategy, which rearranges both d_j and $\hat{p}_k(\pi_k(j))$ in descending order and matches them pairwise by size. When the received Fisher information $\mathcal{W}_{k,\text{received}}$ is greater than or equal to the predefined threshold $\mathcal{W}_{\text{threshold}}$, it indicates that the amount of received information is sufficient and the transmission order remains unchanged.

3.2.2 Pseudocode Display

The pseudo code reveals the details of this algorithm, as shown in Algorithm 1. The time horizon of the process is assumed to be a finite T.

3.3 Computational Scalability and Practical Implementation

This section evaluates the algorithm's complexity and deployment feasibility on resource-constrained edge devices.

Complexity and Scalability Analysis: The main computations of this algorithm are reflected in the following steps:

(i) Sub-observation package scoring: For each observation sub-packet, its importance is quantified by pre-calculating d_j according to equation (26). The complexity of this step is linearly related to the number of observation sub-packets, i.e., $O(p)$.

(ii) Sequence scheduling: Sort the successful transmission probability $\hat{p}_k(j)$ and the sub-packet importance level d_j, and match them with each other. The time complexity of both is $O(p\ logp)$.

(iii) State update: After receiving the observation packets, the estimator updates its state using a Kalman filter, with a computational complexity of $O(n^3)$. It is worth noting that this complexity is not affected by the number of observation packets p, but is determined solely by the state dimension n.

Therefore, the overall computational complexity per time step is

$$\mathcal{C}(p) = \quad O(n^3) + O(p\ \log p) + O(p),$$

where $O(n^3)$ term is a fixed cost determined solely by the system dynamics.

Thus, the proposed method achieves scalability because the only step whose cost grows with p is a lightweight scoring and ranking process. This makes the algorithm computationally tractable for systems with a large number of observation sub-packets.

Hardware Feasibility & Deployment: For typical edge platforms (e.g., ARM Cortex-M, ESP32), the resource requirements are minimal.

Algorithm 1: Dynamic Observation Scheduling under intermittent DoS Attacks

```
Data: Time horizon $T$, sliding-window length $L$,
      information threshold $\mathcal{W}_{threshold}$ and its
      indicator $\alpha$.
Input: System matrices $A$, $C_i$, $R_i$ (for $i = 1, \ldots, p$),
       initial estimates $\hat{x}_0$, initial error covariance
       $P_0$, initial sequence $\pi_0$.
Output: State estimates $\hat{x}_{1:T}$, estimation error
        covariance $P_{1:T}$, and adaptive sequence
        $\{\pi_k\}$.
for $k = 1$ to $T$ do
    Estimator predict: Estimator compute
      predicted state $\hat{x}_{k|k-1}$ and covariance $P_{k|k-1}$;
    Sender sends observations: The sender
      divides the observation data into $p$ data
      subpackets and sends them in sequence
      according to the sequence $\pi_k$;
    Estimator receives observations: After
      suffering intermittent DoS attacks, the
      estimator collects available sub-observations
      $y_{k,i}$ and attack outcomes $\gamma_k$;
    Successful transmission probability
      estimation: Calculate $\hat{p}_{k+1}(j)$ based on the
      sliding window (refer to equation (28));
    Estimator compute information value:
      Combining the sub-packet weights $d_j$ and the
      transmission results $\gamma_k(j)$, calculate the total
      amount of received Fisher information
      $\mathcal{W}_{k,received}$ (refer to the equation (20));
    if $\mathcal{W}_{k,received} < \mathcal{W}_{threshold}$ then
        Reallocate observations: According to
          Theorem 1, the sending sequence can be
          rearranged to $\pi_k^*$ by monotonically
          aligning $d_j$ and $\hat{p}_k(j)$ by size;
        Update transmission sequence: Set
          $\pi_{k+1} = \pi_k^*$;
    else
        Maintain current sequence: Set
          $\pi_{k+1} = \pi_k$;
    end
    Information Fusion: Compute Kalman gain
      and update state using all successfully
      received sub-observations (refer to equation
      (14),(15),(16)).,
end
```

- *Memory & Processing:* The storage for transmission history is negligible (under 1 KB RAM even for $p = 20$), fitting comfortably within typical SRAM limits (20–320 KB). The sorting logic requires significantly fewer CPU cycles than matrix inversions.
- *Implementation Strategy:* Practical challenges such as packet synchronization can be addressed by adding lightweight headers (e.g., 1-byte sequence IDs). Furthermore, for devices lacking Floating-Point Units (FPU), latency can be minimized by pre-computing the static importance weights d_j offline, reducing online operations to simple lookups.

Owing to its high computational scalability and addressed implementation strategies, the proposed algorithm is well-suited for security-critical applications in domains like industrial IoT and smart manufacturing infrastructure.

4 Simulation Results

This section evaluates the performance of the proposed **DOS** algorithm through numerical simulations. First, the basic experimental parameters are listed and presented in Table 1. Then, we compare the **DOS** algorithm with two common transmission methods to demonstrate its effectiveness. Finally, we examine the algorithm's performance under extreme attack conditions to demonstrate its robustness.

4.1 Experimental Setup and Parameter Configuration

The plant is modeled as a linear discrete-time system. We explicitly list the system dynamics and the baseline observation model parameters in Table 1. In the proposed algorithm, the observation is divided into four sub-packets, which are transmitted individually and are subject to intermittent DoS attacks during communication. Among them, the noise covariance matrix R is configured with distinct variances for each sub-channel to reflect heterogeneous sensor quality.

The performance of the algorithm is evaluated using the mean square error (MSE) of state estimation, allowing for a quantitative comparison of different estimation strategies.

4.1.1 Algorithm Configuration

The **DOS** algorithm relies on three key hyperparameters: the sliding window length L, the discount factor r, and the threshold coefficient α. As listed in Table 1, the baseline values are set to $L = 5$, $r = 0.5$, and $\alpha = 0.5$. The choice of L and r is not arbitrary, but based on the analysis and specific experiments presented in Section 3.1.4.

Table 1. Simulation parameters and configuration.

Parameter	**Value / Definition**
System Dynamics	
State Matrix (A)	1.1
Process Noise (Q)	0.01
Init. State (x_0, P_0)	$1, 1$
Baseline Observation ($p = 4$)	
Obs. Matrix (C)	$[3.0, 2.5, 2.0, 1.5]^\top$
Noise Cov. (R)	$\mathrm{diag}([0.04, 0.08, 0.15, 0.20])^*$
Algorithm Settings	
Window Length (L)	5
Discount Factor (r)	0.5
Threshold Coeff. (α)	0.5
Attack Models	
Attack Patterns ($\mathbf{q}$)	$q_{attack}^{(1)} = [0.9, 0.9, 0.2, 0.1]$ $q_{attack}^{(2)} = [0.2, 0.9, 0.9, 0.1]$ $q_{attack}^{(3)} = [0.1, 0.2, 0.9, 0.9]$
Standard attack	$P_{\text{trans}}^{(\textbf{std})} = \begin{bmatrix} 0.6 & 0.2 & 0.2 \\ 0.2 & 0.6 & 0.2 \\ 0.2 & 0.2 & 0.6 \end{bmatrix}$
Extreme attack	$P_{\text{trans}}^{(\textbf{fast})} = \begin{bmatrix} 0.2 & 0.4 & 0.4 \\ 0.4 & 0.2 & 0.4 \\ 0.4 & 0.4 & 0.2 \end{bmatrix}$

4.1.2 *Attack Scenarios*

We designed three intermittent DoS attack patterns, each targeting different parts of a time window sequence—the early window, the middle window, and the late window. Specific configurations are shown as $q_{attack}^{(1)}$, $q_{attack}^{(2)}$, and $q_{attack}^{(3)}$ in Table 1.

To test the performance of the proposed **DOS** algorithm under both standard and extreme attack scenarios, we designed two different Markov transition matrices:

1. **Standard Attack :** Utilizes transition matrix $P_{\text{trans}}^{(\textbf{std})}$ (see Table 1) with dominant diagonal elements, simulating intermittent DoS attacks that persist in a specific phase for a duration.

   Figure 2 illustrates the pattern switching of a attack, showing that the attack pattern persists for a short period after a random transition.

2. **Extreme Attack :** Introduces a new transition matrix $P_{\text{trans}}^{(\textbf{fast})}$ with low diagonal probabilities 0.2 and high off-diagonal probabilities 0.4. This simulates a highly unstable environment where attack patterns switch rapidly.

   Figure 3 illustrates an extreme attack mode switching scenario. By comparing it with Figure 2, we can see that this mode switching occurs very frequently.

4.2 Comparative Performance under Standard Attack

In this section, we primarily compare the proposed algorithm with two common information transmission mechanisms. One method is to randomly select a time window and send all the information at once. The other method is to split the observations into multiple data packets, but send them in a fixed order, such as 1-2-3-4.

It should be noted that the experimental subjects in this section are all Standard intermittent DoS attack mode. Therefore, the Markov state transition matrix used is $P_{\text{trans}}^{(\textbf{std})}$ in Table 1.

4.2.1 *Unsplit Observation and Random Scheduling*

In this set of experiments, the sender selects any time window to transmit all observation data, without splitting the observation vector into p sub-packets. This mechanism reflects a common real-world information transmission method where all system observations are completely exposed to attack. If the selected window is attacked, all observation data will be lost; otherwise, all observation data will be successfully received.

Experimental results show that the proposed algorithm achieves an MSE of 0.0014, whereas the comparison method yields an MSE of 0.0116. This means that the estimation error was reduced by **87.5%** .

Figure 4 shows a comparison of the total amount of Fisher information received by the estimator over time when using the algorithm and when not using the algorithm. As shown in Figure 4, the estimator without the proposed algorithm experiences significant fluctuations in the amount of information received, alternating between full and zero values, indicating that its estimation process is relatively fragile. In contrast, the estimator using the proposed algorithm maintains a more stable and higher level of information, demonstrating stronger robustness.

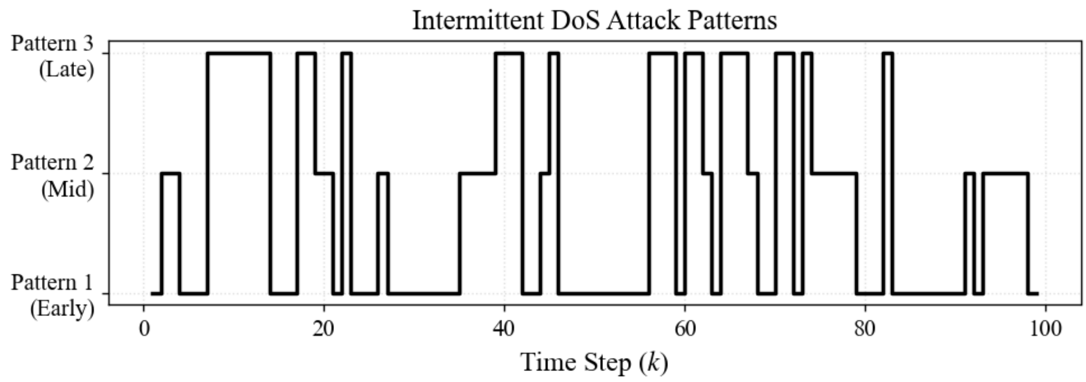


Figure 2. Diagram of the switching patterns of a standard attack.

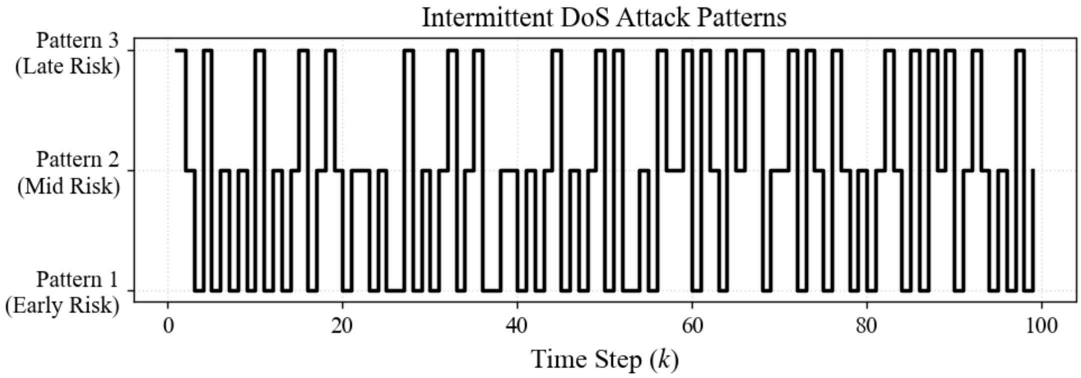


Figure 3. Diagram of the switching patterns of a extreme attack.

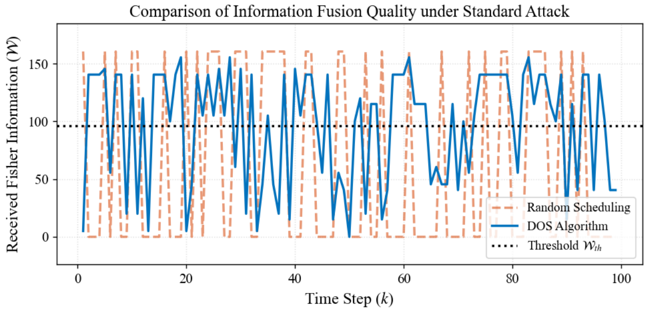


Figure 4. Comparison 1 of Information Fusion Quality under Standard Attack.

4.2.2 *Split Observation and Fixed Sending Order*

In this set of experiments, the sender splits the observation vector into p sub-packets, but regardless of the amount of Fisher information received by the estimator, the sending order remains 1-2-3-4. This mechanism reflects a common information transmission method: reducing the impact of attacks by dividing the data into sub-packets, but failing to predict attacks.

Experimental results show that the proposed algorithm achieves an MSE of 0.0065, whereas the comparison method yields an MSE of 0.0155. This means that the estimation error was reduced by **58.2%**.

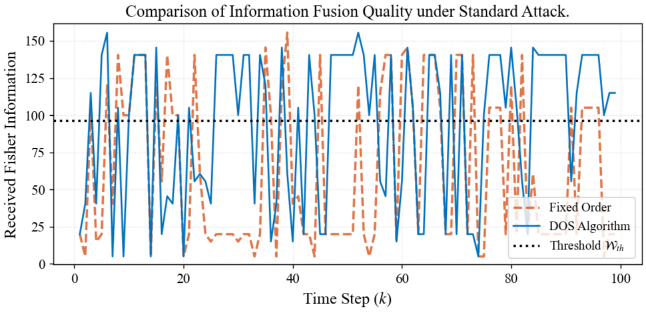


Figure 5. Comparison 2 of Information Fusion Quality under Standard Attack.

Figure 5 shows a comparison of the total amount of Fisher information received by the estimator over time when using the algorithm and when not using the algorithm. It is clear from Figure 5 that when using the **DOS** algorithm, the amount of Fisher information received by the estimator increases significantly and remains relatively stable, which is the reason for the substantial improvement in its estimation accuracy.

4.3 Robustness Analysis against Extreme Attack

This section discusses whether the proposed **DOS** algorithm can still maintain good state estimation performance under extreme attack scenarios (i.e., attack mode changes are very frequent).

The comparison groups used are still "Unsplit Observation and Random Scheduling" and "Split Observation and Fixed Sending Order", but the Markov state transition matrix used is $P_{\text{trans}}^{(\mathbf{fast})}$ in Table 1.

4.3.1 *Unsplit Observation and Random Scheduling*

Experimental results show the proposed algorithm achieves an MSE of 0.0123, whereas the comparison method yields an MSE of 0.0278. This means that the estimation error was reduced by **55.9%** .

Comparing the simulation results under standard attacks (refer to section 4.2.1), we found that the algorithm's performance advantage over the baseline diminished under extreme attack conditions due to more frequent pattern switching, but the estimation accuracy using the proposed method was still markedly superior to the comparison group.

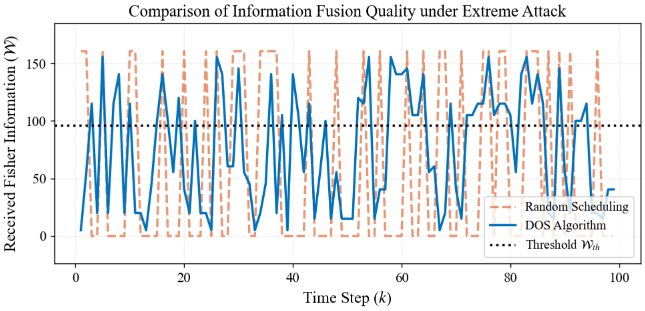


Figure 6. Comparison 1 of Information Fusion Quality under Extreme Attack.

Figure 6 shows a comparison of the total Fisher information received by an estimator using the algorithm versus the "Unsplit Observation and Random Scheduling" method under extreme attack conditions. In Figure 6, the Fisher information received using the algorithm changes less significantly.

4.3.2 *Split Observation and Fixed Sending Order*

Experimental results show that the proposed algorithm achieves an MSE of 0.0085, whereas the comparison method yields an MSE of 0.0102. This means that the estimation error was reduced by **16.7%**.

Comparing the simulation results under standard attacks (refer to section 4.2.2), we found that the algorithm's advantage over the fixed-order strategy was substantially reduced under extreme attack conditions, but the estimation accuracy using the proposed method was still superior to the comparison group.

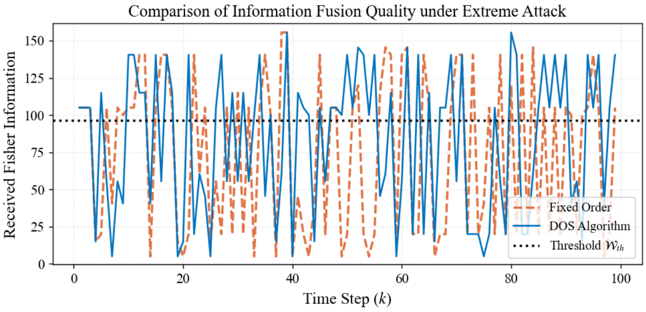


Figure 7. Comparison 2 of Information Fusion Quality under Extreme Attack.

Figure 7 shows a comparison of the total Fisher information received by an estimator using the algorithm versus the "Split Observation and Fixed Sending Order" method under extreme attack conditions. Figure 7 shows that under extreme attack conditions, both sets of Fisher information experienced drastic fluctuations, which is why the estimation accuracy decreased.

4.4 Summary of Simulation Results

The numerical simulations demonstrate that the proposed **DOS** algorithm significantly enhances estimation resilience across varying attack landscapes. Under standard attack patterns, the algorithm outperforms random and fixed scheduling strategies by reducing the Mean Squared Error (MSE) by **87.5%** and **58.2%**, respectively, through efficient Fisher information mapping. It is worth noting that even under extreme attacks with highly frequent attack pattern switching, the algorithm still maintains its superiority, with MSE reduced by **55.9%** and **16.7%** respectively. These results demonstrate that, regardless of whether the attack is standard or extreme, the algorithm ensures that the estimator receives more Fisher information than the general policy, thus verifying the algorithm's robustness and applicability.

5 Conclusion and Future Work

This paper proposes a novel dynamic observation scheduling method that combines the transmission success probability of the transmission window at each moment with the Fisher information weight of the sub-observation packet to address the state estimation challenge under intermittent DoS attacks. The proposed method demonstrates three key advantages: (i) local-statistics-based prioritization that eliminates the need for global state information, (ii) theoretically supported superiority in heterogeneous information fusion, and (iii) Excellent computational scalability and practical applications. Extensive experiments have verified that this method can stably improve the robustness and accuracy of estimation during attacks.

Future work will focus on two strategic directions to further enhance the algorithm's applicability and resilience. First, we aim to extend the proposed framework to time-varying systems by adapting the Fisher information weighting mechanism to accommodate dynamic observation matrices. This extension will allow the scheduler to track physical changes in real-time, ensuring robust estimation even in scenarios with switching topologies or mobile sensors. Second, to address the limitations regarding attack model discussed in Section 2.3, we plan to investigate game-theoretic strategies combined with reinforcement learning. While the current work addresses probabilistic attacks, incorporating reinforcement learning will allow us to model the interaction between the scheduler and an intelligent attacker as a dynamic game. This will prevent intelligent attackers from exploiting deterministic scheduling patterns, thereby securing the system against worst-case scenarios where the attacker possesses inference and adaptation capabilities.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported by the National Natural Science Foundation of China under Grant 62336005.

Conflicts of Interest

The authors declare no conflicts of interest.

AI Use Statement

The authors declare that generative AI tools were used in the preparation of this manuscript. Specifically, ChatGPT-5 and Deepseek-R1 were employed to polish the English writing of several paragraphs. The authors reviewed and edited the content as needed and take full responsibility for the final content of the publication.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Liu, B., Feng, Q., Zhong, L., & Chen, Y. (2025). Physical-information-functional architecture for Internet of Things. *IEEE Internet of Things Journal, 12*(20), 42456–42483. [CrossRef]

[2] Hu, Y., Jia, Q., Yao, Y., Lee, Y., Lee, M., Wang, C., ... & Yu, F. R. (2024). Industrial internet of things intelligence empowering smart manufacturing: A literature review. *IEEE Internet of Things Journal, 11*(11), 19143-19167. [CrossRef]

[3] Packianathan, R., Arumugam, G., Malaiarasan, A., & Natarajan, S. K. (2025). Integrating industrial robotics and internet of things (IoT) in smart transportation system. In *Driving Green Transportation System Through Artificial Intelligence and Automation: Approaches, Technologies and Applications* (pp. 379-395). Cham: Springer Nature Switzerland. [CrossRef]

[4] Sobhiyeh, S., & Naraghi-Pour, M. (2017). Estimation and detection based on correlated observations from a heterogeneous sensor network. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. [CrossRef]

[5] Jung, R., & Weiss, S. (2021). Modular multi-sensor fusion: A collaborative state estimation perspective. *IEEE Robotics and Automation Letters, 6*(4), 6891-6898. [CrossRef]

[6] Trimpe, S., & D'Andrea, R. (2014). Event-based state estimation with variance-based triggering. *IEEE Transactions on Automatic Control, 59*(12), 3266–3281. [CrossRef]

[7] Hespanha, J. P., Naghshtabrizi, P., & Xu, Y. (2007). A survey of recent results in networked control systems. *Proceedings of the IEEE, 95*(1), 138-162. [CrossRef]

[8] Xu, D., Liu, L., Zhang, N., Dong, M., Leung, V. C. M., & Ritcey, J. A. (2023). Nested hash access with post quantum encryption for mission-critical IoT communications. *IEEE Internet of Things Journal, 10*(14), 12204–12218. [CrossRef]

[9] Bai, X., Yan, W., & Ge, S. S. (2021). Distributed task assignment for multiple robots under limited communication range. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52*(7), 4259–4271. [CrossRef]

[10] Yang, C., Yang, W., & Shi, H. (2022). Privacy preservation by local design in cooperative networked control systems. *arXiv preprint arXiv:2207.03904*.

[11] Gao, X., Zhang, D., Bao, W., Zhu, X., & Yan, H. (2020, July). Energy-efficient Cooperative Storage Scheduling for Mobile Edge Cloud under Unstable Communication Conditions. In *2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC)* (pp. 39–42). IEEE. [CrossRef]

[12] Jin, M., Lavaei, J., & Johansson, K. H. (2018). Power grid AC-based state estimation: Vulnerability analysis against cyber attacks. *IEEE Transactions on Automatic*

Control, 64(5), 1784-1799. [CrossRef]

[13] Taha, A. F., Qi, J., Wang, J., & Panchal, J. H. (2016). Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. *IEEE Transactions on Smart Grid, 9*(2), 886-899. [CrossRef]

[14] Sharafian, A., Naeem, H. Y., Ullah, I., Ali, A., Qiu, L., & Bai, X. (2025). Resilience to deception attacks in consensus tracking control of incommensurate fractional-order power systems via adaptive RBF neural network. *Expert Systems with Applications, 270*, 127763. [CrossRef]

[15] Qiu, L., Shao, Z., Dong, L., & Bai, X. (2025). Dual-mode model predictive control for constrained networked control system with DoS attacks and disturbances. *IEEE Transactions on Automation Science and Engineering*. Advance online publication. [CrossRef]

[16] Zhao, N., Shi, P., Xing, W., & Chambers, J. (2020). Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks. *IEEE Transactions on Control of Network Systems, 8*(1), 158-167. [CrossRef]

[17] Yuan, H., Xia, Y., & Yang, H. (2020). Resilient state estimation of cyber-physical system with multichannel transmission under DoS attack. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51*(11), 6926-6937. [CrossRef]

[18] Zhang, Z., Xue, L., Liu, J., & Wu, Y. (2023, August). Aperiodically Intermittent Control for Fixed-Time Stability Under Denial-of-Service Attack. In *2023 38th Youth Academic Annual Conference of Chinese Association of Automation* (*YAC*) (pp. 832-837). IEEE. [CrossRef]

[19] An, L., & Yang, G. H. (2018). Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. *IEEE Transactions on Cybernetics, 49*(3), 827–838. [CrossRef]

[20] Lu, W., Yin, X., Fu, Y., & Gao, Z. (2020). Observer-based event-triggered predictive control for networked control systems under DoS attacks. *Sensors, 20*(23), 6866. [CrossRef]

[21] Wang, Y., Yan, H., Park, J. H., Zhang, H., & Shen, H. (2025). Resilient control of networked control systems with hidden DoS attacks and unknown observation probability. *IEEE Transactions on Control of Network Systems*. [CrossRef]

[22] Wakaiki, M., Cetinkaya, A., & Ishii, H. (2019). Stabilization of networked control systems under DoS attacks and output quantization. *IEEE Transactions on Automatic Control, 65*(8), 3560–3575. [CrossRef]

[23] Farokhi, F., Shames, I., & Batterham, N. (2016). Secure and private cloud-based control using semi-homomorphic encryption. *IFAC-PapersOnLine, 49*(22), 163–168. [CrossRef]

[24] Lin, Y., Farokhi, F., Shames, I., & Nešić, D. (2018, December). Secure control of nonlinear systems using semi-homomorphic encryption. In *2018 IEEE Conference on Decision and Control* (*CDC*) (pp. 5002–5007). IEEE. [CrossRef]

[25] Pan, J., Sui, T., Liu, W., Wang, J., Kong, L., Zhao, Y., & Wei, Z. (2023). Secure control of linear controllers using fully homomorphic encryption. *Applied Sciences, 13*(24), 13071. [CrossRef]

[26] Lesjak, C., Hein, D., Hofmann, M., Maritsch, M., Aldrian, A., Priller, P., ... & Pregartner, G. (2015, July). Securing smart maintenance services: Hardware-security and TLS for MQTT. In *2015 IEEE 13th International Conference on Industrial Informatics* (*INDIN*) (pp. 1243–1250). IEEE. [CrossRef]

[27] Wang, D., Zhang, L., Zhao, N., Liu, Y., & Song, G. (2023, July). Resilient Event-Triggered Control of Networked Markov Jump Systems Under Denial-of-Service Attacks. In *2023 42nd Chinese Control Conference* (*CCC*) (pp. 1131–1136). IEEE. [CrossRef]

[28] Dolk, V. S., Tesi, P., De Persis, C., & Heemels, W. P. M. H. (2016). Event-triggered control systems under denial-of-service attacks. *IEEE Transactions on Control of Network Systems, 4*(1), 93–105. [CrossRef]

[29] Zhao, N., Shi, P., Xing, W., & Lim, C. P. (2021). Event-triggered control for networked systems under denial of service attacks and applications. *IEEE Transactions on Circuits and Systems I: Regular Papers, 69*(2), 811–820. [CrossRef]

[30] Xu, Y., Mu, X., & Cheng, G. (2023). Event-triggered H_∞ control for switched systems under multiple attacks. *International Journal of Control, Automation and Systems, 21*(4), 1089–1097. [CrossRef]

[31] Wang, X., Park, J. H., Liu, H., & Zhang, X. (2020). Cooperative output-feedback secure control of distributed linear cyber-physical systems resist intermittent DoS attacks. *IEEE Transactions on Cybernetics, 51*(10), 4924–4933. [CrossRef]

[32] Freschi, V., & Lattanzi, E. (2019). A study on the impact of packet length on communication in low power wireless sensor networks under interference. *IEEE Internet of Things Journal, 6*(2), 3820-3830. [CrossRef]

[33] Rios, V. D. M., Inácio, P. R. M., Magoni, D., & Freire, M. M. (2022). Detection and mitigation of low-rate denial-of-service attacks: A survey. *IEEE Access, 10*, 76648–76668. [CrossRef]

[34] Cetinkaya, A., Ishii, H., & Hayakawa, T. (2017). Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control, 62*(5), 2434–2449. [CrossRef]

[35] Krejčí, J., Babiuch, M., Suder, J., Krys, V., & Bobovský, Z. (2025). Latency-sensitive wireless communication in dynamically moving robots for urban mobility applications. *Smart Cities, 8*(4), 105. [CrossRef]

[36] Lei, M., Baehr, C., & Del Moral, P. (2010, June). Fisher information matrix-based nonlinear system conversion for state estimation. In *IEEE ICCA 2010*

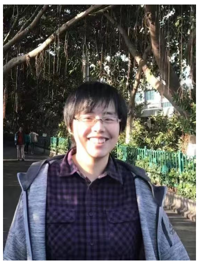
(pp. 837–841). IEEE. [CrossRef]

[37] Ruiz-Gonzalez, M., & Furenlid, L. R. (2015, October). Fisher information analysis of digital pulse timing. In *2015 IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC)* (pp. 1–3). IEEE. [CrossRef]

[38] Huang, J., Gu, K., Wang, Y., Zhang, T., Liang, J., & Luo, S. (2020). Connectivity-based localization in ultra-dense networks: CRLB, theoretical variance, and MLE. *IEEE Access, 8*, 35136–35149. [CrossRef]

Jie Lu received the B.S. degree in Robotics Engineering from Zhejiang University of Science and Technology, Hangzhou, China, in 2024. He is currently pursuing the M.S. degree in Control Science and Engineering at East China University of Science and Technology, Shanghai, China. His research interests include networked control systems and optimal filtering. (Email: y30240982@mail.ecust.edu.cn)

Wenhao Lin received the B.S. degree in Mechanical Design, Manufacturing, and Automation from the East China University of Science and Technology, Shanghai, China, in 2022. He is currently pursuing the Ph.D. degree in Control Science and Engineering at the same university. His research interests include networked control systems, privacy preservation, and optimal filtering. (Email: y12242155@mail.ecust.edu.cn)



Chao Yang received the B.S. degree in theoretical and applied mechanics from the Department of Mechanics and Science Engineering, Peking University, Beijing, China, in 2009 and the Ph.D. degree in electronic and computer engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2013. She is currently an associate professor in the Department of Automation, East China University of Science and Technology, Shanghai, China. Her research interests include optimal estimation in networked control systems, cooperative privacy, and social networks. (Email: yangchao@ecust.edu.cn)