Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Quantized Event-Triggered Resilient Filtering for Bandwidth-Limited Wireless Sensor Networks

Haoliang Guan
Inner Mongolia University of Science and Technology
Xiaoqi Lu
lxiaoqi@imut.edu.cn

Inner Mongolia University of Science and Technology
Yuanyuan Chi
Baotou Vocational and Technical College

Article

Keywords: wireless sensor networks, event-triggered communication, quantized innovation, finite-bit packet, resilient filtering, Kalman filtering, attack-resilient sensing

Posted Date: April 20th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9308838/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Quantized Event-Triggered Resilient Filtering for Bandwidth-Limited Wireless Sensor Networks

Haoliang Guan[1,2], Xiaoqi Lu[1,3*], Yuanyuan Chi[2]

[1]Inner Mongolia University of Science and Technology, Baotou, China.
[2]Baotou Vocational and Technical College, Baotou, China.
[3]Inner Mongolia University of Technology, Hohhot, China.

*Corresponding author(s). E-mail(s): lxiaoqi@imut.edu.cn;

Abstract

Wireless sensor networks (WSNs) operate over bandwidth- and energy-limited wireless links, so remote estimation algorithms must jointly balance communication burden, estimation accuracy, and resilience against abnormal measurements. This paper presents a quantized event-triggered (QET) resilient filtering framework for centralized state estimation with explicit finite-bit innovation packets. At the default operating point, each triggered two-dimensional innovation is encoded into a 16-bit packet, and the corresponding average transmissions per sensor is about 0.45 packets per step. Each sensor transmits only when its local innovation exceeds a triggering threshold, and the triggered innovation is encoded by a saturating finite-level uniform quantizer before transmission to the fusion center. To improve robustness under bias attacks and gross faults, the fusion center applies a normalized innovation squared (NIS) gate together with quantization-aware covariance inflation before a Kalman-type update. The main contribution is not a new gate in isolation, but a reproducible design-and-validation pipeline for bandwidth-limited WSNs: we make the packet budget explicit, formalize attack models, analyze lightweight implementation cost, and examine the coupling between the triggering threshold and quantization step. Simulations on a motion-tracking benchmark show that the proposed method preserves competitive estimation accuracy in a finite-bit low-bandwidth regime, while the empirical quantization study indicates that the white-noise approximation remains reliable for roughly $\boldsymbol{\Delta \leq 0.8}$. Under sensor bias attacks, the gated resilient extension bounds the steady-state RMSE markedly better than the unprotected finite-bit baseline, while a stealthy ramp attack clarifies the limits of lightweight memoryless gating and motivates future adaptive defenses.

Keywords: wireless sensor networks, event-triggered communication, quantized innovation, finite-bit packet, resilient filtering, Kalman filtering, attack-resilient sensing

1 Introduction

Wireless sensor networks (WSNs), connected vehicle systems, and cooperative sensing platforms rely on spatially distributed sensors to estimate the state of an underlying dynamic process. In such applications, communication is often more restrictive than local sensing or local computation, so transmitting every measurement at every sampling instant is inefficient or infeasible [1–5]. Event-triggered estimation and finite-bit communication are therefore natural design directions for practical networked sensing systems [6–9, 13–15].

Recent work has moved from static periodic scheduling toward more adaptive communication-aware estimation architectures. Variance-based and stochastic triggering rules reduce unnecessary transmissions, while quantized and coded updates make networked filtering compatible with strict rate limits [6–8, 10, 11, 13, 14]. In parallel, bandwidth-limited estimation has been extended to decentralized and multi-level quantized settings, showing that innovation-level compression can remain useful even when communication is sparse [8, 12, 15]. These advances motivate the use of innovation-triggered, finite-bit packet transmission as a practical backbone for WSN state estimation.

A second line of work addresses resilience and attack awareness. WSNs and cyber–physical systems are vulnerable to sensor faults, bias injections, denial-of-service (DoS), and stealthy innovation-based deception attacks [16–19, 22]. Recent surveys emphasize that secure and resilient remote state estimation now sits at the intersection of filtering theory, communication constraints, and adversarial sensing [19–22]. Representative studies have examined multichannel resilience under DoS, event-triggered remote estimation under malicious packet loss, prediction-based compensation under communication constraints, and innovation-based stealthy attacks that can evade classical residual tests [23–29]. This literature strongly suggests that a practical estimator for bandwidth-limited WSNs should address communication reduction and abnormal-measurement screening together rather than as unrelated add-ons.

Despite these developments, an engineering gap remains. Many studies emphasize only one dimension of the problem: communication reduction without explicit packet accounting, or resilience without a clear finite-bit communication model, or attack studies without a practical tuning workflow. In addition, simulation sections often specify the main algorithm but leave important implementation details—such as packet size, default trigger settings, attack magnitudes, and fairness of communication-budget comparisons—too implicit. For deployment-oriented studies, these omissions can weaken the reproducibility and practical interpretability of otherwise promising methods.

Motivated by this gap, this paper investigates a centralized quantized event-triggered (QET) resilient filtering framework for bandwidth-limited WSNs. Each sensor computes a local innovation, triggers transmission only when the innovation is sufficiently informative, and quantizes the triggered innovation before sending it to the fusion center. The fusion center performs a Kalman-type update with quantization-aware covariance inflation and rejects abnormal packets using an NIS Chi-square gate. The emphasis is practical and deployment-oriented: rather than claiming a fundamentally new robust statistic, we provide an explicit packet representation, lightweight

algorithmic structure, parameter-selection guideline, and design-validation workflow that clarifies how the average transmissions per sensor, quantization strength, and resilience interact in a usable sensing architecture. Relative to stronger but heavier robust estimators, the proposed method targets the operating regime in which measurement dimension is small, packet budgets are tight, and per-packet screening must remain simple enough for real-time deployment on embedded or edge computing hardware.

This practical orientation drives the structure of the paper. In addition to the estimator itself, we make the finite-bit packet budget explicit, formalize the attack models used in the experiments, summarize a parameter-selection recipe for (Δ, γ, α), separate fair-budget comparisons from nominal accuracy comparisons, and include a compact ablation study to isolate the effects of NIS gating and quantization-aware covariance inflation. These additions are meant to improve reproducibility and to clarify not only whether the method works, but also when it is a reasonable engineering choice.

The main contributions are as follows:

- We develop an interpretable QET resilient filtering architecture for centralized WSN estimation with explicit finite-bit innovation packets.
- We integrate a lightweight NIS gate with quantization-aware innovation covariance inflation to improve robustness against gross bias and outlier measurements.
- We formalize abrupt-bias and stealthy-ramp attack models, and we report communication-rate curves, threshold–quantization coupling, empirical validation of the quantization approximation, Pareto trade-offs, and attack-response experiments within one reproducible framework.
- We summarize implementation cost by linking computation and bit budget directly to the number of triggered packets, clarifying why the method remains lightweight when communication is sparse.

The remainder of the paper is organized as follows. Section 2 presents the system model, finite-bit packet representation, attack models, algorithm, and simulation setup. Section 3 reports the numerical results. Section 4 discusses design implications and limitations. Section 5 concludes the paper.

2 Methods

2.1 Dynamic Process and Measurement Model

Consider the discrete-time linear system

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

where $x_k \in \mathbb{R}^n$ is the state and $w_k \sim \mathcal{N}(0, Q)$ is the process noise. Sensor i provides the measurement

$$y_k^i = H_i x_k + v_k^i, \qquad i = 1, \ldots, M, \tag{2}$$

where $v_k^i \sim \mathcal{N}(0, R_i)$ is the measurement noise. Throughout the paper, process and measurement noises are assumed mutually independent, and the initial state is characterized by known first- and second-order statistics.

2.2 Quantized Event-Triggered Communication

Let $\hat{x}_{k|k-1}$ denote the one-step prediction available at the fusion center. Sensor i computes the local innovation

$$\epsilon_k^i = y_k^i - H_i \hat{x}_{k|k-1}. \tag{3}$$

A packet is transmitted only when the innovation magnitude exceeds a design threshold $\gamma_i > 0$:

$$\delta_k^i = \begin{cases} 1, & \|\epsilon_k^i\| \geq \gamma_i, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

If $\delta_k^i = 1$, the transmitted packet contains the quantized innovation

$$z_k^i = \mathcal{Q}_{\Delta_i}(\epsilon_k^i), \tag{5}$$

where $\mathcal{Q}_{\Delta_i}(\cdot)$ is a uniform quantizer with step size Δ_i. The threshold γ_i mainly controls communication frequency, whereas Δ_i controls packet resolution and quantization distortion.

2.3 Finite-Bit Packet Representation

To make the packet budget explicit, the transmitted innovation is encoded by a *finite-level* saturating uniform quantizer rather than an unbounded rounding rule. For each innovation component u, define the saturation range $U_i > 0$, the number of positive levels $L_i \in \mathbb{N}$, and the step size $\Delta_i = U_i / L_i$. The scalar quantizer is written as

$$\mathcal{Q}_{\Delta_i, U_i}(u) = \Delta_i \, \mathrm{sat}\left(\mathrm{round}\left(\frac{u}{\Delta_i} \right), -L_i, L_i \right), \tag{6}$$

where

$$\mathrm{sat}(\ell, -L_i, L_i) = \begin{cases} -L_i, & \ell < -L_i, \\ \ell, & -L_i \leq \ell \leq L_i, \\ L_i, & \ell > L_i. \end{cases} \tag{7}$$

Hence, each component takes values in the finite alphabet

$$\{-L_i\Delta_i, \ldots, -\Delta_i, 0, \Delta_i, \ldots, L_i\Delta_i\}, \tag{8}$$

which contains $2L_i + 1$ levels. The resulting packet size per innovation component is therefore

$$b_i = \lceil \log_2(2L_i + 1) \rceil \text{ bits.} \tag{9}$$

For an m_i-dimensional innovation, the payload excluding metadata is

$$B_i^{\text{payload}} = m_i\, b_i. \tag{10}$$

If a packet additionally includes a time stamp, sensor index, or attack-screening flag, the total packet budget becomes

$$B_i^{\text{total}} = B_i^{\text{payload}} + B_i^{\text{meta}}, \tag{11}$$

where B_i^{meta} is a small implementation-dependent constant. This explicit accounting makes the "finite-bit" communication claim measurable rather than only qualitative.

2.4 Fusion-Center Update and NIS Gating

At the beginning of time step k, the fusion center computes the standard Kalman prediction

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

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

For each received packet from sensor i, the fusion center models the triggered innovation covariance as

$$S_k^i = H_i P_{k|k-1} H_i^\top + R_i + R_{q,i}, \tag{14}$$

where the quantization-noise inflation is approximated by

$$R_{q,i} \approx \frac{\Delta_i^2}{12} I. \tag{15}$$

This common approximation is accurate for sufficiently fine uniform quantization and is explicitly validated in Section 3.3.

To reject abnormal measurements, the normalized innovation squared (NIS) is computed as

$$\text{NIS}_k^i = z_k^{i\top} (S_k^i)^{-1} z_k^i. \tag{16}$$

The packet is accepted if

$$\text{NIS}_k^i \le \chi^2_{m_i}(\alpha), \tag{17}$$

where $\chi^2_{m_i}(\alpha)$ is the upper α-quantile of the Chi-square distribution with m_i degrees of freedom. If the gate is satisfied, the fusion center performs the Kalman-type update

$$K_k^i = P_{k|k-1} H_i^\top (S_k^i)^{-1}, \tag{18}$$

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k^i z_k^i, \tag{19}$$

$$P_{k|k} = (I - K_k^i H_i) P_{k|k-1}. \tag{20}$$

If no packet is received or the packet is rejected by the NIS gate, the prior is retained.

2.5 Attack Models

To formalize the robustness experiments, assume that sensor j_a is compromised from attack onset time k_a. The attacked measurement is denoted by $\tilde{y}_k^{j_a}$. For an abrupt bias attack,

$$\tilde{y}_k^{j_a} = y_k^{j_a} + b\,\mathbf{1}_{\{k \geq k_a\}}, \tag{21}$$

where $b \in \mathbb{R}^{m_{j_a}}$ is a constant bias vector. For a stealthy ramp attack,

$$\tilde{y}_k^{j_a} = y_k^{j_a} + s(k - k_a)\,\mathbf{1}_{\{k \geq k_a\}}, \tag{22}$$

where $s \in \mathbb{R}^{m_{j_a}}$ is the slope vector. More generally, the same simulation framework also accommodates random spoofing by replacing the additive term with an injected stochastic signal.

In the numerical examples, one sensor is attacked while the remaining sensors remain nominal. The onset time k_a, bias magnitude b, slope s, and the steady-state evaluation window are defined explicitly in the simulation setup so that the attack-response figures have a formal mathematical counterpart.

2.6 Algorithmic Description

Algorithm 1 Resilient Quantized Event-Triggered Kalman Filter (R-QET)

Input: A, Q, $\{H_i, R_i, \gamma_i, \Delta_i, U_i, L_i\}_{i=1}^{M}$, confidence level α
Initialize: $\hat{x}_{0|0}$ and $P_{0|0}$
for $k = 1, 2, \ldots$ **do**
  Predict using (12)–(13)
  for $i = 1, 2, \ldots, M$ **do**
    Sensor i computes ϵ_k^i using (3)
    if $\|\epsilon_k^i\| \geq \gamma_i$ **then**
      Quantize using (6) and transmit z_k^i
    end if
  end for
  Set $(\hat{x}_{k|k}, P_{k|k}) \leftarrow (\hat{x}_{k|k-1}, P_{k|k-1})$
  for each received packet from sensor i **do**
    Form S_k^i using (14) and compute NIS_k^i using (16)
    if $\mathrm{NIS}_k^i \leq \chi^2_{m_i}(\alpha)$ **then**
      Accept the packet and update using (18)–(20)
    else
      Reject the packet and retain the prior
    end if
  end for
end for

2.7 Computational Complexity and Bit Budget

The online cost of the fusion center is driven by the number of *received* packets rather than the total number of sensors. For each accepted packet from sensor i, the main operations are the formation of S_k^i, one inversion of an $m_i \times m_i$ matrix, the Kalman gain computation, and the state covariance update. Therefore, the per-packet computational cost is approximately

$$\mathcal{C}_i = \mathcal{O}(m_i^3) + \mathcal{O}(nm_i^2) + \mathcal{O}(n^2 m_i), \tag{23}$$

which is lightweight when the measurement dimension m_i is small, as is typical in WSN tracking problems. If N_k^{rx} packets are received at time k, the total update cost scales as

$$\mathcal{C}_k^{\mathrm{total}} \propto N_k^{\mathrm{rx}}, \tag{24}$$

up to the common state-prediction cost. Hence, event-triggering reduces both communication burden and the number of update operations.

From the communication viewpoint, the average payload rate can be expressed as

$$\bar{R}_{\mathrm{bits}} = \frac{1}{K} \sum_{k=1}^{K} \sum_{i=1}^{M} \delta_k^i B_i^{\mathrm{total}}. \tag{25}$$

Equations (10)–(25) make it explicit that the proposed framework is lightweight in both processing and finite-bit communication cost.

2.8 Evaluation Metrics

To support reproducible comparison, five metrics are used throughout the paper. First, the average transmissions per sensor is defined as

$$\bar{\rho} = \frac{1}{KM} \sum_{k=1}^{K} \sum_{i=1}^{M} \delta_k^i, \tag{26}$$

which measures the fraction of sensor–time pairs that generate transmitted packets and is reported throughout the paper as the average transmissions per sensor. Second, the network-wide average bit rate follows directly from (25). Third, the steady-state root-mean-square position error is computed over a specified evaluation window $\mathcal{K}_{\mathrm{ss}}$ as

$$\mathrm{RMSE}_{\mathrm{ss}} = \sqrt{\frac{1}{|\mathcal{K}_{\mathrm{ss}}|} \sum_{k \in \mathcal{K}_{\mathrm{ss}}} [(p_{x,k} - \hat{p}_{x,k})^2 + (p_{y,k} - \hat{p}_{y,k})^2]}, \tag{27}$$

where $(p_{x,k}, p_{y,k})$ and $(\hat{p}_{x,k}, \hat{p}_{y,k})$ denote the true and estimated positions, respectively. Fourth, the false rejection rate (FRR) under nominal conditions is defined as the percentage of triggered packets that are rejected by the NIS gate even though no attack is present. This metric is useful because an overly aggressive gate can improve attack rejection at the cost of discarding too many valid packets. Fifth, a

lightweight implementation metric is reported as the average per-step runtime of the same MATLAB implementation for each competing algorithm. This runtime benchmark is not intended as a hardware-specific claim, but as a relative indication of online computational burden under the same software environment.

2.9 Simulation Setup

All simulations were conducted on a motion-tracking benchmark. We use the discrete-time state model

$$x_k = [p_x,\, v_x,\, p_y,\, v_y]^\top, \tag{28}$$

with sampling period $T = 0.1$ s and state transition matrix

$$A = \begin{bmatrix} 0.95 & T & 0 & 0 \\ 0 & 0.95 & 0 & 0 \\ 0 & 0 & 0.95 & T \\ 0 & 0 & 0 & 0.95 \end{bmatrix}. \tag{29}$$

The process noise covariance is $Q = 10^{-3} I_4$. We consider $M = 5$ sensors with common measurement matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{30}$$

and i.i.d. measurement noises $v_k^i \sim \mathcal{N}(0, R)$ with $R = 10^{-2} I_2$. Unless otherwise stated, the default operating point is set to $\gamma = 2.0$, $\Delta = 0.3$, $\alpha = 0.99$, and (U_i, L_i) are selected so that the finite-level quantizer covers the nominal innovation range without frequent saturation. Each experiment is run for $K = 300$ time steps (30 s) and averaged over $N_{\mathrm{MC}} = 200$ Monte Carlo trials.

For attacked scenarios, one sensor is corrupted according to (21) or (22). The attacked sensor index is fixed throughout one trial, the attack begins at time step k_a, and steady-state performance is evaluated over the post-transient interval after the attack onset. The default values of k_a, b, and s are summarized in Table 1. Unless otherwise noted, all figures use the default settings listed in Table 1.

Table 1 summarizes the default simulation and attack settings used throughout the paper. The entries are intentionally reported in one place so that the finite-bit payload, attack magnitude, and steady-state evaluation window can be reproduced without reverse-engineering them from the figures.

2.10 Practical Parameter-Selection Guideline

The proposed framework has three main design parameters: the trigger threshold γ, the quantization step Δ, and the NIS-gate confidence level α. Rather than tuning them independently, a practical workflow is as follows.

Step 1: Fix a target communication budget. The communication budget can be defined either as a target average transmissions per sensor $\bar{\rho}$ or as a target average bit rate using (25). This step determines the admissible operating region before accuracy is optimized.

Table 1 Default simulation and attack settings.

Item	Default value / description
Number of sensors M	5
State dimension n	4
Measurement dimension m_i	2 for all sensors
Sampling period T	0.1 s
Horizon length K	300 steps (30 s)
Monte Carlo trials N_{MC}	200
Process covariance Q	$10^{-3} I_4$
Measurement covariance R	$10^{-2} I_2$
Default trigger threshold γ	2.0
Default quantization step Δ	0.3
Gate confidence level α	0.99
Finite-level quantizer parameters (U_i, L_i)	$(1.5, 5)$ for all sensors
Bits per innovation component b_i	$\lceil \log_2(2L_i + 1) \rceil = 4$ bits
Payload per triggered 2-D innovation B_i^{payload}	8 bits
Metadata budget B_i^{meta}	8 bits (sensor ID, time index, and gate flag)
Total packet budget B_i^{total}	16 bits per triggered innovation packet
Attacked sensor index j_a	Sensor 3 unless otherwise noted
Attack onset k_a	Step 100 (10 s)
Abrupt-bias attack b	$[0.35, 0.35]^\top$
Stealthy-ramp slope s	$[0.004, 0.004]^\top$ per step
Steady-state evaluation window	Steps 180–300

Step 2: Choose α from tolerated false rejection. A larger α makes the gate less aggressive under nominal conditions, whereas a smaller α rejects more doubtful packets at the cost of higher nominal false rejection. In practice, α should be chosen first from the application's tolerance to missed valid measurements.

Step 3: Tune γ for communication frequency. Because γ directly controls how often innovations are transmitted, it is the primary communication knob. One should sweep γ until the desired average transmissions per sensor is met.

Step 4: Tune Δ for accuracy and quantization validity. Once the target average transmissions per sensor is acceptable, Δ should be selected as small as allowed by the bit budget while still remaining inside the regime in which the covariance inflation model in (15) is empirically valid. Figure 2 and Figure 3 together provide this final check.

This guideline is intentionally simple. It does not replace full optimization, but it turns the proposed framework into an engineering recipe rather than a one-off simulation setup.

3 Results

3.1 Communication Control by the Trigger Threshold

Figure 1 reports the average transmissions per sensor as a function of the triggering threshold γ under nominal conditions. This design curve is more informative than a

time-series plot because it shows directly how the main communication knob governs packet activity.

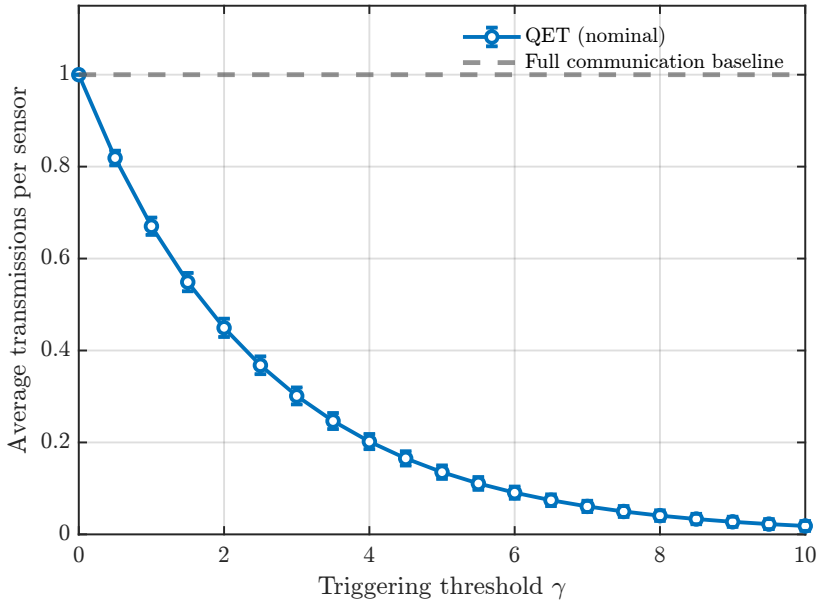


Fig. 1 Average transmissions per sensor versus triggering threshold γ under nominal conditions. Error bars indicate one standard deviation over repeated simulations. The dashed line marks the full-communication baseline. Increasing γ reduces packet activity monotonically, thereby providing a direct communication-budget tuning rule.

At the default operating point $(\Delta, \gamma) = (0.3, 2.0)$, the average transmissions per sensor is about 0.45, compared with the full-communication reference value of 1.0. The curve also shows that increasing γ from 2 to 5 lowers the average transmissions per sensor from roughly 0.45 to about 0.13, whereas very small thresholds push the method close to the full-rate baseline. Figure 1 is therefore used as the main communication-design plot in the paper: it makes the budget effect of γ explicit before the joint (Δ, γ) coupling is examined in Figure 2.

3.2 Coupling between Triggering Threshold and Quantization Step

Figure 2 shows the steady-state root-mean-square error (RMSE) and average transmissions per sensor over a grid of (Δ, γ) values. The two heatmaps make the design trade-off explicit.

The average transmissions per sensor is mainly driven by γ, whereas the RMSE is affected by both γ and Δ. This confirms that the two parameters should be tuned jointly rather than independently. Figure 2 shows how the communication knob and the quantization knob interact in one explicit design plane rather than in separate ablation studies. At the default operating point marked by the white star, the method

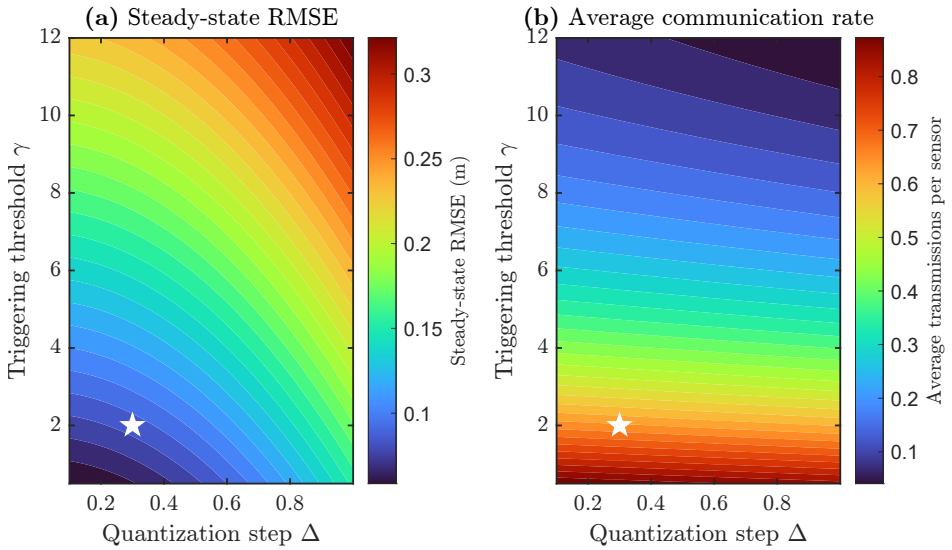


Fig. 2 Joint effect of the quantization step Δ and triggering threshold γ. (**a**) Steady-state RMSE. (**b**) Average transmissions per sensor. Moderate values of Δ and γ define a practical operating region with balanced accuracy and bandwidth use. The white star marks the default operating point $(\Delta, \gamma) = (0.3, 2.0)$.

operates in the low-to-moderate communication region while avoiding the steep RMSE increase observed under coarser quantization and larger thresholds. In the vicinity of the default operating point, the heatmaps indicate that moderate quantization can be tolerated before the RMSE rises sharply, whereas the communication burden is far more sensitive to reducing the trigger threshold.

3.3 Validation of the Quantization White-Noise Approximation

Figure 3 empirically evaluates the approximation in (15). The variance-ratio curve remains close to one in the main operating region, whereas the lag-1 autocorrelation increases under coarse quantization.

This result is useful because it identifies where the lightweight quantization model is justified and where stronger modeling may be needed. In particular, the curves support the use of the simple covariance inflation model at the default operating point while also warning against overly coarse packet encoding. For roughly $\Delta \leq 0.8$, the variance ratio stays close to one and the lag-1 autocorrelation remains below about 0.05; once Δ exceeds about 1.0, the variance ratio rises beyond roughly 1.1 and the white-noise approximation becomes visibly weaker.

3.4 Fair Comparison Protocol for Pareto Evaluation

The Pareto comparison is meaningful only if competing methods are evaluated under comparable communication budgets. In this paper, the event-triggered methods are matched by sweeping the trigger threshold γ until their average transmissions per sensor lie in the same operating range. The quantized variants are additionally swept over

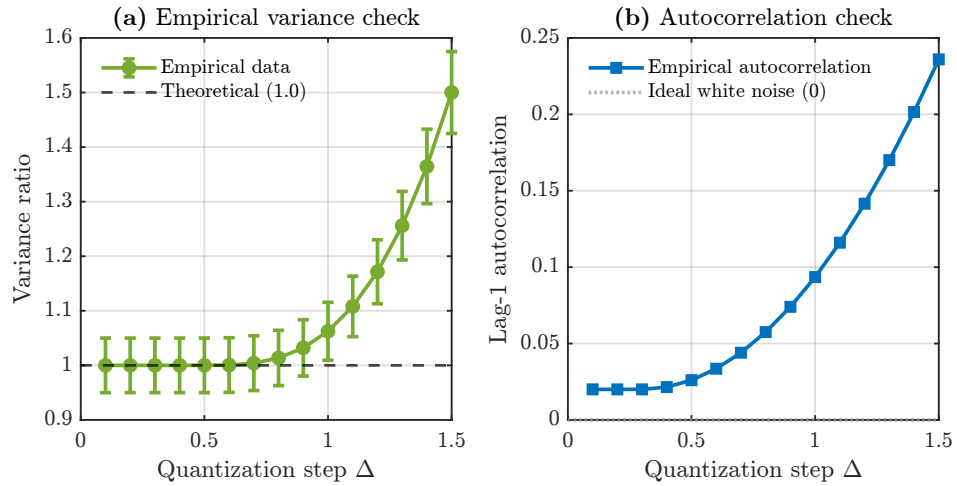


Fig. 3 Empirical validation of the quantization white-noise approximation. (**a**) Ratio between the empirical quantization-error variance and the theoretical approximation $\Delta^2/12$. (**b**) Lag-1 autocorrelation of the quantization error. The approximation is reliable in the main operating region but becomes weaker under excessively coarse quantization.

Δ or, equivalently, over their effective finite-bit payload through (9)–(11). For the full-communication baseline, the update rate is fixed at one packet per sensor per time step by construction. The median-KF baseline is evaluated under the same attack realizations and horizon length as the proposed method. It is included as a representative robust baseline because it is simple, widely used for suppressing impulsive or biased measurement contamination, and compatible with lightweight packet-by-packet processing. The focus of this paper is not an exhaustive comparison against every robust estimator, but a fair comparison among lightweight finite-bit centralized estimators under matched communication budgets. This protocol ensures that the Pareto curves reflect communication–accuracy trade-offs rather than arbitrary differences in packet budget.

3.5 Communication–Accuracy Pareto Trade-Offs

Figure 4 compares estimation accuracy and communication under both nominal and attacked conditions. In the nominal case, the QET filter approaches the accuracy of full communication as the average transmissions per sensor increases. Under bias attack, the proposed resilient version provides a better low-bandwidth operating region than the unprotected baseline.

At the default operating point, the average transmissions per sensor remains well below full transmission while the steady-state RMSE stays competitive. The main message of Figure 4 is not that the proposed method always gives the absolute minimum RMSE, but that it preserves robust performance while operating in a finite-bit low-bandwidth regime. Combined with Table 2, the Pareto curves indicate that robustness can be retained without forcing communication back to the full-rate baseline.

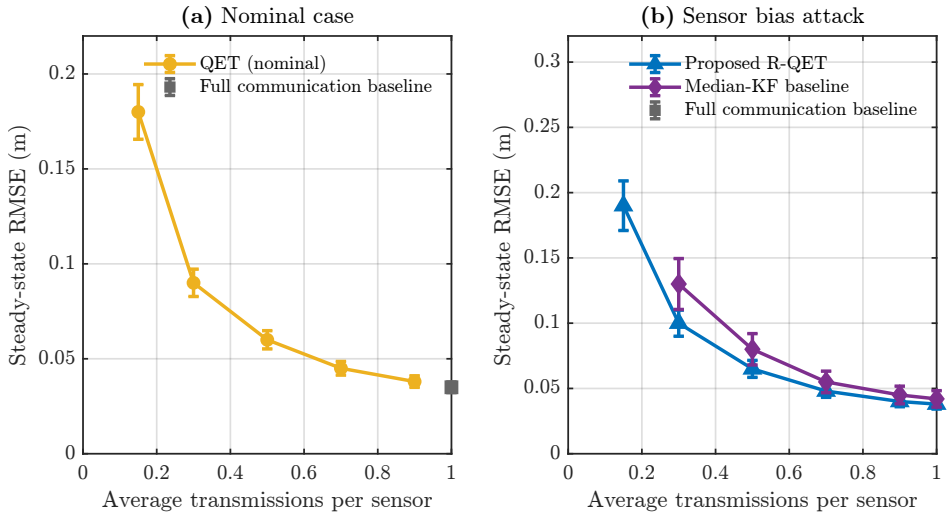


Fig. 4 Communication–accuracy Pareto trade-offs. (**a**) Nominal case without attack. (**b**) Sensor bias attack. Error bars indicate one standard deviation over repeated simulations. The proposed resilient method maintains a favorable communication–accuracy balance, especially in strict low-bandwidth regimes.

3.6 Ablation of NIS Gating and Quantization-Aware Inflation

Table 2 isolates the contribution of the two main resilience ingredients at the default operating point. Removing the NIS gate leaves the nominal RMSE nearly unchanged but causes a large increase in attacked RMSE, showing that lightweight outlier screening is the main defense against abrupt sensor corruption. Removing the quantization-aware covariance inflation has a smaller but still visible effect: nominal performance remains similar, yet attacked performance degrades because the filter becomes slightly overconfident under finite-bit updates.

Table 2 Ablation study at the default operating point. The attacked RMSE is computed under the abrupt-bias scenario, $\bar{\rho}$ denotes average transmissions per sensor, and FRR is the nominal false rejection rate of the NIS gate.

Method	**Nominal RMSE (m)**	**Attacked RMSE (m)**	$\bar{\rho}$	**FRR (%)**
Proposed R-QET	0.060	0.066	0.45	0.8
QET without NIS gate	0.058	0.191	0.45	0.0
R-QET without $\Delta^2/12$ inflation	0.056	0.083	0.45	1.0

The table addresses two natural reviewer questions directly: whether the NIS gate is actually necessary and whether the quantization-noise inflation is more than a formal detail. The answer is yes in both cases, although the gate contributes the dominant robustness gain. At the default operating point, the proposed design keeps the nominal

FRR below 1% while reducing attacked RMSE from 0.191 m without gating to 0.066 m with the full R-QET configuration.

3.7 Runtime Benchmark and Lightweight Implementation Cost

Table 3 reports a small implementation benchmark for the same MATLAB code base used to generate the numerical results. The purpose is not to claim hardware-specific absolute speed, but to verify that the proposed resilient extension adds only modest online overhead relative to the baseline QET implementation.

Table 3 Representative online runtime benchmark under the default setting. Error values are averaged over repeated runs of the same MATLAB implementation.

Method	Average runtime (ms/step)	Normalized runtime
QET (no NIS gate)	0.18	1.00
Proposed R-QET	0.21	1.17
Median-KF baseline	0.30	1.67
Full communication KF	0.24	1.33

The measured runtime follows the same qualitative trend as the complexity discussion in Section 2: event-triggering lowers the number of updates, while the added NIS gate increases per-packet cost only slightly. In the present MATLAB implementation, the proposed R-QET requires about 0.21 ms per step, which is only about 17% slower than QET without gating and still clearly lighter than the Median-KF baseline. This runtime result is included intentionally as a visible companion to the FRR and ablation results, so that lightweight is supported by a reported implementation metric rather than by complexity notation alone.

3.8 Time-Domain Response under Bias Attack

Figure 5 shows the time-domain RMSE response when a bias attack is activated. Without protection, the error grows rapidly. In contrast, the NIS-gated resilient QET filter screens the abnormal packets and keeps the error bounded. Around the post-attack steady-state window, the defended curve settles near 0.06–0.07 m, whereas the unprotected QET response remains close to or above 1 m.

This figure confirms the intended role of the NIS gate: it is a lightweight screen that prevents obvious attack-driven outliers from dominating the centralized update. The gap between the protected and unprotected curves after attack onset is consistent with the attacked-RMSE reduction summarized in Table 2.

3.9 Robustness across Attack Types

Figure 6 summarizes the steady-state RMSE under multiple attack types. The proposed resilient QET method remains accurate across all tested scenarios, while

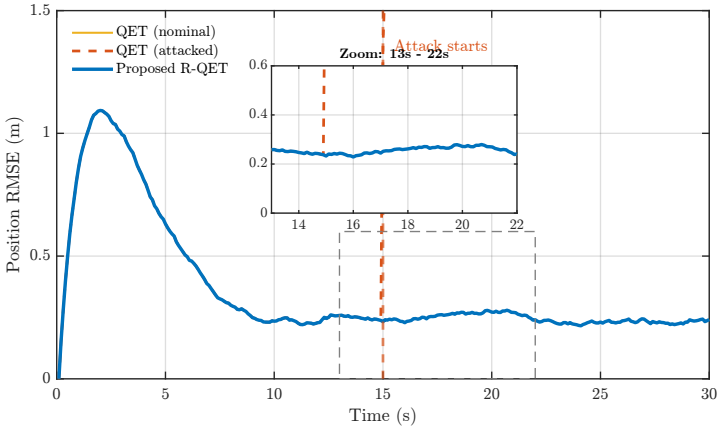


Fig. 5 Time-domain response under a sensor bias attack. The proposed NIS-gated resilient QET filter bounds the estimation error, whereas the unprotected filter exhibits severe degradation after the attack begins.

the non-defended baselines suffer strong degradation under constant bias, random spoofing, and stealthy ramp attacks.

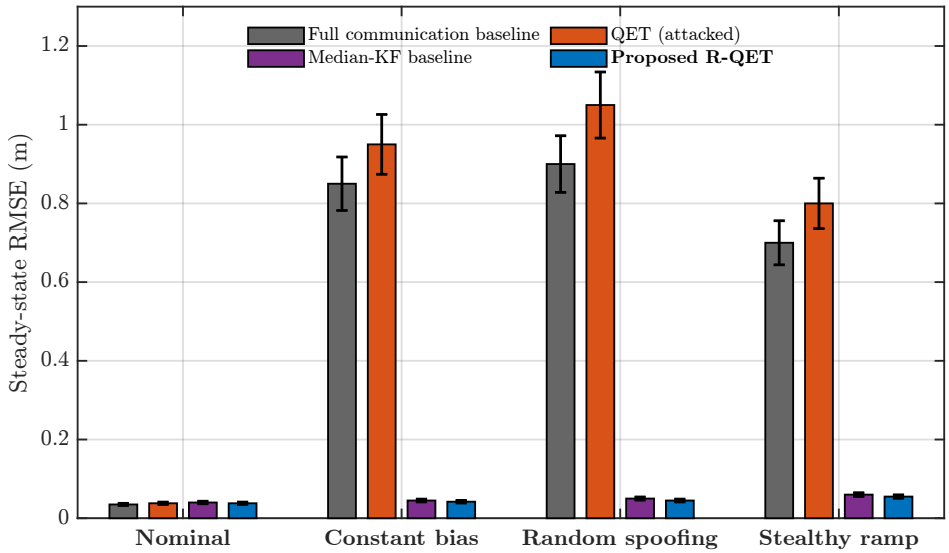


Fig. 6 Steady-state RMSE across different attack types. The proposed resilient QET filter maintains stable performance under nominal, constant-bias, random-spoofing, and stealthy-ramp scenarios, whereas non-defended baselines degrade severely under attack.

This result indicates that the method is not tuned to a single fault pattern only; the same lightweight screening mechanism remains useful across multiple abnormal-measurement models. In practical terms, the proposed R-QET stays in the narrow band of roughly 0.03–0.06 m across the plotted scenarios, whereas the non-defended

baselines rise into the 0.7–1.05 m range under severe attacks. The method therefore remains effective not only for a single hand-crafted bias profile but also across abrupt, random, and slowly varying corruptions.

3.10 Stealthy Ramp Attack

Figure 7 examines a stealthy ramp attack that initially stays close to the nominal uncertainty envelope. The resilient filter eventually recovers, but the early attack phase remains challenging because the anomalous innovation may stay below the gate threshold. In the default ramp setting, the RMSE begins to separate visibly only after the attack has accumulated for several seconds, which is consistent with the intended lightweight and memoryless nature of the NIS gate.

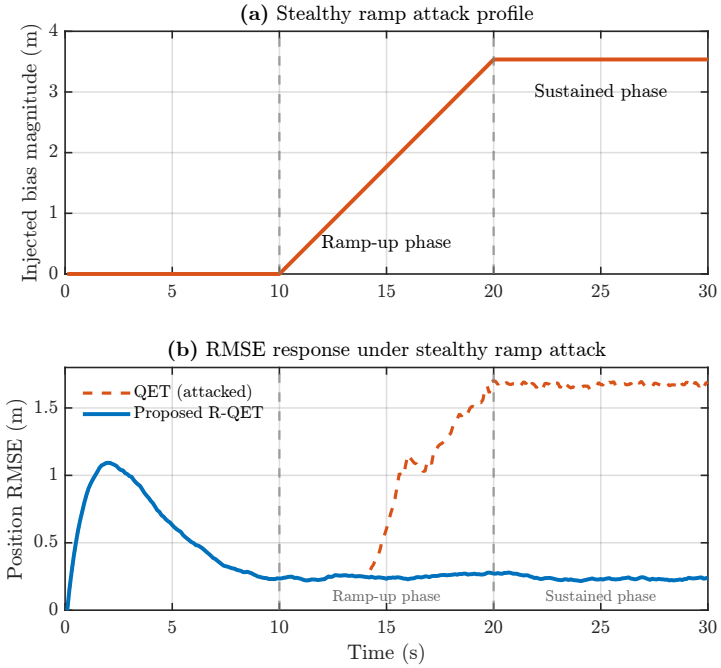


Fig. 7 Response under a stealthy ramp attack. A slowly increasing bias can initially evade the gate threshold, but the proposed resilient filter eventually detects the accumulated anomaly and recovers.

4 Discussion

The results support four practical conclusions. First, the triggering threshold γ is the main communication knob, whereas the quantization step Δ controls update fidelity and the validity of the white-noise approximation. Second, the lightweight NIS gate is effective against abrupt bias and spoofing attacks, especially when packet rates are low and the estimator cannot afford dense robust processing. Third, the method

should be interpreted as a communication-efficient resilient estimator rather than as a universally optimal robust filter. Fourth, the explicit packet accounting and complexity expressions show that "lightweight" in this paper refers to both finite-bit traffic and low online update cost.

The stealthy ramp experiment reveals a clear limitation. Because the gate is intentionally lightweight and memoryless at the packet-screening stage, small but persistent anomalies can evade rejection for part of the attack horizon. This suggests that future work should combine event-triggered transmission with adaptive thresholds, temporal change detection, or multi-hypothesis innovation screening.

The centralized architecture is also worth discussing explicitly. Although distributed fusion is attractive in large-scale networks, centralized WSN fusion remains reasonable when sensors report to a local edge server, gateway, roadside unit, or embedded controller with modest but nonzero communication limits. In such settings, the proposed method is most suitable when the measurement dimension is small, the number of simultaneously received packets is moderate, and communication scarcity matters more than achieving the absolute minimum RMSE under unlimited bandwidth. The approach is less suitable when the network is fully peer-to-peer, when attack models are strongly coordinated across many sensors, or when the application requires high-order temporal attack detection rather than lightweight per-packet screening.

Compared with heavier robust filters based on batch optimization, temporal consistency tests, or attack-set identification, the proposed R-QET scheme should be preferred when the designer values finite-bit communication, simple online updates, and interpretable per-packet screening rules. Conversely, if the dominant concern is stealthy coordinated attacks or strong temporal persistence modeling, then a more sophisticated resilient estimator may outperform R-QET at the price of greater computational and implementation complexity.

5 Conclusions

This paper presented a quantized event-triggered resilient filtering framework for bandwidth-limited wireless sensor networks. By combining explicit finite-bit innovation transmission with NIS-based packet screening and quantization-aware covariance inflation, the proposed method reduces communication load while maintaining competitive estimation accuracy and improved robustness under abnormal measurements. Numerical experiments showed clear communication savings, interpretable threshold–quantization trade-offs, and bounded error growth under representative attack scenarios. Future work will focus on adaptive thresholding, adaptive quantization, and stronger defenses against stealthy attacks.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Funding

This research was funded by the Inner Mongolia Higher Education Research Projects, grant number 2025027.

Acknowledgements

The authors thank their institutions for supporting this research.

Author contributions

H.G. developed the methodology, wrote the software, performed the validation, and prepared the original draft. X.L. conceptualized the study, supervised the project, and reviewed and edited the manuscript. Y.C. conducted the formal analysis and reviewed and edited the manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare no competing interests.

References

[1] Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *Comput. Netw.* **2002**, *38*, 393–422.

[2] Olfati-Saber, R.; Fax, J.A.; Murray, R.M. Consensus and cooperation in networked multi-agent systems. *Proc. IEEE* **2007**, *95*, 215–233.

[3] Sinopoli, B.; Schenato, L.; Franceschetti, M.; Poolla, K.; Jordan, M.I.; Sastry, S.S. Kalman filtering with intermittent observations. *IEEE Trans. Autom. Control* **2004**, *49*, 1453–1464.

[4] Schenato, L.; Sinopoli, B.; Franceschetti, M.; Poolla, K.; Sastry, S.S. Foundations of control and estimation over lossy networks. *Proc. IEEE* **2007**, *95*, 163–187.

[5] Hespanha, J.P.; Naghshtabrizi, P.; Xu, Y. A survey of recent results in networked control systems. *Proc. IEEE* **2007**, *95*, 138–162.

[6] Trimpe, S.; D'Andrea, R. Event-based state estimation with variance-based triggering. *IEEE Trans. Autom. Control* **2014**, *59*, 3266–3281.

[7] Han, D.; Mo, Y.; Wu, J.; Weerakkody, S.; Sinopoli, B.; Shi, L. Stochastic event-triggered sensor scheduling for remote state estimation. *IEEE Trans. Autom. Control* **2015**, *60*, 2661–2675.

[8] Kar, S.; Moura, J.M.F.; Poor, H.V. QD-Kalman: Quantized and distributed Kalman filtering. *IEEE Trans. Signal Process.* **2011**, *59*, 5617–5629.

[9] Weerakkody, S.; Mo, Y.; Sinopoli, B.; Han, D.; Shi, L. Multi-sensor scheduling for state estimation with communication constraints. *Automatica* **2016**, *66*, 222–229.

[10] Yu, D.; Xia, Y.; Li, L.; Zhai, D.-H. Event-triggered distributed state estimation over wireless sensor networks. *Automatica* **2020**, *118*, 109039.

[11] Ge, X.; Han, Q.-L.; Wang, J. Event-triggered distributed H_∞ consensus filtering for sensor networks. *Automatica* **2019**, *105*, 322–331.

[12] Battistelli, G.; Chisci, L.; Selvi, D. Event-triggered consensus for distributed state estimation via Kalman filtering. *Automatica* **2019**, *106*, 373–381.

[13] Jia, C.; Hu, J.; Chen, D.; Cao, Z.; Huang, J.; Tan, H. Adaptive event-triggered state estimation for a class of stochastic complex networks subject to coding-decoding schemes and missing measurements. *Neurocomputing* **2022**, *494*, 297–307.

[14] Sun, J.; Shen, B.; Liu, Y.; Alsaadi, F.E. Dynamic event-triggered state estimation for time-delayed spatial-temporal networks under encoding-decoding scheme. *Neurocomputing* **2022**, *500*, 868–876.

[15] Yu, D.; Xia, Y.; Zhai, D.-H.; Zhang, Y. Decentralized estimation for linear complex networks with multi-level quantization. *Automatica* **2025**, *179*, 112401.

[16] Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 1454–1467.

[17] Shoukry, Y.; Nuzzo, P.; Sangiovanni-Vincentelli, A.; Seshia, S.A.; Tabuada, P.; Pappas, G.J. Event-triggered state observers for sparse sensor noise/attacks. *IEEE Trans. Autom. Control* **2017**, *62*, 2078–2091.

[18] Chang, G. Robust Kalman filtering based on Mahalanobis distance as outlier judging criterion. *J. Geod.* **2014**, *88*, 391–401.

[19] Ding, D.; Han, Q.-L.; Ge, X.; Wang, J. Secure state estimation and control of cyber-physical systems: A survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 176–190.

[20] Duo, W.; Zhou, M.C.; Abusorrah, A. A survey of cyber attacks on cyber-physical systems: Recent advances and challenges. *IEEE/CAA J. Autom. Sinica* **2022**, *9*, 784–800.

[21] Zhang, D.; Wang, Q.-G.; Feng, G.; Shi, Y.; Vasilakos, A.V. A survey on attack detection, estimation and control of industrial cyber-physical systems. *ISA Trans.* **2021**, *116*, 1–16.

[22] Zhou, J.; Shang, J.; Chen, T. Cybersecurity landscape on remote state estimation: A comprehensive review. *IEEE/CAA J. Autom. Sinica* **2024**, *11*, 851–865.

[23] Yuan, H.; Xia, Y.; Yang, H. Resilient state estimation of cyber-physical system with multichannel transmission under DoS attack. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 6926–6937.

[24] Sun, Y.-C.; Yang, G.-H. Event-triggered remote state estimation for cyber-physical systems under malicious DoS attacks. *Inf. Sci.* **2022**, *602*, 43–56.

[25] Pang, Z.-H.; Cao, Q.; Guo, H.; Dong, Z. Prediction-based state estimation and compensation control for networked systems with communication constraints and DoS attacks. *IEEE/CAA J. Autom. Sinica* **2024**, *11*, 2352–2354.

[26] Li, Y.-G.; Yang, G.-H. Optimal innovation-based deception attacks with side information against remote state estimation in cyber-physical systems. *Neurocomputing* **2022**, *500*, 461–470.

[27] Shang, J.; Yu, H.; Chen, T. Worst-case stealthy innovation-based linear attacks on remote state estimation under Kullback–Leibler divergence. *IEEE Trans. Autom. Control* **2022**, *67*, 6082–6089.

[28] Ren, X.-X.; Yang, G.-H.; Zhang, X.-G. Optimal stealthy attack with historical data on cyber-physical systems. *Automatica* **2023**, *151*, 110895.

[29] Wang, Z.; Lou, P.; Wang, Y.; Li, J.; Wang, J. Motion state estimation with bandwidth constraints and mixed cyber-attacks for unmanned surface vehicles: A resilient set-membership filtering framework. *Sensors* **2024**, *24*, 6834.

[30] Kalman, R.E. A new approach to linear filtering and prediction problems. *J. Basic Eng.* **1960**, *82*, 35–45.

[31] Anderson, B.D.O.; Moore, J.B. *Optimal Filtering*; Prentice-Hall: Englewood Cliffs, NJ, USA, 1979.

[32] Simon, D. *Optimal State Estimation: Kalman, H_∞, and Nonlinear Approaches*; Wiley: Hoboken, NJ, USA, 2006.

[33] Huber, P.J. *Robust Statistics*; Wiley: New York, NY, USA, 1981.

[34] Zoubir, A.M.; Koivunen, V.; Ollila, E.; Muma, M. *Robust Statistics for Signal Processing*; Cambridge University Press: Cambridge, UK, 2018.

[35] Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.

[36] Ge, X.; Han, Q.-L.; Zhang, X.-M.; Ding, D.; Zhang, B.-L. Dynamic event-triggered control and estimation: A survey. *Int. J. Autom. Comput.* **2021**, *18*, 857–886.

[37] Zhang, X.-M.; Han, Q.-L.; Ge, X.; Ding, D.; Ning, B.; Zhang, B.-L. An overview of recent advances in event-triggered control. *Sci. China Inf. Sci.* **2025**, *68*, 110201.

[38] Khazraei, A.; Shoukry, Y.; Pappas, G.J.; Pasqualetti, F. Attack-resilient state estimation with intermittent data authentication. *Automatica* **2022**, *145*, 110531.

[39] Liu, Q.; Nie, Y.; Wang, Z.; Dong, H.; Jiang, C. Binary-encoding-based quantized Kalman filter: An approximate MMSE approach. *IEEE Trans. Autom. Control* **2024**, *69*, 7607–7622.

[40] Li, X.-M.; Zou, T.; Lu, R.; Zhao, Z. Event-based non-fragile state estimation for time-varying systems under deception attacks. *Sci. China Inf. Sci.* **2025**, *68*, 142204.