Trust-Enhanced Distributed Kalman Filtering for Sensor Fault Diagnosis in Sensor Networks

Khadija Shaheen, *Member, IEEE*, Apoorva Chawla, *Member, IEEE*, and Pierluigi Salvo Rossi, *Senior Member, IEEE*

***Abstract*—Sensor fault diagnosis is a critical issue in Sensor Networks (SNs) since sensor failures could lead to significant errors in data fusion and state estimation. To address this challenge, we propose a trust-enhanced distributed Kalman filter (TeDKF) designed to improve the state estimation performance of SNs under sensor faults. The TeDKF framework incorporates a novel incremental density-based (IDB) clustering mechanism into the distributed diffusion Kalman filter (DDKF) structure, which can support an intermediate-level feature (innovations) exchange and effectively fuses reliable sensor nodes. Unlike conventional clustering schemes, IDB clustering does not rely on majority voting, where more than half of the nodes must be reliable. Instead, it can effectively detect and eliminate faulty sensors even in scenarios where the majority of nodes are compromised. This dynamic clustering builds-up trust by selectively grouping the reliable nodes based on evolving normal system behavior, which is considered as a dynamic trust reference to detect anomalies and isolate faulty sensors irrespective of majority voting. The experimental results show that TeDKF significantly reduces estimation errors and enhances fault tolerance compared to the traditional Kalman filtering technique. It can handle different sensor faults, like bias, drift, noise, and stuck faults, especially in scenarios where most nodes are faulty.**

***Index Terms*—Distributed Kalman filter, incremental density-based clustering (IDB), sensor networks, sensor faults.**

I. Introduction

SENSOR Networks (SNs) are extensively used in various applications such as environmental monitoring, target tracking, and industrial automation. SNs comprise several spatially-distributed, low-cost, energy-efficient sensor nodes with limited communication and processing capabilities. These sensors interact with the physical world to capture, process, and transmit data, thus the reliability of such sensors is crucial for ensuring the safety and accuracy of SNs [1], [2].

However, sensor faults can significantly impact SN operation and cause performance degradation. Faults may arise due to several elements such as hardware malfunctions, harsh environmental conditions, or communication breakdowns.

Besides, there are several types of sensor faults [3], [4], including

- Bias faults: sensors give inaccurate data due to systematic measurement errors;
- Drift faults: a gradual variation of the sensor readings over time results in a progressive accumulation of errors;
- Noise faults: random variations in sensor readings potentially lead to intermittent errors;
- Stuck faults: sensors become unresponsive and continuously reflect some fixed values, not capturing the real changes in the monitored environment.
- Spike faults: show sudden, large deviations from normal readings that typically only last for one or a small number of time steps; often caused by electromagnetic interference or transient faults.
- Missing data faults: record missing sensor data at certain time steps due to packet loss, communication failure, or hardware interrupts.
- Gain faults: when the output of sensors is scaled incorrectly (e.g., too large or too small) usually because of amplification or calibration circuitry faults.

Amongst the numerous sensor fault types, bias, drift, noise, and stuck-at faults (see Fig. 1) are identified as the most prevalent and impactful in long-term industrial monitoring systems. There is a substantial amount of literature that supports their dominance in terms of frequency and diagnostic relevance [5], [6], [7], [8], [9], [10]. These works recognize these faults as the most frequent occurring in practical systems and characterize them as persistent faults owing to their chronic nature and substantial diagnostic importance [11], [12], [13]. Accordingly, this study focuses on these fault types due to their practical importance and diagnostic relevance. On the other hand, transient faults like spikes, missing data, and gain anomalies are generally handled by either preprocessing (e.g., outlier removal, interpolation, calibration) or system-level redundancy, hence are less critical in long-term degradation analysis [14], [15], [16].

Effective sensor fault diagnosis is essential to uphold the reliability, safety, and operational continuity of sensor network-based systems. Faulty sensor data has the capability to greatly compromise system performance and decision-making and create safety hazards or financial loss. As size and complexity grow in sensor networks, distributed and adaptive fault detection is even more important to handle faults in real time with little

Received 30 December 2024; revised 21 May 2025 and 9 July 2025; accepted 29 August 2025. Date of publication 4 September 2025; date of current version 17 September 2025. This work was supported by the Research Council of Norway through project SIGNIFY with in IKTPLUSS Framework under Grant 311902. The associate editor coordinating the review of this article and approving it for publication was Dr. Wei Hu. *(Corresponding author: Khadija Shaheen.)*

Khadija Shaheen and Apoorva Chawla are with the Department of Electronic Systems, Norwegian University of Science and Technology, 7491 Trondheim, Norway (e-mail: shaheen.khadija@ntnu.no; apoorva.chawla@ntnu.no).

Pierluigi Salvo Rossi is with the Department of Electronic Systems, Norwegian University of Science and Technology, 7491 Trondheim, Norway, and also with the Department of Gas Technology, SINTEF Energy Research, 7491 Trondheim, Norway (e-mail: salvorossi@ieee.org).

Digital Object Identifier 10.1109/TSIPN.2025.3606167

communication overhead and maintenance expense. Therefore, developing fault-tolerant diagnostic techniques is important to enable precise state estimation and fault-tolerant performance in faulty and dynamic operating conditions.

Techniques for detecting and mitigating sensor faults in SNs are generally classified into model-based [17] and data-driven approaches [8], [18]. Although data-driven methods are highly effective, they often require extensive training data. Moreover, they are computationally intensive, which limits their suitability for real-time applications [19]. In contrast, model-based approaches rely on mathematical system models to estimate the expected sensor behavior. Sensor faults in these techniques are identified by comparing the actual sensor measurements with the predicted values of the model.

Among model-based approaches, the Kalman filter (KF) is a highly effective technique to detect and estimate sensor faults [20]. There are two major architectures for implementing KF: centralized and distributed [21]. In the centralized framework, a single filter processes measurements from all sensors. Although this approach may give accurate results, it is not scalable for large SNs due to the communication and computational constraints [22], [23]. Alternatively, distributed architecture is more fault-tolerant and provide scalable solutions. Every sensor node runs a local KF and shares information with the neighboring nodes, allowing the network to jointly estimate the system state. This approach markedly alleviates the communication load while improving fault tolerance, rendering it particularly appropriate for SNs [24], [25]. Although the decentralized architecture may resemble federated learning (FL), it fundamentally differs in purpose: FL is a data-driven, privacy-preserving model training framework, while our approach is model-based and designed for real-time state estimation and fault detection based on physical system dynamics.

Distributed KFs have various types including consensus KF (CKF) [26], federated KF (FKF) [27], and distributed diffusion KF (DDKF) [28]. Although CKF utilizes a consensus technique to combine local estimates from neighboring nodes, it suffers slow convergence and substantial communication overheads, particularly in large networks [29]. On the other hand, FKF reduces communication overhead by enabling each local filter to operate independently, but it may lead to suboptimal performance because of a lack of inter-node cooperation [30]. Further, DDFK employs a diffusion strategy for exchanging information with immediate neighbors, achieving a balance between communication efficiency and estimation accuracy, thus making it effective for sensor fault diagnosis in SNs [24].

Several methods have been proposed to increase the robustness and efficiency of distributed KFs for sensor failure diagnosis in SNs. For instance, a fast finite-time convergence distributed KF algorithm is presented in [31] to enhance convergence speed, however, it might not be appropriate for highly dynamic settings with frequent sensor failures. Similarly, a distributed Bayesian fault diagnosis technique based on sequential Monte Carlo filtering is designed in [32], offering robust fault identification but at the cost of high computational overhead, limiting its suitability for real-time applications. Moreover, a consensus-based distributed KF is introduced in [33] to improve global state estimation, yet it faces slow convergence issues, making it less ideal for bandwidth-constrained SNs. The authors in [34] developed a node selection strategy for distributed KF in heterogeneous sensor networks to reduce computational and communication costs, nevertheless, it may not handle changes in topology or dynamic sensor faults. Furthermore, a diffusion KF based on a covariance intersection approach is proposed in [35] to improve estimation performance, though this approach can introduce additional computational complexity. In [36], a trust-based distributed KF (TDKF) technique is explored for estimating oscillation modes in power systems with faulty measurements, however, its performance may be impacted by subjective threshold selection. Likewise, [37] developed a distributed KF technique based on Adaptive clustering; however, its effectiveness may deteriorate in networks with substantial sensor failures or shifting topologies. In [38], a distributed Tobit Kalman filter is developed to address the issue of delayed and censored measurement while remaining vulnerable to undetected sensor faults. Similarly, [39] develops a maximum correntropy criterion-based distributed Kalman filter for robustness against impulsive noise, but notably lack systematic fault detection mechanisms in the sensors. Moreover, [40] proposes an event-triggered consensus control against DoS attacks for multi-agent systems but based on a priori known fault models and attack/fault isolation that cannot be realized in the presence of concurrent sensor faults and cyber attacks. In addition, [41] suggests a distributed fault detection approach for natural pipelines system, but it fails under multiple sensor faults and domain changes.

Recent development in the sensor fault diagnosis has suggested the incorporation of distributed KF with clustering techniques, which would improve the accuracy and efficiency in fault detection. These techniques usually classify the sensor estimates into trusted and untrusted clusters. In [42], a TDKF approach based on K-means clustering is designed for target tracking under sensor faults or attacks. The K-means clustering algorithm classifies all the local estimates generated by the nodes into trusted and untrusted clusters and selecting the trusted set using a majority voting system. Similarly, [43] introduced a trust-based distributed KF technique utilizing the Gaussian mixture model (GMM) which classifies a node and its neighboring nodes into trusted and untrusted sets by the majority voting. Moreover, a trust-based clustering fusion strategy was proposed by using iterative Wasserstein average-based consensus in [29] for diagnosing sensor faults in SNs.

One major limitation of these clustering-based data fusion methods is their reliance on majority voting, where the cluster with the maximum number of elements is considered the trusted set. All these methods require the majority of sensor nodes to be reliable, with only a minority compromised. However, in large-scale SNs with hundreds/thousands of nodes, it is highly infeasible to ensure a majority of sensors are trusted; therefore, there is a need of trust-based schemes independent of majority voting. Moreover, these methods typically remove faulty nodes in general without providing any estimate that could provide compensation for further degraded state estimation. Another disadvantage is that clustering techniques categorize sensor nodes into trusted/untrusted groups even when no fault occurs. This probably excludes many accurate state estimations of reliable

nodes in data fusion and hence reduces the overall estimation performance. In addition, existing distributed Kalman filtering (DKF) algorithms operate at varying fusion levels—low-level (exchanging raw measurements), high-level (exchanging state estimates), and very high-level (exchanging state estimates and covariances)—with increasing accuracy but at the cost of cumbersome communication overhead. To balance this trade-off, there is a need for a medium-level fusion strategy that exchanges intermediate features, providing an efficient, yet dependable alternative with best estimation accuracy and communication efficacy, particularly under faulty conditions.

To address these challenges, we propose a novel trust-enhanced distributed Kalman filter (TeDKF) approach for robust sensor fault detection in SNs. Our TeDKF approach incorporates a novel incremental density-based (IDB) clustering strategy to detect faulty sensor nodes over large-scale dynamic networks—that is, networks where system states and sensor measurements evolve over time, and the reliability of nodes may alter. The IDB clustering creates a dynamic cluster of reliable nodes that continuously update as new data become available, making it highly suitable for real-world dynamic settings. In addition, our approach does not depend on majority voting scheme and is sufficiently resilient when majority of sensor nodes are faulty. The proposed architecture uses a DDKF, where each node can estimate locally the system's state (e.g., position, velocity) and allowing the exchange of information with the immediate neighboring nodes. Although direct communication is limited to immediate neighboring nodes, the method remains applicable to networks with widely spaced sensors, as long as sensors constitute a connected network allowing information to diffuse between nodes. Unlike the traditional methods that rely on high-level fusion, our approach utilizes medium-level fusion. This method only fuses the innovation (or residual) generated from the measurement, avoiding the fusion of local state estimates and covariance. Consequently, this innovation-based fusion strategy significantly reduces computational and communication load without sacrificing accuracy.

In the proposed approach, trust is treated as a dynamic and continuously adaptive attribute, moving beyond the static majority voting assumption employed in existing methods [29], [42], [43]. The proposed evolving trust scheme allows to validate the reliability of each node based on evolving context-aware trust reference, rather than employing static thresholds or majority consensus. In proposed approach, the trust reference is initially formed by a group of reliable sensor nodes whose behavior aligns with the expected system dynamics during nominal operating conditions. It serves as a contextual baseline to determine the trust value of incoming data across the network. As the system operates further, new information is gained, the trust reference is increasingly updated towards reflecting the latest and most stable sensing patterns. This continuous update allows for the detection of marginal or slowly formed sensor faults, as well as preventing the early elimination of temporarily deviated nodes. Hence, the proposed framework presents a robust and flexible trust mechanism that significantly improves the correctness and robustness of fault detection in dynamic and potentially unstable sensor network environments.

A rapid comparison of our proposed technique with existing methods is provided in Table I. Moreover, the contributions of this work can be summarized as follows:

- We propose a novel Trust-enhanced Distributed Kalman Filter (TeDKF) approach that tackles fault tolerance in SNs. In contrast to traditional methods based on majority voting schemes [42], [43], our strategy employs dynamic confidence weighting that periodically assesses and adjusts each node's reliability in real time. This allows effective detection of simultaneously occurring multiple fault modes including bias, drift, noise, and stuck faults and still allows the system to function when most of the nodes are faulty.
- Our work introduces an efficient medium-level fusion strategy that bridges the gap between high-overhead and low-resilience existing methods. Through strategic exchange of innovation vectors (residuals) among nodes, we have the two-fold advantage of: (1) considerably reduced communication bandwidth (lower than high-level fusion) with high estimation accuracy preserved, and (2) inherent fault detectability via online residual analysis.
- We introduce a novel IDB clustering technique that can effectively handle dynamic and scale-large network clustering. (IDB) clustering adaptively finds reliable node clusters via local density estimation and hierarchical propagation of trust, which self-tunes to network dynamics. This removes the need for majority voting altogether while ensuring operational resilience even if more than 50% of nodes are faulty - a key improvement for large deployments in unreliable environments.

The paper is organized as follows: Section II explains the problem formulation and provides an overview of the preliminaries related to KF; the proposed TeDKF technique for distributed state estimate in SNs is presented in Section III; Section IV presents the numerical results; and some concluding remarks are provided in Section V.

II. Problem Formulation

We consider a linear state-space model for a SN consisting of N connected sensor nodes. The state-space representation for the ith sensor node ($i = 1, 2, \ldots, N$) at the kth time instant is expressed as

$$\mathbf{x}_{k+1}^i = \mathbf{A}_k^i \mathbf{x}_k^i + \mathbf{B}_k^i \mathbf{u}_k^i + \mathbf{w}_k^i, \tag{1}$$

$$\mathbf{z}_k^i = \mathbf{H}_k^i \mathbf{x}_k^i + \mathbf{v}_k^i, \tag{2}$$

where $\mathbf{x}_k^i \in \mathbb{R}^n$, $\mathbf{u}_k^i \in \mathbb{R}^m$ and $\mathbf{z}_k^i \in \mathbb{R}^p$ represent the local state vector, the control input, and the measurement vector corresponding to the ith sensor node, respectively. Further, the matrices $\mathbf{A}_k^i \in \mathbb{R}^{n\times n}$, $\mathbf{B}_k^i \in \mathbb{R}^{n\times m}$ and $\mathbf{H}_k^i \in \mathbb{R}^{p\times n}$ denote the state transition matrix, the control input matrix, and the measurement matrix, respectively. The vectors $\mathbf{w}_k^i \in \mathbb{R}^n \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_k^i)$ and $\mathbf{v}_k^i \in \mathbb{R}^p \sim \mathcal{N}(\mathbf{0}, \mathbf{R}_k^i)$ specify the process and the measurement noise, respectively.

In case of sensor fault, the measurement model is modified as

$$\mathbf{z}_k^i = \mathbf{H}_k^i \mathbf{x}_k^i + \mathbf{v}_k^i + \mathbf{f}_k^i, \tag{3}$$

TABLE I
COMPARISON OF THE PROPOSED METHOD WITH EXISTING TECHNIQUES

Techniques	Fusion level	Fault detection	Fault accommodation	Maximum faulty nodes (%)	Bias fault	Drift fault	Noise fault	Stuck fault
[47]	Low (measurement)	–	✗	–	✗	✗	✗	✗
[48]	High (state)	–	✗	–	✗	✗	✗	✗
[44]	Very high (state, covariance)	K-means	✓	40%	✓	✓	✓	✗
[45]	Very high (state, covariance)	GMM	✓	40%	✓	✓	✓	✗
[46]	Very high (state, covariance)	Wassertein clustering	✓	40%	✓	✓	✓	✗
Proposed	Medium (innovation)	Adaptive clustering	✓	90%	✓	✓	✓	✓

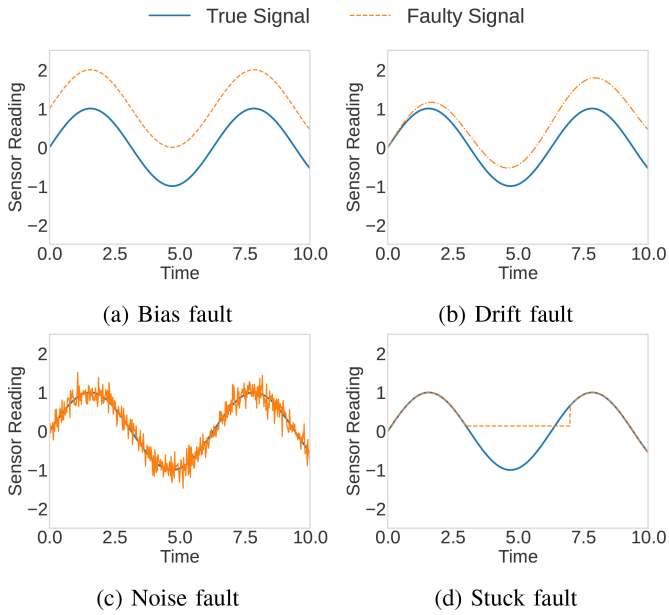


Fig. 1. Common types of sensor faults.

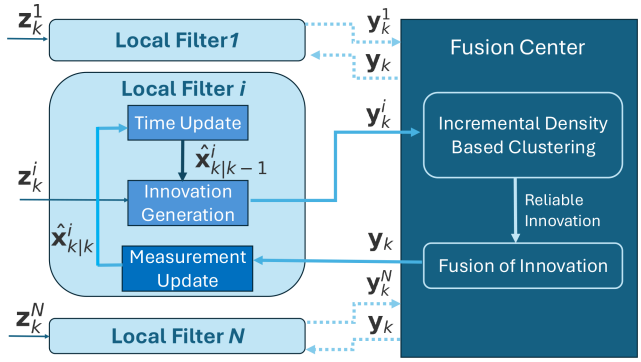


Fig. 2. Proposed architecture.

where $\mathbf{f}_k^i \in \mathbb{R}^p$ represents the sensor fault vector, capturing the deviations caused by the sensor faults. The detection and accommodation of this fault vector is highly challenging due to its unknown and variable nature. These sensor faults can significantly degrade the accuracy of state estimation, therefore it is essential to eliminate their influence.

The primary objective of this work is to identify a wide range of sensor faults and suggest a distributed KF algorithm that can deliver reliable state estimates $\hat{\mathbf{x}}_k$ under their occurrence. We propose a novel distributed architecture for handling sensor faults within connected SNs, as discussed in the next section.

III. PROPOSED METHOD

The proposed architecture incorporates the DDKF algorithm with IDB clustering, as depicted in Fig. 2. Initially, every node in the SN performs the standard KF time update to predict the system state and generates the innovation, representing the difference between the estimated and actual measurements. The IDB clustering algorithm then analyzes the innovations to identify reliable and faulty nodes. Subsequently, the innovations from the reliable nodes are fused to form a global innovation, which is utilized by each node to perform the measurement update. The proposed technique is outlined in Algorithm 1 and based on the following steps:

Initialization: Set the initial values for the state estimate ($\hat{\mathbf{x}}_{0|0}^i \in \mathbb{R}^n$) and covariance ($\mathbf{P}_{0|0}^i \in \mathbb{R}^{n\times n}$) of each node based on the use case.

Time Update (Prediction): For the ith node at the kth time instant, the *a priori* state estimate and covariance matrix are evaluated as

$$\hat{\mathbf{x}}_{k|k-1}^i = \mathbf{A}_{k-1}^i \hat{\mathbf{x}}_{k-1|k-1}^i + \mathbf{B}_{k-1}^i \mathbf{u}_{k-1}^i + \mathbf{w}_k^i,$$
$$\mathbf{P}_{k|k-1}^i = \mathbf{A}_{k-1}^i \mathbf{P}_{k-1|k-1}^i \mathbf{A}_{k-1}^{i\,T} + \mathbf{Q}_{k-1}^i. \quad (4)$$

Innovation Generation: The ith node generates an innovation ($\mathbf{y}_k^i \in \mathbb{R}^p$) using the measurement ($\mathbf{z}_k^i$) as

$$\mathbf{y}_k^i = \mathbf{z}_k^i - \mathbf{H}_k^i \hat{\mathbf{x}}_{k|k-1}^i. \quad (5)$$

The innovations from all nodes are subsequently sent to a central fusion center, where IDB clustering is performed to identify the innovations of the reliable nodes.

Algorithm 1: TeDKF.

Input: *A priori* state estimate $\hat{\mathbf{x}}^i_{k-1|k-1}$, covariance matrix $\mathbf{P}^i_{k-1|k-1}$, process noise covariance matrix $\mathbf{Q}^i_k$, measurement noise covariance matrix $\mathbf{R}^i_k$, state transition matrix $\mathbf{A}^i_{k-1}$, measurement matrix $\mathbf{H}^i_k$, control input $\mathbf{u}^i_k$
Time Update:
for each ith node **do**
  Estimate $\hat{\mathbf{x}}^i_{k|k-1}$ and $\mathbf{P}^i_{k|k-1}$ using (4)
end for
Innovation Generation:
for each ith node **do**
  Compute $\mathbf{y}^i_k$ using (5)
end for
Apply IDB Clustering: Use Algorithm 2
Global Innovation Fusion:
  Compute $\mathbf{y}_k$ using (10)
Measurement Update:
for each ith node **do**
  Estimate $\hat{\mathbf{x}}^i_{k|k}$ and $\mathbf{P}^i_{k|k}$ using (11)
end for
Output: Fault-free *a poteriori* state estimate and covariance matrix

Algorithm 2: IDB Clustering.

Input: Trusted cluster containing reliable set of innovations $\mathcal{Y}^c_{k-1}$ at $(k-1)$th time instant, new set of innovations (test data points) at kth time instant $\mathcal{Y}^{test}_k = \{\mathbf{y}^1_k, \mathbf{y}^2_k, \mathbf{y}^3_k, \ldots, \mathbf{y}^i_k, \ldots, \mathbf{y}^N_k\}$
if k==1 **then**
  $\mathcal{Y}^c_{k-1} = \mathcal{Y}^{test}_k$
end if
for each test data point $\mathbf{y}^i_k$ in $\mathcal{Y}^{\text{test}}_k$ **do**
  for each data point $\mathbf{y}^j_{k-1}$ in $\mathcal{Y}^c_{k-1}$ **do**
    Compute mutual reachability distance between $\mathbf{y}^i_k$ given $\mathbf{y}^j_{k-1}$ using (8)
  end for
end for
Compute adaptive threshold using (9)
for each test data point $\mathbf{y}^i_k$ in $\mathcal{Y}^{\text{test}}_k$ **do**
  Update the cluster $\mathcal{Y}^c_k$ using (6)
end for
Output: Trusted cluster $\mathcal{Y}^c_k$ at kth time instant

IDB Clustering: Dynamic clustering adaptively groups and updates data points or entities based on the evolving similarities/characteristics of system dynamics. A cluster of reliable nodes is initially formed assuming that most data points are accurate, with minimal noise or outliers. The cluster continuously updates with new data from reliable nodes, serving as a reference for evaluating anomalous data points and enabling the identification of faulty nodes. The method is designed to group ML features, such as innovations generated by each local KF, expected to remain relatively invariant for non-faulty nodes as the system evolves.

At the kth time, the set of reliable data points ($\mathcal{Y}^c_k \in \mathbb{R}^{p\times N_t}$) must satisfy the criterion that its detection metric (e^i) falls below a specified threshold (τ), expressed as

$$\mathcal{Y}^c_k = \left\{\mathbf{y}^i_k \mid e^i \leq \tau\right\}. \tag{6}$$

The detection metric (e^i) is defined using the mutual reachability distance ($d_{\text{mreach}}(\mathbf{y}^i_k, \mathbf{y}^j_{k-1})$), which evaluates the connectivity of a data point ($\mathbf{y}^i_k$) relative to the set of reliable points ($\mathbf{y}^j_{k-1} \in \mathcal{Y}^c_{k-1}$) identified during the $(k-1)$th time instant. The detection metric for the ith data point is:

$$e^i = \min_j d_{\text{mreach}}(\mathbf{y}^i_k, \mathbf{y}^j_{k-1}), \tag{7}$$

with the mutual reachability distance between two innovations ($\mathbf{y}^i_k$ and $\mathbf{y}^j_{k-1}$) being calculated as

$$d_{\text{mreach}}(\mathbf{y}^i_k, \mathbf{y}^j_{k-1}) = \max\left(d_{\text{core}}(\mathbf{y}^i_k), d_{\text{core}}(\mathbf{y}^j_{k-1}), d_{ij}\right), \tag{8}$$

where $d_{ij} = \|\mathbf{y}^i_k - \mathbf{y}^j_{k-1}\|_2$ is the Euclidean distance between the ith node and the jth node, and the term $d_{\text{core}}(\mathbf{y}^i_k) = \|\mathbf{y}^i_k - \mathbf{y}^\gamma_{k-1}\|_2$ represents the core distance of the ith node from the γth nearest neighboring data point, with γ denoting the minimum number of data points needed to define the local density around a given data point $\mathbf{y}^i_k$. Using these parameters, the mutual reachability distance ensures that only the data points that are both close to each other and located within dense regions are grouped. This approach effectively eliminates isolated data points or outliers and enhances the reliability of the clustering process.

The steps involved in the IDB clustering are summarized in Algorithm 2. At the initial time step $k = 1$, the IDB clustering assumes that all data points are accurate and each node has fault-free measurement. This ensures a low detection metric given in (7), allowing reference cluster formation of reliable data points, which serves as a foundation for future predictions and updates as new reliable data points are available. As the system progresses to subsequent time steps, the reliable cluster ($\mathcal{Y}^c_{k-1}$) at the previous time instant is used to validate the reliability of a new data point ($\mathbf{y}^i_k$). If the detection metric between the new data point and the reliable points in the existing cluster falls below the threshold (τ), the data point is deemed reliable and used to update the reliable cluster ($\mathcal{Y}^c_k$) at the current time instant. Conversely, if the detection metric exceeds the threshold, the data point is rejected, indicating the presence of a potential fault. Due to the availability of a fault-free reference cluster at each step, this technique allows us to effectively identify faults even in scenarios where the majority of nodes is faulty[1].

To further enhance the detection performance of the IDB clustering, we implement a dynamic threshold (τ) which adapts to the changing data distribution and improves the robustness of the clustering process. The adaptive threshold is determined by averaging the detection metric across all (faulty and non-faulty) nodes and mathematically given as

$$\tau = \frac{1}{N}\sum_{i=1}^{N} e^i + \lambda, \tag{9}$$

[1]This issue has not been addressed in existing works [42], [43].

where λ is a constant tuning parameter that adjusts the threshold sensitivity, and N represents the total number of nodes. In fault-free situations, detection metrics are close to the mean, and the threshold—set just above it through parameter λ—keeps false positives away. During faults, metrics of faulty nodes deviate significantly, and an appropriately tuned λ maintains the threshold sensitive enough to detect such outliers without misclassifying normal nodes. The method assumes at least 10% non-faulty node at time $k > 1$, where the low detection metric of non-faulty nodes helps maintain a suitably low threshold, enabling effective fault diagnosis even when most nodes are faulty.

Fusion of Innovations: The innovations corresponding to the data points in the trusted cluster ($\mathcal{Y}_k^c$), generated using the IDB clustering approach, are fused to create a global fault-free innovation ($\mathbf{y}_k \in \mathbb{R}^p$) as

$$\mathbf{y}_k = \frac{1}{N_t} \sum_{i \in \text{trusted nodes}} \mathbf{y}_k^i, \tag{10}$$

which is shared with all sensor nodes to perform the measurement update while ensuring that all sensor nodes perform accurate state estimates using reliable innovations.

Measurement Update: For the ith node, *a posteriori* local state estimate and the covariance matrix using the Kalman gain matrix ($\mathbf{K}_k^i$) and the innovation covariance matrix ($\mathbf{S}_k^i$) are evaluated as

$$\begin{aligned}
\mathbf{S}_k^i &= \mathbf{H}_k^i \mathbf{P}_{k|k-1}^i \mathbf{H}_k^{i\,T} + \mathbf{R}_k^i, \\
\mathbf{K}_k^i &= \mathbf{P}_{k|k-1}^i \mathbf{H}_k^{i\,T} \mathbf{S}_k^i, \\
\hat{\mathbf{x}}_{k|k}^i &= \hat{\mathbf{x}}_{k|k-1}^i + \mathbf{K}_k^i \mathbf{y}_k, \\
\mathbf{P}_{k|k}^i &= (\mathbf{I} - \mathbf{K}_k^i \mathbf{H}_k^i) \mathbf{P}_{k|k-1}^i.
\end{aligned} \tag{11}$$

IV. Numerical Results

We consider a SN with 10 connected sensor nodes employing a linear heat transfer dynamics system that monitors temperature at 4 separate spatial points, leading to a state vector with 4 components. The state transition matrix ($\mathbf{A}_k^i$), which governs the heat transfer dynamics in the system, is

$$\mathbf{A}_k^i = \begin{bmatrix} 0.8 & 0.1 & 0.0 & 0.0 \\ 0.1 & 0.8 & 0.1 & 0.0 \\ 0.0 & 0.1 & 0.8 & 0.1 \\ 0.0 & 0.0 & 0.1 & 0.8 \end{bmatrix},$$

and the measurement matrix is $\mathbf{H}_k^i = \mathbf{I} \in \mathbb{R}^{4\times4}$. The process and measurement noise covariance matrices are set to $\mathbf{Q}_k^i = 0.05\mathbf{I} \in \mathbb{R}^{4\times4}$ and $\mathbf{R}_k^i = \sigma\mathbf{I} \in \mathbb{R}^{4\times4}$, respectively, where σ represents the noise standard deviation allowing to analyze different signal-to-noise ratios (SNRs). The initial state estimate and covariance matrix are chosen as $\hat{\mathbf{x}}_{0|0}^i = [20, 22, 24, 23]$ and $\mathbf{P}_{0|0}^i = \mathbf{I} \in \mathbb{R}^{4\times4}$, respectively. These settings are based on the reference thermal system model in [46] which provides a realistic basis for distributed temperature phenomenon and sensor response modeling. Although actual noise will typically not obey the Gaussian assumption, we impose it here as a general and analytically convenient approximation of modeling, particularly well-suited to Kalman filter-based schemes applied to thermal systems. We set $\gamma = 5$ (number of data points needed to define local density) empirically based on the accuracy of fault detection performance. This value provided the best trade-off between fault sensitivity and noise immunity.

The fault-free measurement (z_k^j) for the jth sensor at the kth time instant is generated by adding zero-mean white Gaussian noise, namely q_k^j, to the initially generated values (x_k^j), which are free from both noise and faults. The fault-free measurement is expressed as

$$z_k^j = x_k^j + q_k^j.$$

To evaluate the fault diagnosis performance of the proposed technique, we introduce 4 types of synthetically generated sensor faults into the simulated data to emulate both hard and soft failures, based on the following mathematical models.

Bias Fault: A constant bias is added to the sensor measurements over M consecutive samples, defined as

$$z_k^{j(\mathrm{f})} = \begin{cases} z_k^j + b, & 0 \le k - m \le M \\ z_k^j, & \text{otherwise} \end{cases},$$

where $z_k^{j(\mathrm{f})}$ is the faulty measurement associated with the jth node, M represents the duration (in samples) over which a constant bias b is added, and m is the onset time of the fault.

Drift Fault: The sensor measurements gradually deviate from the true values over time, expressed as

$$z_k^{j(\mathrm{f})} = \begin{cases} z_k^j + \frac{b_d(k-m+1)}{M}, & 0 \le k - m \le M \\ z_k^j + b_d, & M \le k - m \le M + K \\ z_k^j, & \text{otherwise} \end{cases},$$

where M denotes the number of samples during which the drift fault is introduced and K is the number of samples over which the drift fault maintains the saturated bias level b_d. We emphasize the drift fault by assuming $M > K$.

Noise Fault: Random noise is added to the sensor measurements, introducing unpredictable fluctuations, given as

$$z_k^{j(\mathrm{f})} = \begin{cases} z_k^j + n(k), & 0 \le k - m \le M, \\ z_k^j, & \text{otherwise}, \end{cases}$$

where $n(k)$ is a noise vector with zero mean and variance σ_n, characterizing the measurement uncertainty.

Stuck Fault: The sensor continuously reports a fixed value, defined as

$$z_k^{j(\mathrm{f})} = \begin{cases} z_m^j, & 0 \le k - m \le M \\ z_k^j, & \text{otherwise} \end{cases}.$$

We evaluate the performance of our proposed techniques for various sensor fault scenarios, focusing on both weak and strong faults. For bias and drift faults, the absolute bias value b is uniformly distributed between 20% to 40% (resp. 60% to 90%) for weak (resp. strong) faults, with a randomly-assigned positive or negative sign. Similarly, the variance matrix σ_n follows the same distribution values for noise faults. Fault durations M and K are randomly selected between 6 and 10 samples. Further,

TABLE II
COMPARING THE RMSE OF DIFFERENT TECHNIQUES AT DIFFERENT SNR VALUES UNDER NON-FAULTY SCENARIO

SNR value	Fusion	Technique	RMSE
5 dB	VHL	DDKF	0.000286
		DDKF with K-means	0.0005792
		DDKF with GMM	0.00058
	ML	DDKF	0.000286
		DDKF with K-means	0.23167
		DDKF with GMM	0.230424
		Proposed	**0.000336**
0 dB	VHL	DDKF	0.0046660
		DDKF with K-means	0.00658
		DDKF with GMM	0.006569
	ML	DDKF	0.004666
		DDKF with K-means	0.230807
		DDKF with GMM	0.229238
		Proposed	**0.004714**
-5 dB	VHL	DDKF	0.191094
		DDKF with K-means	0.213904
		DDKF with GMM	0.21376
	ML	DDKF	0.191094
		DDKF with K-means	0.234062
		DDKF with GMM	0.233181
		Proposed	**0.191241**

uniform distribution is used for fault level and duration, which allows a thorough evaluation of the proposed technique across diverse sensor fault scenarios. Faults can occur randomly in time and across sensors, but their characteristics remain fixed once introduced, while the noise level (via SNR) is kept constant across all sensors and time steps.

Several baseline approaches, including DDKF with K-means clustering [42], GMM-based clustering [43], and the standard DDKF, are utilized for comparison. Additionally, we compare our proposed method against baselines featuring different levels of data fusion, namely very high-level (VHL) fusion, which fuses both the state vector and covariance matrix, and ML fusion, which only fuses the innovations. These comparisons offer a comprehensive assessment of the performance and robustness of our approach across various fusion strategies.

To assess the state estimation performance in the fault-free scenario, we compute the root mean squared error (RMSE) at three different SNR values, i.e., -5 dB, 0 dB, and 5 dB, as shown in Table II. Furthermore, the RMSE results for the fault-free scenario at a fixed SNR of 1 dB are presented in Fig. 3. These results clearly illustrate that our proposed method achieves RMSE close to the traditional DDKF technique for VHL and ML fusions and is lower than other clustering-based approaches. Other clustering-based techniques classify sensor nodes into trusted and untrusted groups even in non-faulty scenarios that potentially exclude accurate state estimates from reliable nodes during data fusion, leading to degradation in estimation performance. We evaluate the RMSE of the proposed method and compare it to other baseline techniques under different fault scenarios.

Moreover, the impact of the number of faulty nodes on the estimation accuracy is examined by analyzing the RMSE for

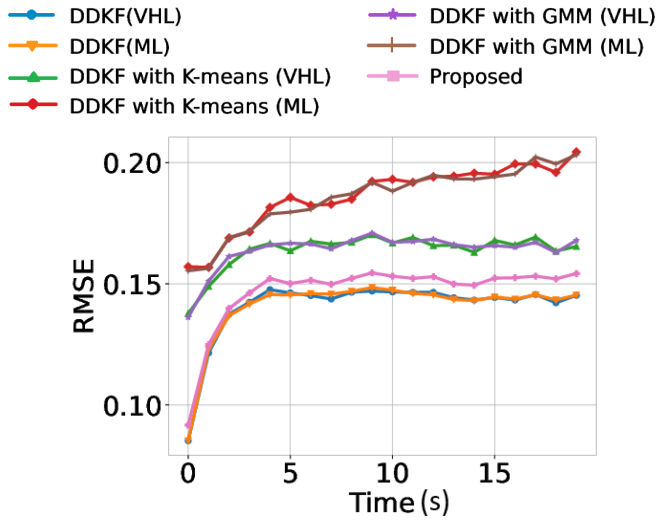
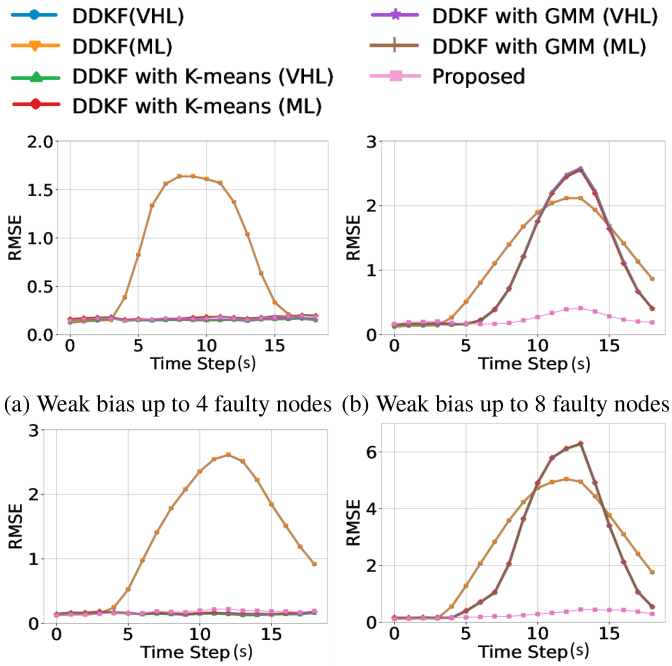


Fig. 3. RMSE comparison of proposed and baseline techniques without sensor fault at 1 dB SNR.



(a) Weak bias up to 4 faulty nodes (b) Weak bias up to 8 faulty nodes

(c) Strong bias up to 4 faulty nodes (d) Strong bias up to 8 faulty nodes

Fig. 4. RMSE comparison of proposed and baseline techniques with bias fault at 1 dB SNR.

scenarios with a few faulty nodes (up to four) and a majority of faulty nodes (up to eight), as shown in Fig. 4. In the case of a few faulty nodes, our approach achieves similar results as other clustering-based baselines. However, when most faulty nodes are considered, our method consistently achieves a significantly lower RMSE than other baselines.

These findings highlight the effectiveness of our approach in maintaining accurate state estimation even in the presence of sensor faults. Traditional methods that rely on majority voting, require a majority of reliable nodes for accurate state estimation.

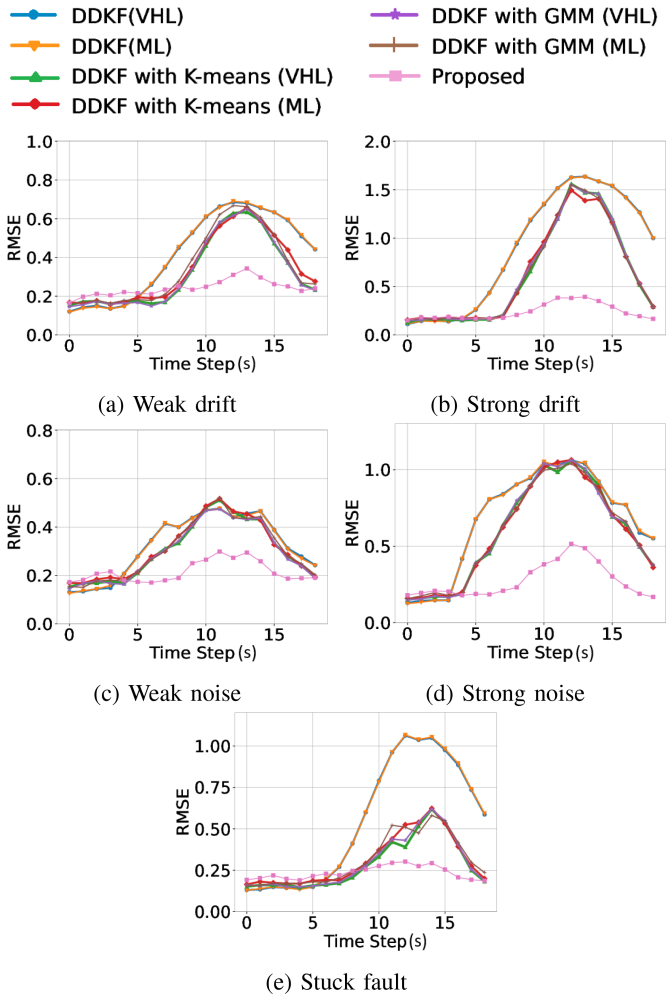


Fig. 5. RMSE comparison of proposed and baseline techniques at 1 dB SNR (upto 8 faulty nodes).

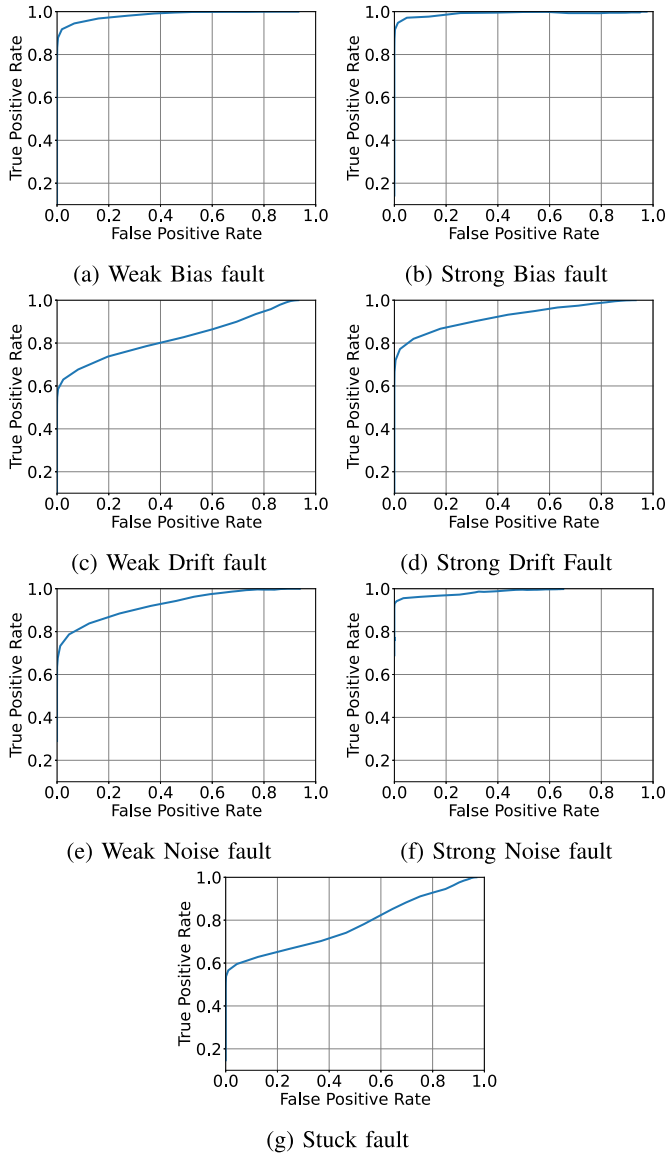


Fig. 6. ROC curves illustrating the performance of the proposed techniques across various types of sensor faults.

Consequently, baseline techniques fail to identify and isolate faults when most nodes are faulty. In contrast, our proposed method consistently attains lower RMSE even as the proportion of faulty sensors increases. Similarly, we assess the RMSE for scenarios involving weak and strong drift, weak and strong noise, and stuck-at faults, focusing on cases where most nodes are faulty. The results in Fig. 5 demonstrate that our proposed technique consistently surpasses the baseline methods, achieving notably lower RMSE across all fault types. This highlights the increased accuracy and effectiveness of our approach in handling various fault conditions, particularly when most nodes are compromised.

We use accuracy as detection metrics which is calculated as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

where TP (true positives) is the number of faulty nodes that are identified correctly, TN (true negatives) is the number of healthy nodes that are classified correctly, FP (false positives) is the number of healthy nodes that are incorrectly identified as faulty, and FN (false negatives) is the number of faulty nodes that are not detected by the fault detection algorithm. This metric computes the overall fault detection accuracy for each tested scenario.

We evaluated the accuracy of the proposed method against baseline techniques under fault scenarios involving both a small number of faulty nodes (up to four) and a majority of faulty nodes (up to eight). Table III presents the results for the scenario with fewer faulty nodes, where the proposed approach maintains high accuracy as compared to baseline techniques. In cases where the majority of faulty nodes are considered, as shown in Table IV, our method still exhibits higher accuracy as compared to baselines that demonstrate a significant decline in performance, as they fail to handle scenarios with a majority of faulty nodes.

To further assess the fault detection capability of our approach, we generate the receiver operating characteristic (ROC) curve, for different fault scenarios and types, as shown in Fig. 6.

TABLE III
COMPARING THE ACCURACY (%) OF DIFFERENT TECHNIQUES WHEN UP TO 4 NODES ARE FAULTY

Technique	Fault Type						
	Weak Bias	Strong Bias	Weak Drift	Strong Drift	Weak Noise	Strong Noise	Stuck Fault
Proposed	**99.42**	**99.84**	85.96	**96.22**	**99.29**	**99.89**	80.23
DDKF with GMM (ML)	91.49	91.12	75.87	86.07	91.33	90.63	79.94
DDKF with K-means (ML)	91.67	91.58	75.86	85.85	90.94	90.99	79.94
DDKF with GMM (VHL) [45]	82.44	87.42	90.76	91.27	91.33	91.79	**81.5**
DDKF with K-means (VHL) [44]	81.57	86.75	**91.18**	90.64	91.26	91.06	80.64

TABLE IV
COMPARING THE ACCURACY (%) OF DIFFERENT TECHNIQUES WHEN UP TO 8 NODES ARE FAULTY

Technique	Fault Type						
	Weak Bias	Strong Bias	Weak Drift	Strong Drift	Weak Noise	Strong Noise	Stuck Fault
Proposed	**92.15**	**99.73**	**75.39**	**85.97**	**92.6**	**99.43**	**92.19**
DDKF with GMM (ML)	58.12	58.795	65.08	69.72	60.94	59.39	70.29
DDKF with K-means (ML)	58.97	58.87	65.86	67.96	58.88	59.41	69.34
DDKF with GMM (VHL) [45]	67.43	68.44	60.08	60.33	59.75	58.66	69.69
DDKF with K-means (VHL) [44]	67.77	68.67	60.31	58.81	59.99	58.85	71.8

This curve demonstrates the true positive rate against the false positive rate for different tuning parameter values (λ) of the adaptive threshold defined in (9). The ROC curves illustrate that the proposed technique achieves a higher value true positive rate at a low false positive rate, even in the presence of weak sensor faults.

V. CONCLUSION

This paper proposes a novel TeDKF method for the sensor fault diagnosis and estimation in SNs. By combining an innovative IDB clustering method with DDKF in the TeDKF framework and leveraging intermediate (innovation-based) fusion, the technique effectively detects and isolates faulty sensor measurements. Besides, the proposed innovation-based data fusion approach remarkably reduces computational cost without any degradation in estimation performance. The empirical results have proved the effectiveness of proposed TeDKF method, which demonstrate significantly reduced estimation errors along with improved fault tolerance for a broad range of fault types such as bias, drift, noise, and stuck faults. Future work will focus on distributed sensor fault diagnosis for large-scale nonlinear systems.

REFERENCES

[1] A. Chawla et al., "IoT-based monitoring in carbon capture and storage systems," *IEEE Internet Things Mag.*, vol. 5, no. 4, pp. 106–111, Dec. 2023.

[2] K. Shaheen, A. Chawla, F. E. Uilhoorn, and P. S. Rossi, "Model-based sensor-fault detection and isolation in natural-gas pipelines for transient flow," in *Proc. IEEE SENSORS*, 2023, pp. 1–4.

[3] H. Darvishi, D. Ciuonzo, and P. Salvo Rossi, "Deep recurrent graph convolutional architecture for sensor fault detection, isolation, and accommodation in digital twins," *IEEE Sensors J.*, vol. 23, no. 23, pp. 29877–29891, Dec. 2023.

[4] K. Shaheen, A. Chawla, F. E. Uilhoorn, and P. S. Rossi, "Partial-distributed architecture for multi-sensor fault detection, isolation and accommodation in hydrogen-blended natural gas pipelines," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 35420–35431, Nov. 2024.

[5] S. Zidi, T. Moulahi, and B. Alaya, "Fault detection in wireless sensor networks through SVM classifier," *IEEE Sensors J.*, vol. 18, no. 2, pp. 340–347, Jan. 2018.

[6] S. U. Jan, Y. D. Lee, and I. S. Koo, "A distributed sensor-fault detection and diagnosis framework using machine learning," *Inf. Sci.*, vol. 547, pp. 777–796, 2021.

[7] S. Gnanavel et al., "Analysis of fault classifiers to detect the faults and node failures in a wireless sensor network," *Electronics*, vol. 11, no. 10, 2022, Art. no. 1609.

[8] H. Darvishi, D. Ciuonzo, and P. S. Rossi, "A machine-learning architecture for sensor fault detection, isolation, and accommodation in digital twins," *IEEE Sensors J.*, vol. 23, no. 3, pp. 2522–2538, Feb. 2023.

[9] R. Khan, U. Saeed, and I. Koo, "Robust sensor fault detection in wireless sensor networks using a hybrid conditional generative adversarial networks and convolutional autoencoder," *IEEE Sensors J.*, vol. 25, no. 8, pp. 13912–13926, Apr. 2025.

[10] P. S. Shakunt, "Diagnosis of faults in wireless sensor networks through machine learning approach," in *Proc. Int. Conf. Hum.-Centric Smart Comput.*, 2023, pp. 207–217.

[11] Z. Noshad et al., "Fault detection in wireless sensor networks through the random forest classifier," *Sensors*, vol. 19, no. 7, 2019, Art. no. 1568.

[12] G. H. Adday, S. K. Subramaniam, Z. A. Zukarnain, and N. Samian, "Fault tolerance structures in wireless sensor networks (WSNs): Survey, classification, and future directions," *Sensors*, vol. 22, no. 16, 2022, Art. no. 6041.

[13] S. Sharma, K. Gupta, D. Gupta, S. Rani, and G. Dhiman, "An insight survey on sensor errors and fault detection techniques in smart spaces," *CMES Comput. Model. Eng. Sci.*, vol. 138, no. 3, pp. 2029–2059, 2024.

[14] Y. Tian, J. Wang, Z. Qi, C. Yue, P. Wang, and S. Yoon, "Calibration method for sensor drifting bias in data center cooling system using Bayesian inference coupling with autoencoder," *J. Building Eng.*, vol. 67, 2023, Art. no. 105961.

[15] U. Saeed, Y. -D. Lee, S. U. Jan, and I. Koo, "CAFD: Context-aware fault diagnostic scheme towards sensor faults utilizing machine learning," *Sensors*, vol. 21, no. 2, 2021, Art. no. 617.

[16] L. K. Wardhani, R. A. Febriyanto, and N. Anggraini, "Fault detection in wireless sensor networks data using random under sampling and extra-tree algorithm," in *Proc. 10th Int. Conf. Cyber IT Service Manage.*, 2022, pp. 1–6.

[17] K. Shaheen, A. Chawla, F. E. Uilhoorn, and P. S. Rossi, "Hybrid technique for sensor fault diagnosis in natural-gas pipelines," in *Proc. IEEE SENSORS*, 2024, pp. 1–4.

[18] H. Darvishi, D. Ciuonzo, E. R. Eide, and P. S. Rossi, "Sensor-fault detection, isolation and accommodation for digital twins via modular data-driven architecture," *IEEE Sensors J.*, vol. 21, no. 4, pp. 4827–4838, Feb. 2021.

[19] K. Shaheen, A. Chawla, F. E. Uilhoorn, and P. S. Rossi, "Model-based architecture for multisensor fault detection, isolation, and accommodation in natural-gas pipelines," *IEEE Sensors J.*, vol. 24, no. 3, pp. 3554–3567, Feb. 2024.
[20] M. Khodarahmi and V. Maihami, "A review on Kalman filter models," *Arch. Comput. Methods Eng.*, vol. 30, no. 1, pp. 727–747, 2023.
[21] Z. Feng, G. Wang, B. Peng, J. He, and K. Zhang, "Distributed minimum error entropy Kalman filter," *Inf. Fusion*, vol. 91, pp. 556–565, 2023.
[22] A. Vafamand, B. Moshiri, and N. Vafamand, "Fusing unscented Kalman filter to detect and isolate sensor faults in DC microgrids with CPLs," *IEEE Trans. Instrum. Meas.*, vol. 71, 2021, Art. no. 3503608.
[23] N. Jihani, M. N. Kabbaj, and M. Benbrahim, "Kalman filter based sensor fault detection in wireless sensor network for smart irrigation," *Results Eng.*, vol. 20, 2023, Art. no. 101395.
[24] V. Nkemeni, F. Mieyeville, and P. Tsafack, "A distributed computing solution based on distributed Kalman filter for leak detection in WSN-based water pipeline monitoring," *Sensors*, vol. 20, no. 18, 2020, Art. no. 5204.
[25] J. Yang, W. -A. Zhang, and F. Guo, "Distributed Kalman-like filtering and bad data detection in the large-scale power system," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5096–5104, Aug. 2022.
[26] C. Lo, J. P. Lynch, and M. Liu, "Distributed model-based nonlinear sensor fault diagnosis in wireless sensor networks," *Mech. Syst. Signal Process.*, vol. 66–67, pp. 470–488, 2016.
[27] Z. Xing and Y. Xia, "Distributed federated Kalman filter fusion over multisensor unreliable networked systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 10, pp. 1714–1725, Oct. 2016.
[28] K. Shaheen, A. Chawla, F. E. Uilhoorn, and P. S. Rossi, "Partial-distributed particle filter for multi-sensor fault diagnosis in carbon dioxide pipelines," *IEEE Internet Things J.*, vol. 12, no. 15, pp. 30128–30141, Aug. 2025.
[29] D. -J. Xin, L. -F. Shi, and X. Yu, "Distributed Kalman filter with faulty/reliable sensors based on Wasserstein average consensus," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 4, pp. 2371–2375, Apr. 2022.
[30] M. E. Campbell and N. R. Ahmed, "Distributed data fusion: Neighbors, rumors, and the art of collective knowledge," *IEEE Control Syst. Mag.*, vol. 36, no. 4, pp. 83–109, Aug. 2016.
[31] Z. Wu, M. Fu, Y. Xu, and R. Lu, "A distributed Kalman filtering algorithm with fast finite-time convergence for sensor networks," *Automatica*, vol. 92, pp. 1–8, 2018.
[32] H. Snoussi and C. Richard, "Distributed Bayesian fault diagnosis of jump Markov systems in wireless sensor networks," *Int. J. Sensor Netw.*, vol. 2, no. 5/6, pp. 383–396, 2007.
[33] R. Olfati-Saber, "Distributed Kalman filter with embedded consensus filters," in *Proc. 44th IEEE Conf. Decis. Control, Eur. Control Conf.*, 2005, pp. 8179–8184.
[34] D. D. Paola, A. Petitti, and A. Rizzo, "Distributed Kalman filtering via node selection in heterogeneous sensor networks," *Int. J. Syst. Sci.*, vol. 46, no. 8, pp. 1467–1479, 2015.
[35] J. Hu, L. Xie, and C. Zhang, "Diffusion Kalman filtering based on covariance intersection," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 891–902, Feb. 2012.
[36] T. Jiang, I. Matei, and J. Baras, "A trust based distributed Kalman filtering approach for mode estimation in power systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6.
[37] H. Zhang, X. Zhou, Z. Wang, H. Yan, and J. Sun, "Adaptive consensus-based distributed target tracking with dynamic cluster in sensor networks," *IEEE Trans. Cybernetics*, vol. 49, no. 5, pp. 1580–1591, Apr. 2018.
[38] J. Zhang and S. Zhao, "Distributed adaptive Tobit Kalman filter for networked systems under sensor delays and censored measurements," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 445–458, 2022.
[39] C. Hu and B. Chen, "An efficient distributed Kalman filter over sensor networks with maximum correntropy criterion," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 433–444, 2022.
[40] C. Liu, B. Jiang, Y. Li, and R. J. Patton, "Distributed event-triggered fault-tolerant consensus control of multi-agent systems under DoS attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 10, pp. 390–402, 2024.
[41] K. Shaheen, A. Chawla, F. E. Uilhoorn, and P. S. Rossi, "Sensor-fault detection, isolation and accommodation for natural-gas pipelines under transient flow," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 10, pp. 264–276, 2024.
[42] C. Liang, F. Wen, and Z. Wang, "Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks," *Inf. Fusion*, vol. 46, pp. 44–50, 2019.
[43] J. Luo and H. Zhu, "GMM-based distributed Kalman filtering for target tracking under cyber attacks," *IEEE Sens. Lett.*, vol. 8, no. 1, Jan. 2024, Art. no. 6000604.
[44] F. S. Cattivelli and A. H. Sayed, "Diffusion strategies for distributed Kalman filtering and smoothing," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2069–2084, Sep. 2010.
[45] V. D. Blondel, J. M. Hendrickx, A. Olshevsky, and J. N. Tsitsiklis, "Convergence in multiagent coordination, consensus, and flocking," in *Proc. 44th IEEE Conf. Decis. Control*, 2005, pp. 2996–3000.
[46] T. J. van den Boom and B. De Schutter, "Modelling and control of discrete event systems using switching max-plus-linear systems," *Control Eng. Pract.*, vol. 14, no. 10, pp. 1199–1211, 2006.

Khadija Shaheen (Member, IEEE) received the M.Sc. degree in electrical engineering with specialization in digital systems and signal processing from the School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, Pakistan. She is currently working toward the Ph.D. degree in electronics with the Department Electronic Systems, Norwegian University of Science and Technology, Trondheim, Norway. Her research interests include sensor validation, machine learning, and digital signal processing.

Apoorva Chawla (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Gautam Buddh Technical University, Greater Noida, India, in 2012, and the M.Tech. and the Ph.D. dual degree in electrical engineering from the Indian Institute of Technology Kanpur, Kanpur, India, in 2022. She is currently a Postdoctoral Researcher with the Department of Electronic Systems, Norwegian University of Science and Technology, Trondheim, Norway. Her research interests include sensor validation, Internet of Things, distributed detection, wireless communication, and signal processing. She was awarded TCS Research Fellowship for pursuing graduate studies at the Indian Institute of Technology Kanpur. In 2019, she was selected as one of the finalists for Qualcomm Innovation Fellowship by Qualcomm, India.

Pierluigi Salvo Rossi (Senior Member, IEEE) was born in Naples, Italy, in 1977. He received the Dr.Eng. (summa cum laude) degree in telecommunications engineering, and the Ph.D. degree in computer engineering from the University of Naples Federico II, Naples, Italy, in 2002 and 2005, respectively. He was with the University of Naples Federico II, Second University of Naples, Naples, Norwegian University of Science and Technology (NTNU), Trondheim, Norway, and Kongsberg Digital AS, Norway. He held visiting appointments with Drexel University, Philadelphia, PA, USA, Lund University, Lund, Sweden, NTNU, and Uppsala University, Uppsala, Sweden. He is currently a Full Professor and Deputy Head with the Department Electronic Systems, NTNU. He is also a part-time Research Scientist with Department Gas Technology, SINTEF Energy Research, Trondheim. His research interests include communication theory, data fusion, machine learning, and signal processing. Prof. Salvo Rossi was awarded as an Exemplary Senior Editor of the IEEE Communications Letters in 2018. He is/was with the Editorial Board of IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, IEEE SENSORS JOURNAL, IEEE COMMUNICATIONS LETTERS, and IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.