Mr. Akshai Vinu. K, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Resilient Event Triggered Estimation under Coordinated False Data Injection Attacks

Mr. Akshai Vinu. K, Dr. F. Ramesh Dhanaseelan Professor , Dr. M. Jeya Sutha Associate Professor

Department of Computer Applications,St. Xavier's Catholic College of Engineering,
Chunkankadai, Nagercoil-629 003

Abstract- Distributed state estimation in nonlinear systems faces critical security and efficiency challenges, particularly under stealthy cyber-attacks and energy constraints. This project introduces a detection strategy for nonlinear consensus filters, allowing sensor nodes to verify local state estimates and error covariances to identify subtle intrusions. To enhance resource efficiency, an event-triggered distributed Cubature Kalman filtering (DKF) algorithm is proposed. Unlike traditional methods that require continuous data transmission, this approach activates updates only when necessary, significantly reducing communication overhead while maintaining estimation accuracy. Stability analysis confirms the reliability of the algorithm, ensuring robust performance even in adversarial conditions. Practical implementation in sensor networks demonstrates its effectiveness in mitigating stealthy attacks and optimizing energy consumption. By integrating advanced detection mechanisms with event-driven filtering, this work provides a secure, efficient, and resilient solution for nonlinear state estimation in distributed systems.

Keywords- Event-triggered estimation, Distributed Cubature Kalman Filtering, Stealthy Cyber-Attacks, Wireless Sensor Networks, Resilient State Estimation.

I. INTRODUCTION

Distributed state estimation has emerged as a vital strategy in both defense and civilian applications due to its ability to deliver high-precision results while minimizing communication overhead [1–3]. To support coordinated estimation across networked systems, a variety of consensus- based filtering algorithms have been developed—focusing on consensus over state estimates [4], information matrices [5], and observation data [6]. Among these, consensus on information is particularly valued for its ability to ensure system stability with minimal requirements, such as collective detectability and consistent network connectivity [7]. This approach has garnered substantial interest from the research community, leading to numerous advancements and practical implementations.

Recent studies have further explored consensus on information-based estimation specifically in linear systems [8–10]. However, as real-world environments often exhibit nonlinear dynamics, extensions of Kalman filter variants— such as the Extended Kalman Filter (EKF), Unscented Kalman Filter (UKF), and Cubature Kalman Filter (CKF)— have been adapted for use in distributed, nonlinear consensus scenarios. In addition to handling nonlinearities, modern systems must contend with increasing cyber-security challenges. Within wireless sensor networks, the data shared among distributed filters is particularly vulnerable to malicious interference. While Denial-of-Service (DoS)attacks disrupt communication by overwhelming wireless channels, deception-based attacks pose an even greater threat by subtly manipulating transmitted data. These stealthy intrusions are capable of degrading estimation accuracy without immediate detection.

Stealthy attacks are especially dangerous in the context of nonlinear information consensus filters because they can simultaneously alter both local state estimates and associated error covariances, leading to significant performance degradation. As a result, securing distributed estimation frameworks against such covert threats has become an urgent and important research direction.

II. RELATED WORKS

Related Work Xudong Wang introduces a secure interval estimation method for nonlinear cyber-physical systems (CPSs) facing stealthy attacks. By implementing a dynamic event-triggered scheme (DETS), the approach minimizes unnecessary communication overhead while ensuring accurate state estimation. The method transforms nonlinear error dynamics into a linear parameter-varying (LPV) framework to maintain stability and performance. Using a zonotope-based estimation algorithm, the approach accounts for disturbances, measurement noise, nonlinearities, and adversarial attacks. Simulations on a vehicle lateral dynamic system demonstrate its resilience and effectiveness.
Yahan Deng investigates stealthy insider attacks on stochastic event-based state estimation, where a smart sensor using a Kalman filter transmits local estimates. The attack manipulates the scheduler by reversing the triggering condition and altering schedule parameters to degrade remote estimation accuracy. The study introduces the complete Gaussian crater (CGC) distribution to analyze innovation properties within the event-triggered scheme (ETS) and extends it to model packet loss effects. A closed-form expression for estimation error covariance under attack is derived. Additionally, a strategy leveraging Markov chain ergodicity is proposed to evade communication rate detection. Simulations confirm the attack's effectiveness in impairing estimation performance.
Abdul Basit explores secure filtering for discrete-time nonlinear systems in wireless sensor networks (WSNs) facing deception attacks and dynamic topologies. The study addresses stochastic attacks on both measurement and state estimate channels, incorporating a time-varying network topology modeled by a homogeneous Markov chain. An event-triggered set-membership filtering framework ensures bounded estimation errors despite perturbations and attacks. The analysis extends to nonlinear systems with global and local Lipschitz conditions, converting the filter design into a convex optimization problem to determine optimal gains andXXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE ellipsoidal estimates.

The paper presents the first investigation into secure ellipsoidal filtering for locally Lipschitz nonlinear systems under two-channel stochastic attacks, with simulations validating its effectiveness.

Jiahao Huang addresses security challenges in consensus- based distributed state estimation under stealthy attacks. Each node is equipped with an attack defender relying on its sensor measurements. The study examines resilience and convergence in two attack scenarios: one where attackers have sufficient communication resources to degrade estimation, and another where attackers operate with limited resources.

Optimal attack conditions and Kalman gain adjustments are derived to quantify and mitigate estimation performance degradation. Sufficient conditions for estimation convergence are established, with numerical simulations validating the effectiveness of the defense mechanisms in ensuring network resilience.

Guangdeng Chen presents a tracking control method for nonlinear systems under sparse sensor attacks, where adversaries can manipulate nearly half of the measurements. A sampled-data event-triggered strategy is introduced to minimize unnecessary transmissions while ensuring data reliability through a selector mechanism. An improved continuous-discrete observer estimates system states from event-triggered outputs rather than traditional time-triggered samples. A backstepping approach incorporating tracking differentiators is employed for controller design. The method's effectiveness is validated through simulations on a rigid aircraft system.

III. METHODOLOGY

The proposed system follows a decentralized architecture where each sensor node functions autonomously with its own estimator, scheduler, and attack detection module. These components interact across a wireless sensor network and collaboratively perform distributed state estimation. This design eliminates dependency on any central controller, enabling the network to scale efficiently and remain resilient under partial node failure or communication issues.

Instead of sending data at regular intervals, the system employs an event-triggered approach that monitors for significant changes in local estimates. When such changes surpass a predefined threshold, only then is the data transmitted. This reduces communication overhead and conserves energy—both critical factors in wireless sensor networks. Each node runs a Cubature Kalman Filter (CKF), chosen for its high accuracy in nonlinear environments and its suitability for lightweight, real-time computation.

Security is reinforced through a dedicated stealthy attack detection mechanism. This module continuously monitors inconsistencies in the received data and error covariances. If deviations suggest manipulation—such as a false data injection that avoids typical alarm thresholds—it is flagged and isolated, ensuring contaminated information does not propagate through the network. The detector enhances system resilience without introducing significant computational burden.

The system is implemented using Java and evaluated under varying network sizes and attack conditions. Performance metrics like estimation error, communication cost, energy consumption, and attack detection rate are recorded. Results show a clear improvement in scalability, energy efficiency, and resilience when compared to centralized or periodic estimation methods. The lightweight nature of the proposed approach makes it suitable for real- time, secure applications across fields like industrial monitoring, environmental sensing, and intelligent transportation systems. The Fig 1 shows the Architecture of the proposed system.

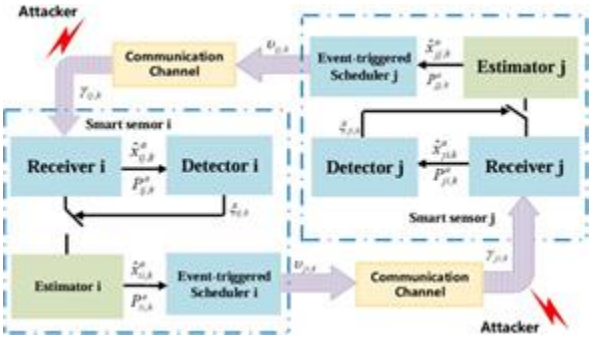

Fig 1: Architecture Diagram.

The proposed architecture features a decentralized network of smart sensor nodes designed for secure and efficient state estimation in nonlinear environments. Each node is equipped with its own estimator, an event-triggered scheduler, and a security detector, allowing it to operate independently while collaborating with neighboring nodes. The Cubature Kalman Filter (CKF) is employed locally to process state estimates with nonlinear precision, while the scheduler ensures data is only transmitted during meaningful state changes. This design conserves energy and reduces bandwidth usage significantly. Communication between nodes occurs wirelessly, making the system more scalable but also more susceptible to stealthy attacks—subtle manipulations that avoid immediate detection.

To counteract this, each node includes a stealthy attack detection module that continuously monitors both internal estimates and incoming messages from peers. By analyzing patterns in error covariance and deviations in expected state values, it can flag and neutralize suspicious data. The system architecture also incorporates receivers, buffers, and scheduling interfaces to manage the flow of data and ensure resilience, even in the face of partial node failures or adversarial interference. Together, the modular design and layered defense mechanisms support a robust, scalable, and intelligent estimation process suitable for real-time applications such as environmental monitoring,

industrial automation, and cyber-physical infrastructure.

IV. PROPOSED ALGORITHM

Kalman Filtering Algorithm

The Kalman Filtering algorithm is a powerful recursive method used for estimating the internal state of dynamic systems, even in the presence of noisy measurements. It operates in two steps: first predicting the system's future state based on prior knowledge and then correcting that prediction using actual sensor data to produce an optimal estimate. Complementing this, the Quartz algorithm schedules tasks to run at specific time intervals or events. By waiting an initial delay and then repeatedly executing tasks at fixed intervals, it ensures timely and efficient operation in systems requiring precise coordination. Together, these algorithms offer robust, accurate, and energy-efficient solutions for distributed systems, especially those vulnerable to unpredictable conditions or cyber threats.

Initialization (at time t = 0)
Before starting the filter, initialize the state estimate and error covariance:

Prediction Step (Time Update)

This step predicts the state and its uncertainty at the next time step based on the previous state estimate.

State Prediction:
Covariance Prediction:

Update Step (Measurement Update)
This step corrects the predicted estimate using the measurement zkz_kzk.

Compute the Kalman Gain:
Update the State Estimate:
Update the Covariance Matrix:

Quartz Algorithm
Step 1: Define Parameters
Let
T = fixed interval between task executions D = initial delay before first execution t_0 = system start time t_1 = time of first execution → $t_1 = t_0 + D$
n = execution count (starting at 1)
Step 2: Wait for Initial Delay

Scheduler pauses for duration D before beginning.
Wait until $t_1 = t_0 + D$
Step 3: Repeat Execution in Loop
For each execution n:
Calculate Scheduled Execution Time
$t_n = t_1 + (n - 1) \times T$ Where:

- t_n is the ideal time for the n^{th} execution.
- $n \in \{1, 2, 3, \ldots\}$

Wait Until t_n
Wait until current_time = t_n
Run the Task
Execute task at time t_n
Step 4: Increment Execution Count
n = n + 1
Then go back to Step 3 unless stopping criteria are met.
To stop after N executions:
If n > N → Terminate

V. RESULTS AND DISCUSSION

The existing system employs a centralized Kalman Filtering approach with periodic transmissions, resulting in several limitations. These include low energy efficiency due to constant transmissions, inefficient bandwidth usage from sending unnecessary data, and poor scalability as centralized processing struggles in large networks. Additionally, the existing system suffers from high latency in large networks due to central computation and has weak security mechanisms, making it vulnerable to stealthy attacks. Furthermore, the system's fault tolerance is low, as failure at the central unit can affect the entire system, and the computation load is high on the central unit, leading to a short network lifetime due to energy drain. In contrast, the proposed system adopts a Distributed Cubature Kalman Filtering approach triggered by events, which significantly enhances performance. This approach optimizes

energy efficiency by reducing transmissions to only when significant data changes occur, conserves bandwidth by transmitting only essential data, and supports large-scale deployment through distributed processing across nodes. The proposed system also features robust security with pattern-based stealthy attack detection mechanisms, exhibits high fault tolerance by allowing operation even with some node failures, and reduces latency due to parallel local processing at nodes. By distributing the computation load across nodes, the proposed system prolongs network lifetime and provides a more efficient, scalable, and secure solution. This makes it highly suitable for real-world applications that require reliable and effective performance in complex environments. The proposed system's improvements enable it to support a wide range of applications, from kinship verification to large-scale tracking and monitoring systems.

VI. CONCLUSION

The Event-Triggered Distributed Cubature Kalman Filtering (ET-DCKF) algorithm plays a crucial role in ensuring accurate state estimation in sensor networks, particularly in environments vulnerable to stealthy cyber- attacks. By employing an event-triggered mechanism, this algorithm reduces the frequency of state updates, thereby optimizing network resources such as bandwidth and energy. The distributed architecture enables collaborative data fusion among sensors, enhancing robustness and accuracy. Moreover, the integration of the Cubature Kalman Filter (CKF) improves nonlinear state estimation performance, making it more effective for real-time applications. However, the presence of stealthy attacks poses a significant challenge, as these attacks are designed to evade traditional anomaly detection techniques while subtly degrading estimation accuracy.

This study highlights how the ET-DCKF algorithm can mitigate the impact of such threats by leveraging adaptive event-triggered thresholds and incorporating innovative anomaly detection techniques. Through simulation results and theoretical analysis, it has been demonstrated that this filtering algorithm enhances resilience against stealthy attacks while maintaining efficient resource utilization. Overall, ET-DCKF presents a promising approach for secure and efficient distributed estimation in sensor networks.

REFERENCES

1. Anderson, B. D. O., & Moore, J. B. (1979). Optimal Filtering.
2. Prentice-Hall Arulampalam, M. S., Maskell, S., Gordon, N., & Clapp, T. (2002). A Tutorial on Particle Filters for Online Nonlinear/Non-Gaussian Bayesian Tracking. IEEE Transactions on Signal Processing.
3. S Bar-Shalom, Y., Li, X. R., & Kirubarajan, T. (2001). Estimation with Applications to Tracking and Navigation. Wiley-Interscience
4. Chen, Z., & Guo, L. (2013). Event-Triggered Control and Filtering of Networked Control Systems. Springer.
5. He, H., Yan, J., & Xu, Y. (2017). Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey. IEEE Transactions on Industrial Informatics.
6. Julier, S. J., & Uhlmann, J. K. (1997). A New Extension of the Kalman Filter to Nonlinear Systems. SPIE Proceedings.
7. Li, X. R., & Jilkov, V. P. (2003). Survey of Maneuvering Target Tracking: Dynamic Models. IEEE Transactions on Aerospace and Electronic Systems.
8. Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., & Sastry, S. (2007). Foundations of Control and Estimation over Wireless Networks. Proceedings of the IEEE.
9. Simon, D. (2006). Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches. Wiley.
10. Zhang, Y., & Varshney, P. K. (2010). Distributed Detection and Data Fusion. Springer.