International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.34, August 2025

Secure Extended Kalman Filter-Based State Estimation and PID Controller for Resilience Water Systems under Sensor False Data Injection Attacks

MD Masud Rana
Computer Science
Lamar University
4400 MLK Blvd
Beaumont, Texas 77710

Bo Sun
Computer Science
Lamar University
4400 MLK Blvd
Beaumont, Texas 77710

ABSTRACT

Secure state estimation and optimal control in cyber-physical systems (CPS) such as interconnected water tanks are necessary to ensure reliability, safety, and stability under adversarial conditions. This paper identifies three key research challenges: (1) Develop an attack-resilient water level state estimation process under false data injection attacks, (2) Design an optimal controller for maintaining stability of water levels, and (3) Conduct extensive simulations to find a suitable solution for practical water system implementation under adversarial conditions. These are critical business issues, as water cannot be stored in a large- scale, however water is essential for daily life and industries. Therefore, it is important to know the water level observability through state estimation process, afterward we will need to apply the control framework to maintain the water level stability as an acceptable level. To address these important challenges, this paper proposes the Chi-square residual based extended Kalman filter algorithm for accurate water level estimation under adversarial conditions. Afterwards, the PID controller is adopted to maintain the stability of the water level at the reference position. Extensive simulations demonstrate that the proposed algorithm can estimate and maintain water level at an acceptable level in a short period of time. Hopefully, these contributions and findings can significantly help cybersecurity education, CPS secure control ecosystems, and water reservoir framework development.

General Terms

Water Systems, Kalman Filter

Keywords

Extended Kalman filter, False data injection attacks; State estimation, Water-tank digital twins

1. INTRODUCTION

Water is one of the most important parts of our daily life, and the water system can integrate the physical process, communication network, sensors, valves, and cyber infrastructure [1], [2]. This cyber-physical integration introduces critical vulnerabilities to cyber threats, especially false data injection (FDI) and denial of service (DoS) attacks. In water ecosystems, the sensors, actuators, and the communication network can play an important role [3]. Due to the limitation of key water sensor data, it is very difficult to analyze this mission critical ecosystem [4]. It should be create significant disruption to the the public and industries [1]. To address these challenges, this paper proposed a Chi-square residual based secure extended Kalman filter (EKF) cyber attach detection, mitigation and control method for the water system. The water system digital twin is designed using physical and electric relationships such as Mass balances and Bernoulli's law. The whole process is implemented through software that uses the system dynamics, EKF algorithm, Chi-square residual attack detection and mitigation, and PID control loop in real time, ensuring resilient and accurate operation of the water-level ecosystem. The developed framework is scalable and transferable, and this study contributes to the implementation of a resilient and demand-responsive water network. In future, the data will be available for Lab, research and investigation.

There are some existing methods that have been used for water level digital twin design, state estimation and control. To begin with, the Kalman Filter (KF) method is used for water level prediction, but it is mainly used linear systems [5]. The extended KF is used for the nonlinear system [6], [7] but it has not considered the cyber attacks. Moreover, an even triggered method under DoS attacked is presented in [8]. The ML is used for predicting internal corrosion of crude oil and gas pipelines [9]. Furthermore, an optimal and complex stealthy attack with side information against remote state estimation is demonstrated in [10]. Additionally, an agent-based supervision for service-oriented industrial CPS is derived in [11]. Beside, a reinforcement leaning method is applied for controlling the water levels in [12], and it takes signification amount of time for training the process. Moreover, a mathematical tool for analysis cyber attack has been proposed in [13]. Finally, a factor graph based belief propagation and LSTM based methods are proposed in [14] and [15]. They will need huge amount of data and not scalable. Overall, this process can challenge to this critical infrastructure such as reliability of water level estimation algorithm, controller design and impact analysis. To address these challenges,

this paper proposes the Chi-square residual based extended Kalman filter algorithm for water level estimation under adversarial condition. The PID controller is adopted to maintain water level in the reference position. Extensive simulations demonstrate that the proposed algorithm can able to estimate and maintaining water level at an acceptable level within a short period of time. Hopefully, these contributions can significantly helpful for cybersecurity education, CPS secure control ecosystems and water reservoir framework development.

The reminder of paper is organized as follows. The water system digital twin is designed in Section 2 which follows the EFK algorithm. The simulation result is Section 4 which follows the conclusion.

2. WATER TANK DIGITAL TWIN PROCESS

The figure 1 shows the water tank systems. Here, there are four water tanks and the dynamic system is demonstrated in [16]. It can be seen that it will need to control the level in the lower two water tanks with two pumps. The voltage is applied to water pump. The flow is regulated using valve [18]. The goal is to estimate the water levels in all 4 tanks. The details physical and electrical relationship are described in [16], [17]. Here, the state vector $\mathbf{x} = [h_1\ h_2\ h_3\ h_4]^T$ is the water levels in tanks 1 to 4 (in cm) and the input vector $\mathbf{u} = [u_1\ u_2]^T$ is the control inputs (pump voltages). The nonlinear water tank dynamics are governed by Torricelli's law and pump inflows as follows [19]:

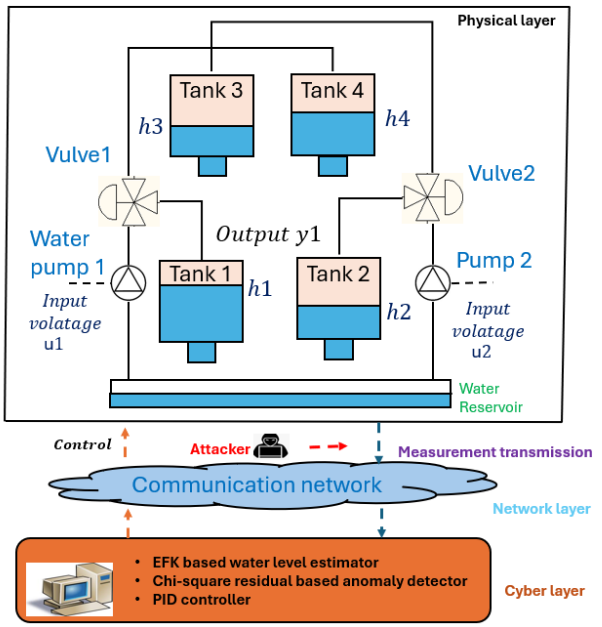

Fig. 1: The quadruple water tank process [16], [17].

$$\frac{dh_1}{dt} = -\frac{a_1}{A_1}\sqrt{h_1} + \frac{k_1\gamma_1}{A_1}u_1$$
$$\frac{dh_2}{dt} = -\frac{a_2}{A_2}\sqrt{h_2} + \frac{k_2\gamma_2}{A_2}u_2$$
$$\frac{dh_3}{dt} = -\frac{a_3}{A_3}\sqrt{h_3} + \frac{k_2(1-\gamma_2)}{A_3}u_2$$
$$\frac{dh_4}{dt} = -\frac{a_4}{A_4}\sqrt{h_4} + \frac{k_1(1-\gamma_1)}{A_4}u_1$$

where a_i is the outlet hole area of tank i, A_i is the cross-sectional area of tank i, k_1,and k_2 are pump gain constants, γ_1, and γ_2 are flow split ratios, $g = 981$ cm/s^2 is the gravitational constant. The measurements are obtained by a set of sensors which can be compromised by false data incretion attacks [20]. For the system dynamics, the Jacobian matrix is:

$$F(\mathbf{x}) = \begin{bmatrix} -\frac{a_1}{2A_1\sqrt{h_1}} & 0 & 0 & 0 \\ 0 & -\frac{a_2}{2A_2\sqrt{h_2}} & 0 & 0 \\ 0 & 0 & -\frac{a_3}{2A_3\sqrt{h_3}} & 0 \\ 0 & 0 & 0 & -\frac{a_4}{2A_4\sqrt{h_4}} \end{bmatrix}$$

We assume that only the tanks (Tank 1 and Tank 2) are directly measured by a set of sensors such as Motorola MPX5010DP (Differential Pressure Sensor):

$$\mathbf{y} = h(\mathbf{x}) = \begin{bmatrix} h_1 \\ h_2 \end{bmatrix}$$

The sensing Jacobian matrix $H = \frac{\partial h}{\partial \mathbf{x}}$ is obtained as follows:

$$H(\mathbf{x}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

From these measurements, we will need to fully estimate all water level then the controller is applied to maintain water level stability.

3. CHI-SQUARE BASED SECURE EXTENDED KF

The Prediction and Correction are the two steps for the EKF algorithm [21], [7].

1. Prediction Step:

$$\hat{\mathbf{x}}_{k|k-1} = \hat{\mathbf{x}}_{k-1|k-1} + T_s f(\hat{\mathbf{x}}_{k-1|k-1}, \mathbf{u}_{k-1})$$

$$P_{k|k-1} = FP_{k-1|k-1}F^\top + Q$$

2. Update Step:

$$\mathbf{y}_k = h(\mathbf{x}_k) + \mathbf{v}_k$$

$$K_k = P_{k|k-1}H^\top(HP_{k|k-1}H^\top + R)^{-1}$$

$$\hat{\mathbf{x}}_{k|k} = \hat{\mathbf{x}}_{k|k-1} + K_k(\mathbf{y}_k - h(\hat{\mathbf{x}}_{k|k-1}))$$

$$P_{k|k} = (I - K_kH)P_{k|k-1}$$

The water sensor attacks are detected by calculating the residual $\mathbf{r} = \mathbf{y} - \mathbf{y}_{\text{pred}}$ using the Chi-square test $\chi^2 = \mathbf{r}^T(HPH^T + R)^{-1}\mathbf{r}$ [22]. If χ^2 exceeds a predefined threshold (e.g., 9.21 for 2 DOF at 95% confidence), the sensory measurement is rejected and replaced with the prediction to maintain state estimation integrity [23]. The

validation and effective of the algorithm is demonstrated through simulation with Python.

4. SIMULATION RESULTS AND DISCUSSIONS

The four-tank ecosystem is implemented using two water level sensors, two voltage-controlled pumps, and a PID controller guided by EKF-based dynamic state estimates. Real-time anomaly detection ensures robust control by switching to predicted measurements during sensor attack conditions. For simulation, a sensor false data injection attack is introduced on the tank one measurement between 10s and 20s, where a constant offset is added to simulate tampering. Having said this, if $100 < k < 200$, then attack on tank one h1 is = 2.0. All the simulation parameters are described in Table I [16], [24]. It includes physical constraints, tank reference values, noise, and other parameters. Considered the four tanks in

Table 1. : Simulation parameters for 4 water tanks.

Key Parameter	Value
g	981 cm/s^2
$A_1 = A_2 = A_3 = A_4$	28.0 cm^2
$a_1 = a_2 = a_3 = a_4$	0.071 cm^2
$k_1 = k_2$	3.33 cm^3/Vs
γ_1	0.7
γ_2	0.6
h_1^{ss}	12.4 cm
h_2^{ss}	12.7 cm
h_3^{ss}	1.8 cm
h_4^{ss}	1.4 cm
T_s	0.1 s
Simulation Time	30 s
Process Noise, Q	$0.001 \cdot \mathrm{I}_4$
Measurement Noise, R	$0.01 \cdot \mathrm{I}_2$
Chi-square Threshold	9.21

Fig.1, the simulation results are described in 2. It can be seen that the proposed EKF algorithm can able to estimate the system states within short time. The EKF successfully detects this anomaly using a chi-square residual test [25], and the mitigation process replaces the corrupted sensor measurement with the predicted value during the attack condition. The cyber attack detection rate is shown 3. Obviously, the mean squared error remains low. The attack detection indicator also indicates timely identification of the injected anomaly, validating the robustness of the EKF estimator.
For better accessibility and visibility, the system has been extended considering 96 tanks. The results are described in Fig. 4. It can be seen that the results are consistence and algorithm can apply large-scale system.
Next our targe is to maintain the water level at an acceptable level. Otherwise the water tank can be overflow and create many problems. After applying the PID, the results are described in Fig. 5. The controller is able to maintain the stability of the water levels within short time.

5. CONCLUSION AND FUTURE WORK

The four-tank water system dynamics with water levels and pump inputs where are nonlinear where output vector cannot be directly measured. After obtaining measurements by sensors, the Chi-square residual based EKF is applied to estimate the water level under adversarial conditions. Simulation results demonstrated

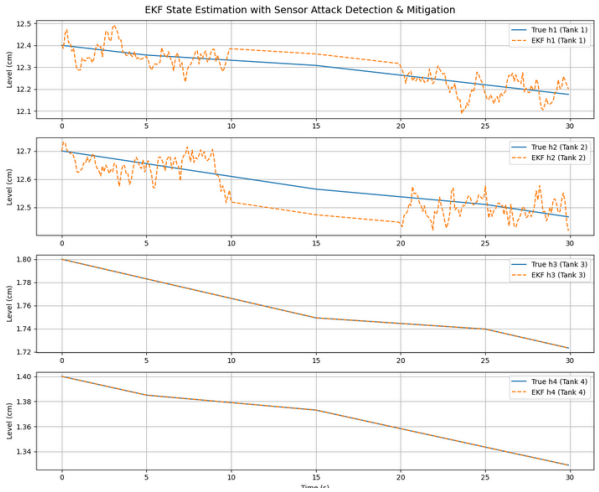

Fig. 2: Water level state estimation results.

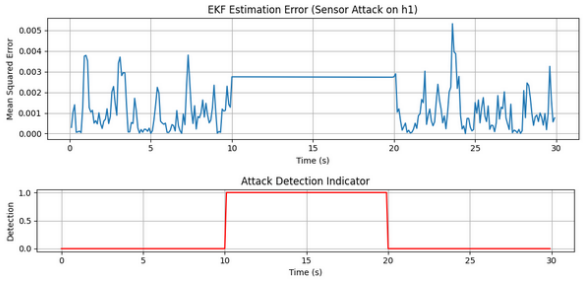

Fig. 3: Attack detection performance.

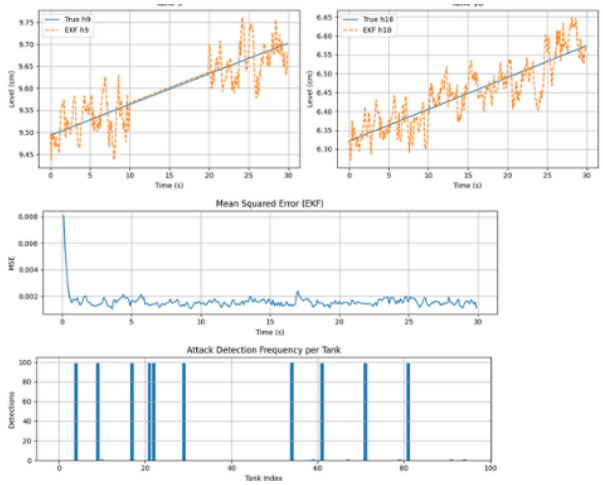

Fig. 4: Estimation simulation results with 96 tanks.

that the EKF algorithm with chi-square residual test can able identified and mitigate the cyber attacks at an acceptable level. The system has been extended to 96 tanks, and it can apply the considered method. Finally, the PID controller is applied to maintain the water levels. In future, we will combine the water system with energy to nexus including corrosion for the real-time CPS application [9].

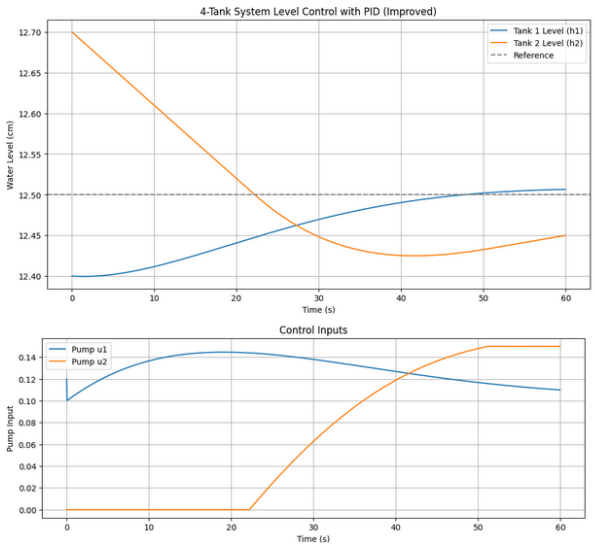

Fig. 5: Simulation results with PID controller.

Hopefully, the proposed framework supports reliable monitoring and control in CPS susceptible to sensor faults or malicious attacks. Additionally, the data will be available for Lab, research and investigation.

6. REFERENCES

[1] N. Tuptuk, P. Hazell, J. Watson, and S. Hailes, "A systematic review of the state of cyber-security in water systems," *Water*, vol. 13, no. 1, p. 81, 2021.

[2] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2020.

[3] Y. H. Choi, A. Sadollah, and J. H. Kim, "Improvement of cyber-attack detection accuracy from urban water systems using extreme learning machine," *Applied Sciences*, vol. 10, no. 22, p. 8179, 2020.

[4] H. Mahmoud, W. Wu, and M. M. Gaber, "A time-series self-supervised learning approach to detection of cyber-physical attacks in water distribution systems," *Energies*, vol. 15, no. 3, p. 914, 2022.

[5] X. Wang and V. Babovic, "Application of hybrid Kalman filter for improving water level forecast," *Journal of Hydroinformatics*, vol. 18, no. 5, pp. 773–790, 2016.

[6] R. Adnan, F. A. Ruslan, and Z. M. Zain, "Extended Kalman Filter (EKF) prediction of flood water level," in *IEEE Control and System Graduate Research Colloquium*. IEEE, 2012, pp. 171–174.

[7] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 13–25, 2012.

[8] X. Li, Z. Tian, and D. Lu, "Event-triggered protocol-based control for cyber-physical systems vulnerable to dual-channel DoS attacks," *IEEE Transactions on Control Systems Technology*, vol. 33, no. 1, pp. 369–383, 2015.

[9] J. Fang, X. Cheng, H. Gai, S. Lin, and H. Lou, "Development of machine learning algorithms for predicting internal corrosion of crude oil and natural gas pipelines," *Computers & Chemical Engineering*, vol. 177, p. 108358, 2023.

[10] L.-W. Mao and G.-H. Yang, "Optimal stealthy attack with side information against remote state estimation: A corrupted innovation-based strategy," *IEEE Transactions on Cybernetics*, vol. 55, no. 2, 2025.

[11] A. Biskupovic, A. Villalonga, F. Castaño, R. E. Haber, and F. Núñez, "Agent-based supervision for service-oriented industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 3, pp. 2719–2728, 2025.

[12] A. Nezamzadeh and M. Esmaeilidehkordi, "Disturbance rejection in quadruple-tank system by proposing new method in reinforcement learning," in *IEEE 14th International Conference on Computer and Knowledge Engineering*. IEEE, 2024, pp. 137–142.

[13] P. Griffioen, B. H. Krogh, and B. Sinopoli, "Ensuring resilience against stealthy attacks on cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 69, no. 12, pp. 8234–8246, 2024.

[14] D. Wang, P. Wang, J. Zhou, L. Sun, B. Du, and Y. Fu, "Defending water treatment networks: Exploiting spatio-temporal effects for cyber attack detection," in *IEEE International Conference on Data Mining*. IEEE, 2020, pp. 32–41.

[15] Q. Han, R. Eguchi, S. Mehrotra, and N. Venkatasubramanian, "Enabling state estimation for fault identification in water distribution systems under large disasters," in *IEEE 37th Symposium on Reliable Distributed Systems*. IEEE, 2018, pp. 161–170.

[16] K. H. Johansson, "The quadruple-tank process: A multivariable laboratory process with an adjustable zero," *IEEE Transactions on Control Systems Technology*, vol. 8, no. 3, pp. 456–465, 2002.

[17] J. Xie, F. Bonassi, and R. Scattolini, "Learning control affine neural narx models for internal model control design," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 8137–8149, 2025.

[18] J. O. d. A. Limaverde Filho, M. T. de Sousa, A. B. Rodrigues, and E. Fortaleza, "A derivative-free Kalman filter-based disturbance observer using flat inputs," in *IEEE International Conference on Automation/XXVI Congress of the Chilean Association of Automatic Control*. IEEE, 2024, pp. 1–6.

[19] O. F. A. Aal and R. Hemeimat, "Data-driven based decoupled control scheme for interacting quadruple tank process," in *IEEE 12th International Conference on Systems and Control*. IEEE, 2024, pp. 149–154.

[20] A. Abughali, M. Alansari, and A. S. Al-Sumaiti, "Deep learning strategies for detecting and mitigating cyber-attacks targeting water-energy nexus," *IEEE Access*, vol. 12, pp. 129 690–129 704, 2024.

[21] G. A. Terejanu *et al.*, "Extended Kalman filter tutorial," *University at Buffalo*, vol. 27, p. 6, 2008.

[22] Y. Takefuji, "Chi-square and P-values versus machine learning feature selection," *Annals of Oncology*, vol. 36, no. 2, pp. 227–228, 2025.

[23] D. M. Bui, D. P. Le, and H. M. Nguyen, "Development of a novel backup fault protection algorithm for low-voltage DC microgrids based on local measurements and Chi-square statistics," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15 106–15 120, 2024.

[24] D. Mikhaylenko and P. Zhang, "Robust mirror attacks on cyber-physical systems," in *IEEE 10th International Conference on Control, Decision and Information Technologies*. IEEE, 2024, pp. 724–729.

[25] C. Ning and Z. Xi, "Improved stealthy false data injection attacks in networked control systems," *IEEE Systems Journal*, vol. 18, no. 1, pp. 505–515, 2024.