Fast Detection of FDI Attacks and State Estimation of Unmanned Surface Vessels Based on Dynamic Encryption

Zheng Liu , Li Liu * , Hongyong Yang , Zengfeng Wang * , Guanlong Deng , Chunjie Zhou

Posted Date: 19 June 2025

doi: 10.20944/preprints202506.1666.v1

Keywords: unmanned surface vessels; cyber-physical systems; FDI attack; dynamic data encryption; H∞ filter

 doi:10.20944/preprints202506.1666.v1

Article

Fast Detection of FDI Attacks and State Estimation of Unmanned Surface Vessels Based on Dynamic Encryption

Zheng Liu, Li Liu *, Hongyong Yang, Zengfeng Wang *, Guanlong Deng and Chunjie Zhou

The School of Information and electrical engineering, LUDONG University, Yantai 264001, China
* Correspondence: liulildu@163.com (L.L.); wzf_ldu@163.com (Z.W.)

Abstract: Wireless Sensor Networks (WSNs) are used for data acquisition and transmission in unmanned surface vessels (USVs). However, the openness of wireless networks makes USVs highly susceptible to false data injection (FDI) attacks during data transmission, which affects the sensors' ability to receive real data and leads to decision-making errors in the control center. In this paper, a novel dynamic data encryption method is proposed whereby data is encrypted prior to transmission and the key is dynamically updated using historical system data, with a view to increasing the difficulty of attackers cracking the ciphertext. At the same time, a dynamic relationship is established between ciphertext, key, and auxiliary encrypted ciphertext, and an attack detection scheme based on dynamic encryption is designed to realize instant detection and localization of FDI attacks. Secondly, the H_∞ fusion filter is designed to filter the external interference noise, and the real information is estimated or restored by the weighted fusion algorithm. Ultimately, the validity of the proposed scheme is confirmed through simulation experiments.

Keywords: unmanned surface vessels; cyber-physical systems; FDI attack; dynamic data encryption; H_∞ filter

1. Introduction

Cyber-physical systems (CPSs) are becoming increasingly important in modern science and technology, especially in areas such as ocean monitoring and defense [1–3]. CPS closely integrates computational, cyber, and physical processes, enabling systems to sense and respond to environmental changes in real time [4–6]. Wireless Sensor Networks (WSNs), as an integrated system, usually integrate multiple sources of sensors and information sources such as Global Navigation Satellite Systems (GNSS), Doppler Velocimeters (DVL), Inertial Navigation Systems (INS), and so on, at their core [7,8]. Through the effective combination of CPS and wireless sensor networks, CPS shows great potential in data acquisition, processing and transmission. Unmanned Surface Vessels (USVs), as a key application of this system [9–11], relies on WSNs for real-time data collection and transmission for efficient monitoring and decision-making in the marine environment [12,13].

The reliability of data is directly related to the USVs' ability to perform its mission [14–16], especially in the complex maritime environment and potential cyberattacks, where ensuring the authenticity and integrity of the data is of particular importance. In USVs applications, WSNs enable these vessels to efficiently perform data acquisition and real-time monitoring in a vast marine environment. By integrating data from different sensors, USVs are able to quickly adapt to complex marine environments, enhancing their operational efficiency and safety. During data measurement and transmission, the data are susceptible to a variety of external disturbances, including marine environmental disturbances (e.g., the effects of wind, waves, currents, etc., on USVs) and signal disturbances, which can lead to variations in the data, further exacerbating the uncertainty in the system's decision-making and thus affecting the safety and efficiency of USVs. To make the data transmission more accurate, the use of WSNs and H_∞ fusion filtering techniques is necessary. In the

 doi:10.20944/preprints202506.1666.v1

recent period, the rapid development of H_∞ filtering technology has provided a new solution for data processing in complex systems [17–19]. With its superior anti-interference ability, this technology can effectively filter external interference noise and improve the reliability and accuracy of data. By fusing data from different sensors, H_∞ fusion filtering can significantly improve the accuracy of the data, thus enhancing the autonomous decision-making level of USVs. This is essential for autonomous navigation and operation of USVs in dynamic and uncertain marine environments.

Although USVs show great advantages in data acquisition and transmission, their high reliance on wireless communication also exposes them to potential cybersecurity threats, especially in terms of False Data Injection (FDI) attacks [20–22]. FDI attacks are a type of cyber-attacks that mislead the system decision-making by tampering or falsifying data, and the attacker can influence the behaviour of the USVs through these false data, leading to wrong navigation and decision-making. FDI attacks are highly stealthy, and malicious attackers are often able to inject false information into USVs through wireless networks without being detected [23–25]. Such attacks can not only mislead the USVs' mission execution, e.g., wrong course selection or improper action strategies, but also lead to more serious consequences such as personnel casualties. In addition, FDI attacks may also cause a chain reaction to other USVs-dependent data systems, affecting the overall efficiency of maritime surveillance and defence. Therefore, the development of effective protective measures and data processing strategies has become an urgent need for current research.

Currently, many researches have been conducted for FDI attacks. For example, Chen et al. [26] developed a framework capable of simultaneously estimating system states and FDI attack signals under FDI and denial-of-service attacks and implementing compensatory control. At the same time, a novel co-design methodology was developed. The method is capable of estimating and compensating unknown FDI attacks without relying on any a priori constraints on the frequency, duration, or derivatives of the FDI attack signals, and effectively suppressing their negative impacts. The compensation method is effective against jamming attacks, however, the FDI attack is detected only after the injection into the system, when the system state information has been tampered with.

To address the above FDI detection issues, Xia et al. [27] proposed a distributed detection method, which consists of two steps: the kernel entropy-based discrimination scheme identifies secure nodes and attacked nodes by calculating the kernel entropy of the measured data between nodes, while the state-aware scheme enables each node to monitor its own state and filter reliable neighbouring nodes. They theoretically derive the conditions that guarantee the stability of the algorithm's mean value and reveal how its performance changes under an FDI attack.

Zhang et al. [28] introduced the adaptive backstepping technique into nonlinear CPS and integrated the dynamic surface control technique, which successfully overcame the computational complexity (computational explosion) problem existing in the traditional backstepping method. The method significantly reduces the computational burden by bypassing the direct complex computation of higher-order systems through stepwise design of virtual control inputs. In addition, they developed a novel defense strategy centered on a nonlinear interference observer. The strategy is capable of accurately estimating the external composite disturbances and substantially improving the system robustness. The nonlinear disturbance observer dynamically estimates the magnitude of the disturbance and its trend by monitoring the system state and output in real time, enabling the controller to compensate accordingly in real time, thus effectively enhances the system's stability when it is subjected to attacks and disturbances. Although the above methods have a certain degree of fault tolerance and FDI attack resistance, they do not solve the privacy protection problem in the data transmission process.

Li et al. [29] designed a low computational complexity encryption scheme for data based on random matrices to achieve instant detection and localisation of FDI attacks during local estimation transmission. Using the results of the encryption detection scheme, a secure fusion estimation algorithm is proposed. The algorithm is able to discard the attacked local estimation information and use only the unattacked local estimation information for fusion estimation. Although the method proposed in

 doi:10.20944/preprints202506.1666.v1

the article has significant advantages in terms of privacy protection of data, the static key it uses lacks forward security and the entire cryptographic detection scheme will fail once it is intercepted on the transmission link or restored through brute force decryption.

Hence, improving the ability of USVs to protect data privacy against FDI attacks and ensuring the accuracy of data estimation through dynamic key management and data encryption techniques has become very meaningful and urgent research. The primary contributions of this paper can be outlined as follows:

- Aiming at the privacy leakage problem during data transmission, this paper proposes a novel dynamic data encryption scheme. The scheme encrypts the data before data transmission and dynamically updates the key by utilizing historical system data, which increases the difficulty for attackers to crack the ciphertext compared to the literature [29].
- Establish a dynamic relationship between the ciphertext, the key and the auxiliary encrypted ciphertext. Once the ciphertext or auxiliary encrypted ciphertext is maliciously tampered with, the dynamic relationship is destroyed. Based on this feature, we design an attack detection scheme based on dynamic data encryption. The scheme can detect FDI attacks in real time and immediately discard the damaged data.
- H_∞ fusion filters are proposed to suppress external noise and interference during data measurement and transmission. The weighted fusion algorithm fuses the data that has not received the attack to more accurately estimate and restore the real signal, ensuring the information integrity and reliability of USVs during data transmission.

The organization of this paper is as follows: Section 2 develops the system model for the problem under consideration; Section 3 details the proposed dynamic data encryption scheme and the FDI attack detection method; Section 4 introduces the design of the H_∞ fusion filter and explores its applications; Section 5 employs simulation experiments to validate the performance of the proposed scheme.

Notations: Let $R^{n\times n}$ denotes the n-dimensional Euclidean space, I and 0 represent the identity matrix and the zero matrix of appropriate dimensions, respectively. The transpose of a matrix is indicated by a superscript T. For any matrix $X \in R^{n\times n}$, the condition $X > 0 (X < 0)$ defines X as a real symmetric positive definite matrix (or a real symmetric negative definite matrix). $\oplus$ represents the XOR operator.

2. System Description

Since USVs are susceptible to the interference of unpredictable environmental factors such as wind and wave currents during navigation, they will not only directly change their motion attitude but also introduce uncertainty noise in their motion control system and sensor measurement data. As shown in Figure 1, when the USVs transmit data to the sensors via the wireless network, the communication link may be subjected to FDI attack, which tamper with the transmitted data, resulting in distortion of the sensor reception, which in turn leads to wrong decision making by the control center.

Based on [14], the mathematical model of the motion of the USVs can be described as $\dot{\eta} = J(\varphi)v$, $M\dot{v} = -Dv + \tau + d(t)$. In which $\eta = [u, v, r]^T$ represents the position vector of the vessel and consisting of north-east position (χ, μ) and bow-rock angle $\sigma \in [0, 2\pi]$,$v = [u, \nu, r]^T$ denotes the USVs velocity vector in the vessel coordinate system, which consists of longitudinal u, transverse ν and bow-rock angular velocities r. The rotation matrix $J(\varphi)$ is expressed as

$$J(\varphi) = \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Based on [30], a class of discrete-time multi-sensor network systems are modelled as follows:

 doi:10.20944/preprints202506.1666.v1

$$\begin{cases} x_{k+1} = Ax_k + B\omega_k \\ y_{i,k} = H_{i,k}x_k + v_{i,k} \\ z_k = Lx_k \end{cases} \tag{1}$$

where, let $x_k = [P_{x,k}, P_{y,k}, \sigma_k]^T$ denotes the position state information, let $x_k = \eta_k$, $(P_{x,k}, P_{y,k})$ denotes position coordinates, σ_k denotes bow rocker. x_k and $y_{i,k}$ are the system state and measured output of the ith sensor at the moment k, respectively. z_k is the state to be estimated. $\omega_k \in R^{n_\omega}$ is an unknown external disturbance, $v_{i,k}$ is a measurement noise belonging to $l_2[0, \infty)$. Matrices A, B, $H_{i,k}$ and L known to have the appropriate dimensions.

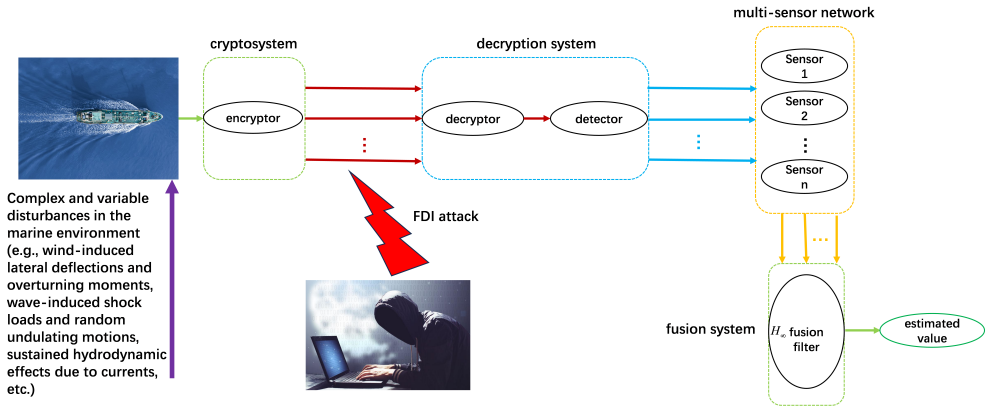

Figure 1. USVs with dynamic data encryption under FDI attack.

At the time of instants of k, each sensor receives a packet from the USVs containing the ciphertext and its auxiliary encrypted ciphertext. The detector applies an attack detection scheme to the packet and discards the packet that has been maliciously altered by the attacker; subsequently, it performs a decryption operation on the ciphertext in the legitimate packet. However, marine environmental disturbances (e.g., the effects of wind, waves, and currents on USVs) are inevitable during data transmission. These disturbances introduce system state noise, which in turn leads to biased data. Therefore, H_∞ fusion filtering is used to filter the interference noise and estimate or restore the real information by weighted fusion algorithm.

As shown in Figure 1, during the transmission of data packets, a malicious attacker may launch an FDI attack on unknown data in the communication links to tamper with these data. Whereas, in a multi-sensor system, due to the limited resources of the attackers, it is unlikely that they can attack all communication links at the same time. Therefore, it is reasonable to assume that there is at least one unattacked communication link in a multi-sensor system. This assumption ensures that the sensors receive at least one true system state. If all of them were attacked, then the sensors would not be able to obtain reliable data.

3. Encryption Attack Detection Scheme

This section designs an attack detection method incorporating dynamic data encryption, aiming to achieve real-time identification of FDI attacks. First, a dynamic data encryption mechanism with low computational overhead is constructed to ensure the security of transmitted data. Subsequently, based on this encryption mechanism, a corresponding attack detection scheme is designed.

3.1. Dynamic Data Encryption Scheme

As shown in Figure 1, local data $x_{i,k}$ is encrypted using a key $c_{i,k}$ before transmission. Once it reaches the decryptor, it will be restored from it using the decryption scheme. The specific encryption scheme is designed as follows:

 doi:10.20944/preprints202506.1666.v1

$$\begin{cases} c_{i,0} = s_{i,0} \\ x^c_{i,k} = x_{i,k} - \varphi(c_{i,k}) \\ E^c_{i,k} = x_{i,k} \oplus c_{i,k} - \varphi(c_{i,k}) \\ c_{i,k+1} = x_{i,k} + s_{i,k} \end{cases} \tag{2}$$

where $c_{i,k} \in \mathrm{R}^{n\times(n+1)}$ is the key in the encryption process, $s_{i,k} \in \mathrm{R}^{n\times(n+1)}$ is a matrix of random numbers with suitable dimensions, $c_{i,k}$ is updated each time by summing with $s_{i,k}$ based on the historical system data to achieve dynamic encryption, and $c_{i,0} = s_{i,0}$ is the given initial key. $x^c_{i,k}$ is the ciphertext corresponding to the encryption of $x_{i,k}$, and $E^c_{i,k}$ is the auxiliary encrypted ciphertext used for detecting FDI attacks. Function $\varphi(c_{i,k}) : \mathrm{R}^{n\times(n+1)} \to \mathrm{R}^{n\times(n+1)}$ is an arbitrary encryption function about $c_{i,k}$. In addition, the encryption function $\varphi(c_{i,k})$ can be selected according to the application scenarios as well as the requirements of computational complexity. After the encryption is completed, the encryptor sends the packet $\{x^c_{i,k}, E^c_{i,k}\}$ to the decryptor through the communication network.

To recover the original data $x_{i,k}$ from $x^c_{i,k}$, the decryption scheme is designed as follows:

$$\begin{cases} d_{i,0} = s_{i,0} \\ x^d_{i,k} = x^c_{i,k} + \varphi(d_{i,k}) \\ D^d_{i,k} = E^c_{i,k} + \varphi(d_{i,k}) \\ d_{i,k+1} = x^d_{i,k} + s_{i,k} \end{cases} \tag{3}$$

where $d_{i,k} \in \mathrm{R}^{n\times(n+1)}$ is the key in the decryption process, $x^d_{i,k}$ is the decrypted value of $x_{i,k}$ and $D^d_{i,k}$ is an auxiliary value to be used in an attack detection scheme.

Notations: under the encryption method (2) and the decryption method (3), a random matrix $s_{i,k}$ is introduced, which has to be consistent during encryption and decryption. In order to ensure that $d_{i,k}$ is equal to $c_{i,k}$, the ciphertext $x^c_{i,k}$ is recovered as $x_{i,k}$. In fact, since the use of the same seed when using a random number generator produces unique random sequences, it is possible to use in (2) and (3) the same random number generator seed to ensure the consistency of $s_{i,k}$, and this is a widely used solution in cryptography [31].

In the attack-free, the following propositions about dynamic data encryption schemes (2) and (3) can be obtained:

Proposition 1. In the absence of FDI attacks, the following conclusions can be drawn using dynamic data encryption schemes (2) and (3):

$$\begin{cases} x^d_{i,k} = x_{i,k} \\ x^d_{i,k} \oplus D^d_{i,k} = d_{i,k} = c_{i,k} \end{cases} \tag{4}$$

Proof 1. According to the dynamic data encryption scheme (2) and (3), $d_{i,k} = c_{i,k}$ is established, when the decryptor receives the data packet $\{x^c_{i,k}, E^c_{i,k}\}$, the decryption process is shown in (5):

$$\begin{cases} x^d_{i,k} = x^c_{i,k} + \varphi(d_{i,k}) = x_{i,k} - \varphi(c_{i,k}) + \varphi(d_{i,k}) = x_{i,k} \\ D^d_{i,k} = E^c_{i,k} + \varphi(d_{i,k}) = x_{i,k} \oplus c_{i,k} - \varphi(c_{i,k}) + \varphi(d_{i,k}) = x_{i,k} \oplus c_{i,k} \end{cases} \tag{5}$$

The decrypted data is then examined using the detection scheme to get the following results

$$x^d_{i,k} \oplus D^d_{i,k} = x_{i,k} \oplus x_{i,k} \oplus c_{i,k} = c_{i,k} = d_{i,k} \tag{6}$$

According to the mathematical description of Eqs. (5)-(6), the correct data can be obtained in the ideal case of FDI attack free, and the attack detection scheme does not detect that the packet suffers from an FDI attack.

 doi:10.20944/preprints202506.1666.v1

3.2. Scheme for Detection of Encryption-Based Attacks

Note that from Proposition 1, it is clear that in the dynamic data encryption schemes (2) and (3), $x_{i,k}^d \oplus D_{i,k}^d = d_{i,k}$, this feature enables us to determine whether the system data has been tampered with by a malevolent attacker. Based on the dynamic data encryption schemes (2) and (3), an attack detection scheme as shown in Algorithm 1 is proposed, which can detect whether the data is attacked by FDI in a very short time.

Algorithm 1 Attack detection algorithm based on dynamic data encryption

Step 1 (encryption process): At moment k, the encryptor executes the encryption process, generates the ciphertext $x_{i,k}^c$ and the auxiliary encryption ciphertext $E_{i,k}^c$, and encapsulates them into a data packet $\{x_{i,k}^c, E_{i,k}^c\}$.
Step 2 (data transmission): The encryptor sends the packet to the decryptor through the communication network.
Step 3 (decryption process): When the decryptor receives the received packet, it performs the decryption process.
Step 4 (Attack Detection): After the decryption process, the following detection scheme is executed.
Case 1: If $x_{i,k}^d \oplus D_{i,k}^d = d_{i,k}$, this received packet is not attacked by FDI. $k \to k+1$, return to step 1.
Case 2: If $x_{i,k}^d \oplus D_{i,k}^d \neq d_{i,k}$, then this received packet is subject to FDI attack. Discard the data packets received on this communication link this time. $k \to k+1$, return to step 1.

Theorem 1. In the absence of FDI attacks, the original data can be recovered using Algorithm 1.
Proof 2. In the absence of a cyberattack, $x_{i,k}^d = x_{i,k}$ is known from Proposition 1, which implies that the original data $x_{i,k}$ can be recovered using Algorithm 1. Also, $x_{i,k}^d \oplus D_{i,k}^d = d_{i,k} = c_{i,k}$ implies that Case 1 in Algorithm 1 is always satisfied.
Remark 1. In encryption schemes (2) and (3), only XOR operations and basic arithmetic operations are employed, featuring low computational complexity. It enhances data security and keeps the system performance overhead within a negligible range.
Remark 2. From Theorem 1, the system exists with a specific dynamic relation, i.e., $x_{i,k}^d \oplus D_{i,k}^d = d_{i,k}$, when there is without FDI attack. This dynamic relation will be changed when subjected to FDI attack. This property can be used as a sufficient criterion for attack detection and provides a theoretical basis for the cryptographic detection algorithm proposed in this paper.

4. H_∞ Fusion Estimation Under FDI Attack

In data transmission, the effects of complex and variable marine environmental disturbances (e.g., wind-induced offsets, wave-induced impacts, etc.) on USVs are unavoidable. These powerful environmental factors can cause unpredictable attitude changes and position drifts of USVs, resulting in increased system state noise and biased data. For this reason, the H_∞ fusion filtering technique is used to filter out the noise, and the real state information is estimated by a weighted fusion algorithm.

4.1. The effectiveness of the encryption-based attack detection scheme in detecting FDI attacks

In Algorithm 1, $x_{i,k}^c$ and $E_{i,k}^c$ will be packaged and sent to the decryptor via the communication network. It is assumed that the attacker can recognize $x_{i,k}^c$ and $E_{i,k}^c$ to implement the tampering. The attack strategy consists of the following three scenarios:

Scenario 1: The attacker modifies only $x_{i,k}^c$ as follows:

$$x_{i,k}^{'c} = x_{i,k}^c + a_{i,k} \tag{7}$$

Scenario 2: The attacker modifies only $E_{i,k}^c$ as follows:

$$E_{i,k}^{'c} = E_{i,k}^c + b_{i,k} \tag{8}$$

 doi:10.20944/preprints202506.1666.v1

Scenario 3: The attacker modifies both $x_{i,k}^c$ and $E_{i,k}^c$ as follows:

$$\begin{cases} x_{i,k}^{'c} = x_{i,k}^c + a_{i,k} \\ E_{i,k}^{'c} = E_{i,k}^c + b_{i,k} \end{cases} \tag{9}$$

where $a_{i,k}$ and $b_{i,k}$ are arbitrary non-zero attack signals of the appropriate dimensions.

Theorem 2. For Algorithm 1, if the FDI attacks Eqs. (7)-(9) in scenarios 1-3 at time k, the encryption-based attack detection algorithm will trigger an alert immediately from time k onwards.

Proof 3. If the FDI attack under Eq. (7) in Scenario 1 starts at time k, the decryption process is as follows:

$$\begin{cases} x_{i,k}^{'d} = x_{i,k}^{'c} + \varphi(d_{i,k}) \\ \quad = x_{i,k} + a_{i,k} \\ D_{i,k}^d = E_{i,k}^c + \varphi(d_{i,k}) \\ \quad = x_{i,k} \oplus c_{i,k} \end{cases} \tag{10}$$

Then, the improved format can be obtained

$$x_{i,k}^{'d} \oplus D_{i,k}^d = [x_{i,k} + a_{i,k}] \oplus [x_{i,k} + c_{i,k}] = a_{i,k} \oplus c_{i,k} \neq d_{i,k} \tag{11}$$

If the FDI attack (8) in scenario 2 begins at the time k, the decryption process is defined as follows:

$$\begin{cases} x_{i,k}^d = x_{i,k}^c + \varphi(d_{i,k}) = x_{i,k} \\ D_{i,k}^{'d} = E_{i,k}^{'c} + \varphi(d_{i,k}) \\ \quad = x_{i,k} \oplus c_{i,k} + b_{i,k} \end{cases} \tag{12}$$

And thus, it can be derived that

$$x_{i,k}^{'d} \oplus D_{i,k}^{'d} = x_{i,k} \oplus x_{i,k} \oplus c_{i,k} + b_{i,k} = c_{i,k} + b_{i,k} \neq d_{i,k} \tag{13}$$

From the mathematical description of Eqs. (10)-(13), it can be seen that Scenario 1 and Scenario 2 always satisfy the Case 2 decision condition in Algorithm 1, which ensures that the encryption-based attack detection algorithm achieves a zero-delay alarm at the attack initiation moment k. For the FDI attack corresponding to Scenario 3 (Eq. (9)), the consistency conclusion can be obtained by the same methodological derivation, and its proof process is omitted here.

4.2. H_∞ Fusion Estimation Based on Fast Attack Detection

Although attack detection algorithms can effectively filter out data tampered with by malicious attackers, the external noise interference inherent in the measurement and transmission process can still lead to biased system state information obtained by the sensors, which in turn affects the accuracy of control decisions. Therefore, the aim of this study is to design the H_∞ filter that mitigates the effect of noise on the estimated system state. The H_∞ filter is able to effectively cope with the noise and ensure that the system can still provide accurate state estimation and control in the event of noise interference. Then, a secure fusion estimation algorithm is proposed to perform optimal weighted fusion of unattacked data, thereby significantly improving the accuracy of state estimation while ensuring security and enabling more precise estimation and reconstruction of the true signal.

Consider the following local filter structure on sensor i:

$$\begin{cases} \hat{x}_{i,k+1} = A_{pi}\hat{x}_{i,k} + B_{pi}y_{i,k} \\ \hat{z}_{i,k} = C_{pi}\hat{x}_{i,k} \end{cases} \tag{14}$$

where $\hat{x}_k$ and $\hat{z}_k$ are the estimated values of x_k and z_k, respectively. A_{pi}, B_{pi} and C_{pi} are the filter parameter matrices to be probe-based.

 doi:10.20944/preprints202506.1666.v1

Introducing the local error $\tilde{z}_{i,k} = z_k - \hat{z}_{i,k}$ and combining Eqs. (1) and (14), the local filtering error system for sensor i is established as follows:

$$\begin{cases} \varsigma_{i,k+1} = \bar{A}_i \varsigma_{i,k} + \bar{B}_i \omega_k + \bar{D}_i v_{i,k} \\ \tilde{z}_{i,k} = \bar{C}_i \varsigma_{i,k} \end{cases} \tag{15}$$

In order to facilitate the derivation of the formula for the filter performance, the symbols in Eq. (5). are denoted as follows: $\varsigma_{i,k} = \begin{bmatrix} x_k \\ \hat{x}_{i,k} \end{bmatrix}; \bar{A}_i = \begin{bmatrix} A & 0 \\ B_{pi} H_{i,k} & A_{pi} \end{bmatrix}; \bar{B}_i = \begin{bmatrix} B \\ 0 \end{bmatrix}; \bar{C}_i = \begin{bmatrix} L & -C_{pi} \end{bmatrix}; \bar{D}_i = \begin{bmatrix} 0 \\ B_{pi} \end{bmatrix}$.

$\varsigma_{i,k}$ denotes the state vector of the localized filtering error, $\omega_k \in R^{n_\omega}$ is the unknown external interference, v_k is the measurement noise belonging to $l_2[0, \infty)$, and $\bar{C}_i$ is the gain matrix of the localized filter.

In the case of non-zero noise interference, the stability of the system can be determined by the H_∞ filter performance criterion. Specifically, when the upper bound of the filter output energy is smaller than a given performance criterion, the filter system is proved to be asymptotically stable. Based on the actual noise characteristics and filter structure analysis, the H_∞ performance criterion adopted in this chapter is expressed as follows:

$$\sum_{k=0}^{\infty} \|\tilde{z}_{i,k}\|^2 < l^2 \left(\sum_{k=0}^{\infty} \|\omega_k\|^2 + \sum_{k=0}^{\infty} \|v_{i,k}\|^2 + x_0^T \theta_1 x_0 + (x_0 - \hat{x}_0)^T \theta_2 (x_0 - \hat{x}_0) \right) \tag{16}$$

where θ_1 and θ_2 are the two given positive definite real symmetric auxiliary matrices, and these two parameter matrices achieve boundedness control of the system paradigm through a weight adjustment mechanism.

Theorem 3. For a scalar $\rho > 0$ and real positive definite matrices θ_1 and θ_2, the system (15) is asymptotically stable, if there exists a real symmetric matrix Q satisfying under Eq. (17).

Proof 4. According to the auxiliary matrices P and θ given below, the rewritable inequality satisfying the filter performance criterion is obtained:

$$\begin{cases} \begin{bmatrix} \bar{A}_i^T Q \bar{A}_i + \bar{C}_i^T \bar{C}_i - Q & \bar{A}_i^T Q \bar{B}_i & \bar{A}_i^T Q \bar{D}_i \\ \bar{B}_i^T Q \bar{A}_i & \bar{B}_i^T Q \bar{B}_i - \rho^2 I & \bar{B}_i^T Q \bar{D}_i \\ \bar{D}_i^T Q \bar{A}_i & \bar{D}_i^T Q \bar{B}_i & \bar{D}_i^T Q \bar{D}_i - \rho^2 I \end{bmatrix} < 0 \\ Q < \rho^2 \theta \end{cases} \tag{17}$$

where

$$\mathrm{P} = \begin{bmatrix} \bar{C}_i^T \bar{C}_i - Q & 0 & 0 \\ 0 & -\rho^2 I & 0 \\ 0 & 0 & -\rho^2 I \end{bmatrix}; \theta = \begin{bmatrix} \theta_1 + \theta_2 & -\theta_1 \\ -\theta_1 & -\theta_1 \end{bmatrix}. \tag{18}$$

Proof 5. Set up the Lyapunov function:

$$V_k = \varsigma_{i,k}^T Q \varsigma_{i,k} \tag{19}$$

There are two scenarios that need to be discussed here.

1) When $\omega_k = 0$ and $v_{i,k} = 0$:

$$\begin{aligned} &\Delta V_k \\ &= V_{k+1} - V_k \\ &= \varsigma_{i,k}^T (\bar{A}_i^T Q \bar{A}_i - Q) \varsigma_{i,k} \end{aligned} \tag{20}$$

Considering $\bar{C}_i^T \bar{C}_i \geq 0$ and combining it with Eq. (17) shows the inequality $\bar{A}_i^T Q \bar{A}_i - Q < 0$. Therefore, $\Delta V_k < 0$ guarantees the asymptotic stability of the filter under noiseless conditions.

 doi:10.20944/preprints202506.1666.v1

2) When $\omega_k > 0$ and $v_{i,k} > 0$:

$$\begin{aligned} &\Delta V_k \\ &= V_{k+1} - V_k \\ &= \varsigma_{i,k+1}^T Q \varsigma_{i,k+1} - \varsigma_{i,k}^T Q \varsigma_{i,k} \\ &= \vartheta_{i,k}^T \Xi(Q) \vartheta_{i,k} \end{aligned} \tag{21}$$

Set as $\vartheta_{i,k} = \begin{bmatrix} \varsigma_k \\ \omega_k \\ v_{i,k} \end{bmatrix}; \Xi(Q) = \begin{bmatrix} \bar{A}_i^T Q \bar{A}_i - Q & \bar{A}_i^T Q \bar{B}_i & \bar{A}_i^T Q \bar{D}_i \\ \bar{B}_i^T Q \bar{A}_i & \bar{B}_i^T Q \bar{B}_i & \bar{B}_i^T Q \bar{D}_i \\ \bar{D}_i^T Q \bar{A}_i & \bar{D}_i^T Q \bar{B}_i & \bar{D}_i^T Q \bar{D}_i \end{bmatrix}$.
Continuing the derivation yields:

$$\begin{aligned} \Delta V_k &= V_{k+1} - V_k \\ &= \vartheta_{i,k}^T \Upsilon(k) \vartheta_{i,k} + \rho^2 \omega_k^T \omega_k + \rho^2 v_{i,k}^T v_{i,k} + \tilde{z}_{i,k}^T \tilde{z}_{i,k} \end{aligned} \tag{22}$$

where

$$\Upsilon(k) = \begin{bmatrix} \bar{A}_i^T Q \bar{A}_i + \bar{C}_i^T \bar{C}_i - Q & \bar{A}_i^T Q \bar{B}_i & \bar{A}_i^T Q \bar{D}_i \\ \bar{B}_i^T Q \bar{A}_i & \bar{B}_i^T Q \bar{B}_i - \rho^2 I & \bar{B}_i^T Q \bar{D}_i \\ \bar{D}_i^T Q \bar{A}_i & \bar{D}_i^T Q \bar{B}_i & \bar{D}_i^T Q \bar{D}_i - \rho^2 I \end{bmatrix}$$

Combined with equation (17), the inequality can be written as

$$\Delta V_k - \rho^2 \omega_k^T \omega_k - \rho^2 v_{i,k}^T v_{i,k} + \tilde{z}_{i,k}^T \tilde{z}_{i,k} < 0 \tag{23}$$

Can get

$$\vartheta_{i,k}^T \Upsilon(k) \vartheta_{i,k} < 0 \tag{24}$$

Satisfying

$$\begin{aligned} &\sum_{k=0}^{\infty} \left(\Delta V_k - \rho^2 \omega_k^T \omega_k + \rho^2 vi, k^T vi, k + \tilde{z}_{i,k}^T \tilde{z}_{i,k} \right) \\ &= \sum_{k=0}^{\infty} \left(||\tilde{z}_{i,k}||^2 - \rho^2 (||\omega_k||^2 + ||vi, k||^2) \right) - v_1 < 0 \end{aligned} \tag{25}$$

This can be obtained after further derivation:

$$\sum_{k=0}^{\infty} ||\tilde{z}_{i,k}||^2 < \rho^2 \sum_{k=0}^{\infty} (||\omega_k||^2 + ||v_{i,k}||^2) + v_1 \tag{26}$$

Since $Q < \rho^2 \theta$,

$$\begin{aligned} &\sum_{k=0}^{\infty} \|\tilde{z}_{i,k}\|^2 < \rho^2 \sum_{k=0}^{\infty} (\|\omega_k\|^2 + \|v_{i,k}\|^2) + \rho^2 \begin{bmatrix} x_k & \hat{x}_{i,k} \end{bmatrix} \theta \begin{bmatrix} x_k \\ \hat{x}_{i,k} \end{bmatrix} \\ &= \rho^2 \sum_{k=0}^{\infty} (\|\omega_k\|^2 + \|v_{i,k}\|^2) + \rho^2 \begin{bmatrix} x_k & \hat{x}_{i,k} \end{bmatrix} \begin{bmatrix} \theta_1 + \theta_2 & -\theta_1 \\ -\theta_1 & -\theta_1 \end{bmatrix} \begin{bmatrix} x_k \\ \hat{x}_{i,k} \end{bmatrix} \\ &= \rho^2 \left(\sum_{k=0}^{\infty} (\|\omega_k\|^2 + \|v_{i,k}\|^2) + x_1^T \theta_2 x_1 + (x_1 - \hat{x}_1)^T \theta_2 (x_1 - \hat{x}_1) \right) \end{aligned} \tag{27}$$

And get

$$\sum_{k=0}^{\infty} \|\tilde{z}_{i,k}\|^2 < \rho^2 \left(\sum_{k=0}^{\infty} (\|\omega_k\|^2 + \|v_{i,k}\|^2) + x_1^T \theta_2 x_1 + (x_1 - \hat{x}_1)^T \theta_2 (x_1 - \hat{x}_1) \right) \tag{28}$$

It can be concluded that $\triangle V_k$ satisfies the H_∞ fusion filtering performance criteria of this paper.

 doi:10.20944/preprints202506.1666.v1

Define Λ_k and $\bar{\Lambda}_k$ as the set of attacked local estimation indexes and the set of unattacked local estimation indexes, $\Lambda_k \cup \bar{\Lambda}_k = \{1, 2, ..., n\}$, respectively, at time k. For the multi-sensor configuration of system (1), the proposed distributed H_∞ fusion filter design is presented below:

$$\hat{z}_k = \sum_{i=1}^{n} \iota_i \hat{z}_{i,k} \tag{29}$$

$$\iota_i = \frac{1/\kappa_i^2}{\sum_{j=1}^{n} \kappa_j^2} \tag{30}$$

where $\hat{z}_k$ denotes the fused global estimate, $\iota_i > 0$ denotes the fused weights and satisfies the normalization condition $\sum_{i \in \bar{\Lambda}_k} \iota_i = 1$, n denotes the total number of sensors, and κ_i represents the filter error.

5. Simulations

To verify the effectiveness of the dynamic data encryption fusion estimation strategy for USVs-oriented FDI attacks proposed, a simulation experiment platform is constructed in this study. Based on the dynamics model of USVs and the established system model, it is assumed that the sensor network contains six nodes. In order to enhance the security, the first three sensors receive the first state component of the system, and the last three sensors receive the second state component of the system. During the measurement process, the communication data is affected by the measurement noise $v_{1,k} = 0.022\sin(k), v_{2,k} = 0.044\sin(k)$. The external interference noise $\omega_k = \begin{bmatrix} 0.2\cos(2k) & 0.1\sin(k) \end{bmatrix}^T$ is used to simulate the effect of wind, waves, and other factors on data acquisition and transmission in the marine environment. The simulation duration is set to [0, 100] seconds, and the initial state value of the system is $x_0 = \begin{bmatrix} 1 & 2 \end{bmatrix}^T$. The system parameter matrix is defined as $A = \begin{bmatrix} 0.77 & 0 \\ 0 & 0.77 \end{bmatrix} and B = \begin{bmatrix} 1.1 & 0 \\ 0 & 1.1 \end{bmatrix}$. It is assumed that there exists at least one sensor that is not subject to the FDI attack in the first three sensor groups and the last three sensor groups at any time, and the location of the FDI attack occurs randomly. In addition, we set the value of the attack signal as a random value in the interval [40, 80]. In the dynamic data encryption scheme, the initial key matrix $c_{i,0}$ is randomly generated, and the key $c_{i,k}$ is updated according to the historical system data during the subsequent encryption process, with the update step set to 1. The encryption function $\varphi(c_{i,k}) = -c_{i,k}$. The following H_∞ fusion filter parameters are given according to the Monte Carlo method:

$$A_{pi} = \begin{pmatrix} 0.4 & \\ & 0.4 \end{pmatrix}, B_{pi} = \begin{pmatrix} 0.4 & \\ & 0.4 \end{pmatrix}, C_{pi} = \begin{pmatrix} 1.005 & \\ & 1.005 \end{pmatrix}, F_{pi} = \begin{pmatrix} 0.6 & \\ & 0.6 \end{pmatrix}.$$

To address the issue of privacy protection during data transmission, using dynamic encryption methods for protection. Figure 2 demonstrates the effect of the decryptor on the recovery of key state quantities of the system. Figure (a) depicts the horizontal position of the system ($x_{1,k}$) Dynamic: the black dashed line represents the true horizontal position, and the red line represents the decrypted position ($x_{1,k}^d$) obtained by the decryptor. Figure (b) depicts the velocity of the system ($x_{2,k}$) Dynamic: the black dashed line represents the true velocity, and the blue solid line represents the decryption velocity ($x_{2,k}^d$) obtained by the decryptor. The comparison shows that the positions and velocities output by the decryptor can effectively track and approximate their corresponding true values, indicating that the decryptor has a excellent performance in recovering the position and velocity states of the system.

 doi:10.20944/preprints202506.1666.v1

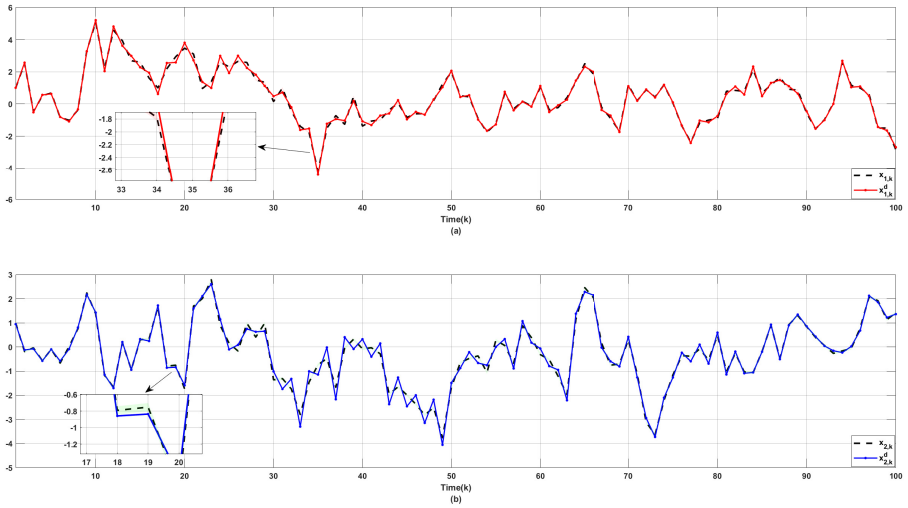

Figure 2. Comparison of real and decrypted values of horizontal position and velocity.

Figure 3 and Figure 5 together show the state observation effect of the multi-sensor system under FDI attack. Figure 3(a) marks the true horizontal position of the system ($x_{1,k}$) by the black dashed line, while presenting the observed values of sensor 1/2/3 pairs of $x_{1,k}$ by the red, blue, and orange solid lines, respectively. And the red block in Figure 3(b) marks the FDI attack occurring at the corresponding moment. Figure 5(a) similarly presents the true speed ($x_{2,k}$, black dashed line) with the three sensors' observations of $x_{2,k}$ (red/blue/orange solid lines). Figure 5(b) synchronizes the distribution of FDI attacks in the $x_{2,k}$ channel. The comparison of the two sets of images clearly shows that the observed data acquired by the sensors during the normal operation hours without attacks maintains a remarkable consistency with the real state, while there is a significant deviation during the 40 to 80 FDI attack time period (red blocks), verifying the destructive impact of the attack on the data. Figure 4 and Figure 6 show the FDI attack detection results for sensors 1-3 and sensors 4-6, respectively, where the red crosses indicate that an alert is issued when an attack is detected and the corresponding data is discarded.

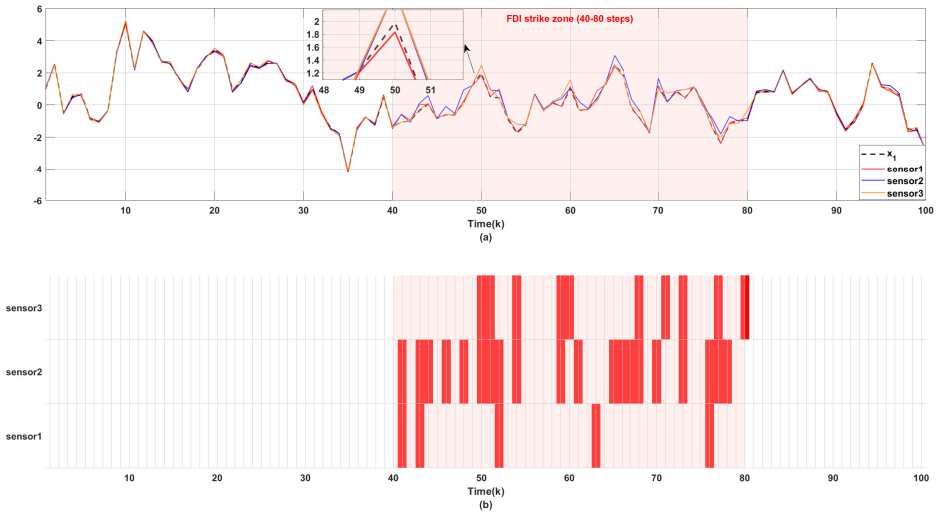

Figure 3. Comparison of USV location observation and FDI attack distribution.

 doi:10.20944/preprints202506.1666.v1

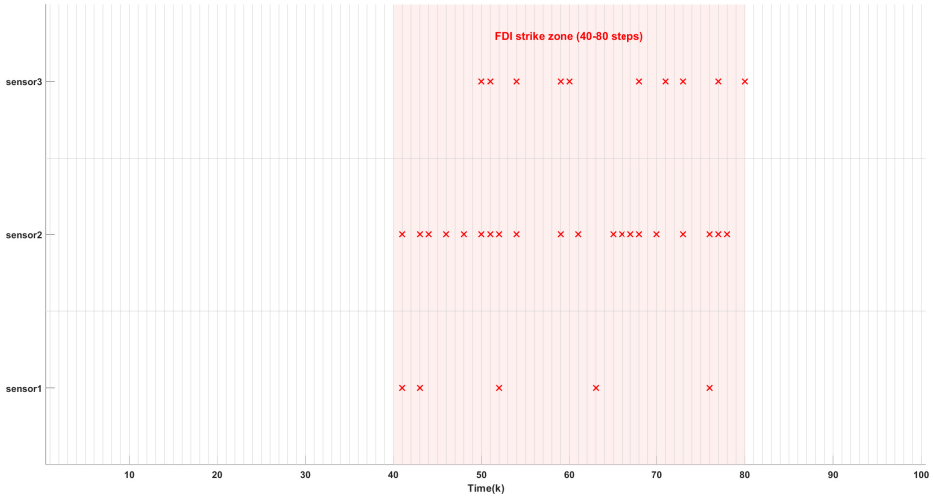

Figure 4. Sensor 1-3 FDI Detection Results.

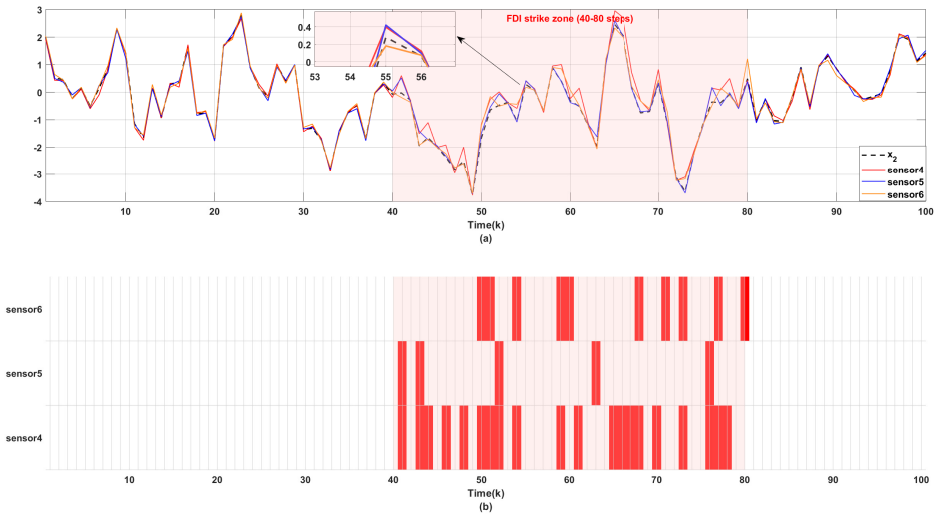

Figure 5. Comparison of USV velocity observation and FDI attack distribution.

 doi:10.20944/preprints202506.1666.v1

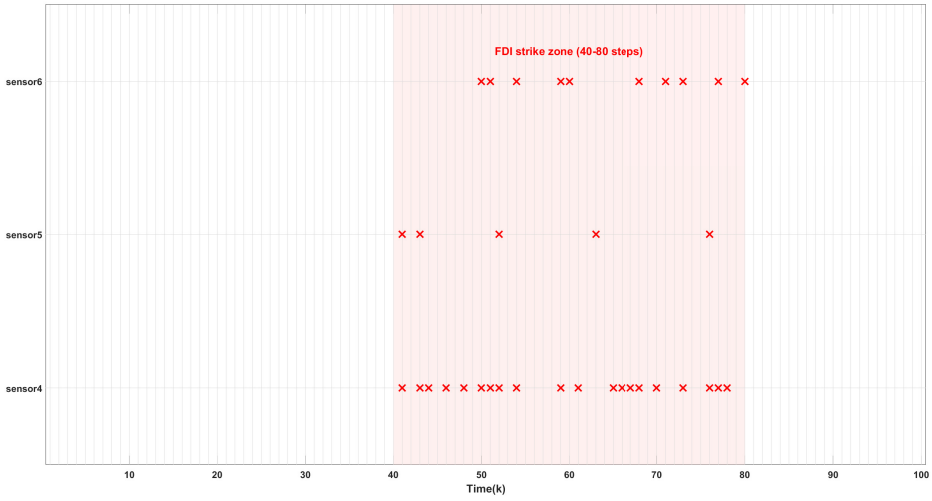

Figure 6. Sensor 4-6 FDI Detection Results.

The actual values and the estimated values of the USVs' horizontal position are shown in Figure 7, while Figure 8 presents the actual and the estimated values of the USVs' velocity. From Figure 7 and Figure 8, the proposed fusion estimation method can accurately obtain both the horizontal position and velocity of the USVs. Moreover, due to the dynamic nature of the encryption keys, the encryption scheme remains secure without risk of compromise. The estimation results demonstrate significant superiority over the CI fusion estimation results presented in the comparative literature [29].

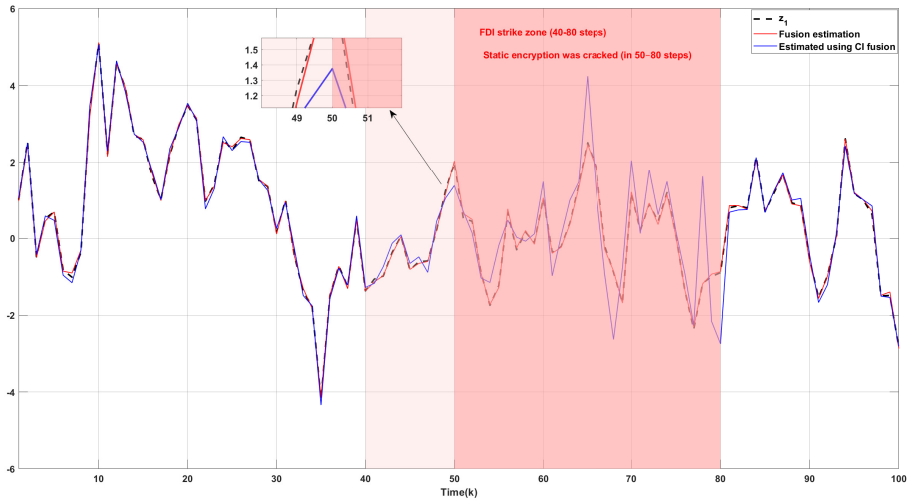

Figure 7. State estimation for horizontal position.

 doi:10.20944/preprints202506.1666.v1

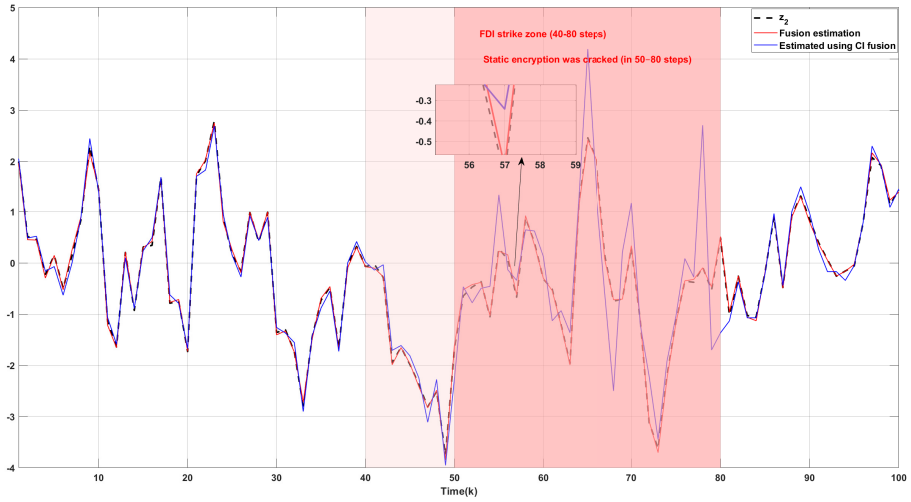

Figure 8. State estimation of velocity values.

Table 1 demonstrates the standard deviation(SD) and mean square errors(MSEs) results for speed. The comparison shows that the mean square error value obtained from this paper's method is smaller and has better robustness, indicating that the method is more resilient to FDI attacks.

Table 1. Standard deviation(SD) and mean square errors(MSEs) of the position with respect to the comparison literature [29].

	Standard deviation	**mean square errors**
Methods of comparison	0.1559	0.0243
This method	**0.0603**	**0.0036**

6. Conclusions

The innovative security solution for the problem of FDI attacks faced by is investigated USVs during data transmission in CPSs. Due to the open nature of WSNs, attackers can tamper with sensor data, leading to poor decision-making in the control center. To solve this problem, a dynamic data encryption method is developed. Encrypting the data before transmission, dynamically updating the key using historical data to enhance the difficulty of cracking. At the same time, constructing a dynamic correlation mechanism between the ciphertext, the key, and the auxiliary encrypted ciphertext. The goal is to create a detection system that can quickly identify and map FDI attacks. In addition, the external noise interference is filtered by the H_∞ fusion filter, and the weighted fusion algorithm is used to restore the actual information. The effectiveness of the scheme in improving the security of USVs' data and system reliability is verified by simulation experiments.

Author Contributions: Methodology, Z.L.; Formal analysit, Z.L. and L.L.; Investigationt, Z.L. and L.L.; Writing—original draft, Z.L.; Writing—Review and Editingt, Z.L. and L.L.;Supervision, H.Y. and Z.W.; Funding acquisition, G.D. and C.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 62273172, 62403227), Shanghai Key Laboratory of Power Station Automation Technology, and the Natural Science Foundation of Shandong Province (Grant Nos. ZR2023MF105, ZR2022MF231, ZR2022MF292).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed at the corresponding authors the system, when the system state information has been tampered with.

Conflicts of Interest: The authors declare no conflicts of interest.

 doi:10.20944/preprints202506.1666.v1

References

1. Kim, S.; Park, K.J.; Lu, C. A survey on network security for cyber–physical systems: From threats to resilient design. *IEEE Communications Surveys & Tutorials* **2022**, *24*, 1534–1573.
2. Cui, D.; Li, H. Dual self-triggered model-predictive control for nonlinear cyber-physical systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2021**, *52*, 3442–3452.
3. Lu, K.D.; Wu, Z.G.; Huang, T. Differential evolution-based three stage dynamic cyber-attack of cyber-physical power systems. *IEEE/ASME Transactions on Mechatronics* **2022**, *28*, 1137–1148.
4. Yu, Z.; Gao, H.; Cong, X.; Wu, N.; Song, H.H. A survey on cyber–physical systems security. *IEEE Internet of Things Journal* **2023**, *10*, 21670–21686.
5. Zhang, Y.; Fei, M.; Du, D.; Hu, Y. Security State Assessment in Cyber-Physical Systems Post-DoS Attack Based on Cyber Layer Partitioning. *IEEE Transactions on Industrial Informatics* **2024**.
6. Xu, Q.; Li, X.; Jiang, Y.; Zhu, S.; Yang, B.; Chen, C.; Duan, S.; Guan, X. Transportation-Energy-Communication Integrated Management of Ship Cyber-Physical Systems Against Cyber Attacks. *IEEE Transactions on Smart Grid* **2025**.
7. Younus, M.U.; Khan, M.K.; Bhatti, A.R. Improving the software-defined wireless sensor networks routing performance using reinforcement learning. *IEEE Internet of Things Journal* **2021**, *9*, 3495–3508.
8. Zheng, Y.; Hu, J.; Zhao, Y.; Yang, K. Average age of sensing in wireless powered sensor networks. *IEEE Transactions on Wireless Communications* **2024**, *23*, 9265–9281.
9. Fei, Z.; Wang, X.; Wang, Z. Event-based fault detection for unmanned surface vehicles subject to denial-of-service attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2021**, *52*, 3326–3336.
10. Su, N.; Wang, J.B.; Zeng, C.; Zhang, H.; Lin, M.; Li, G.Y. Unmanned-surface-vehicle-aided maritime data collection using deep reinforcement learning. *IEEE Internet of Things Journal* **2022**, *9*, 19773–19786.
11. Tang, C.; Zhang, H.T.; Wang, J. Flexible formation tracking control of multiple unmanned surface vessels for navigating through narrow channels with unknown curvatures. *IEEE Transactions on Industrial Electronics* **2022**, *70*, 2927–2938.
12. Ghoumid, K.; Ar-Reyouchi, D.; Rattal, S.; Yahiaoui, R.; Elmazria, O.; et al. Protocol wireless medical sensor networks in IoT for the efficiency of healthcare. *IEEE Internet of Things Journal* **2021**, *9*, 10693–10704.
13. Karimi-Bidhendi, S.; Guo, J.; Jafarkhani, H. Energy-efficient deployment in static and mobile heterogeneous multi-hop wireless sensor networks. *IEEE Transactions on Wireless Communications* **2021**, *21*, 4973–4988.
14. Wu, C.; Zhu, G.; Lu, J. Indirect adaptive neural tracking control of USVs under injection and deception attacks. *Ocean Engineering* **2023**, *270*, 113641.
15. Duan, H.; Yuan, Y.; Zeng, Z. Distributed robust learning control for multiple unmanned surface vessels with fixed-time prescribed performance. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2023**, *54*, 787–799.
16. Liu, C.; Jiang, B.; Wang, X.; Zhang, Y.; Xie, S. Event-based distributed secure control of unmanned surface vehicles with DoS attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2024**, *54*, 2159–2170.
17. Wang, L.; Wang, Z.; Han, Q.L.; Wei, G. Event-Based Variance-Constrained H_∞ Filtering for Stochastic Parameter Systems over Sensor Networks with Successive Missing Measurements. *IEEE transactions on cybernetics* **2017**, *48*, 1007–1017.
18. Zhang, L.; Sun, S. Distributed H_∞ fusion filtering for multi-sensor networked systems with DoS attacks and sensor saturations. *Digital Signal Processing* **2023**, *134*, 103908.
19. Hu, Z.; Chen, K.; Deng, F.; Luo, S.; Hu, S. H_∞ controller design for networked systems with two-channel packet dropouts and FDI attacks. *IEEE Transactions on Cybernetics* **2023**, *54*, 1661–1670.
20. Li, Y.G.; Yang, G.H. Optimal stealthy false data injection attacks in cyber-physical systems. *Information Sciences* **2019**, *481*, 474–490.
21. Liu, C.; He, W.; Deng, R.; Tian, Y.C.; Du, W. False-data-injection-enabled network parameter modifications in power systems: Attack and detection. *IEEE Transactions on Industrial Informatics* **2022**, *19*, 177–188.
22. Xiao, L.; Chen, H.; Xu, S.; Lv, Z.; Wang, C.; Xiao, Y. Reinforcement Learning-Based False Data Injection Attacks in Smart Grids. *IEEE Transactions on Industrial Informatics* **2025**.
23. Jafari, M.; Rahman, M.A.; Paudyal, S. Optimal false data injection attack against load-frequency control in power systems. *IEEE Transactions on Information Forensics and Security* **2023**, *18*, 5200–5212.
24. Guo, H.; Sun, J.; Pang, Z.H. Residual-based false data injection attacks against multi-sensor estimation systems. *IEEE/CAA Journal of Automatica Sinica* **2023**, *10*, 1181–1191.
25. Du, M.; Wang, L.; Zhou, Y. High-stealth false data attacks on overloading multiple lines in power systems. *IEEE Transactions on Smart Grid* **2022**, *14*, 1321–1324.

 doi:10.20944/preprints202506.1666.v1

26. Chen, X.; Hu, S.; Li, Y.; Yue, D.; Dou, C.; Ding, L. Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks. *IEEE Transactions on Smart Grid* **2022**, *13*, 2357–2368.
27. Xia, W.; Zhang, Y. Resilient distributed estimation against FDI attacks: a correntropy-based approach. *Information Sciences* **2023**, *635*, 236–256.
28. Zhang, Q.; He, D. Adaptive neural control of nonlinear cyber–physical systems against randomly occurring false data injection attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2022**, *53*, 2444–2455.
29. Li, T.; Weng, P.; Chen, B.; Zhang, D.; Yu, L. Encryption-based attack detection scheme for multi-sensor secure fusion estimation. *IEEE Transactions on Aerospace and Electronic Systems* **2024**.
30. Ma, Y.; Nie, Z.; Hu, S.; Li, Z.; Malekian, R.; Sotelo, M. Fault detection filter and controller co-design for unmanned surface vehicles under DoS attacks. *IEEE Transactions on Intelligent Transportation Systems* **2020**, *22*, 1422–1434.
31. Blum, M.; Micali, S. How to generate cryptographically strong sequences of pseudo random bits. In *Providing sound foundations for cryptography: on the Work of Shafi Goldwasser and Silvio Micali*; 2019; pp. 227–240.