HiLL PUBLISHING

Advances in Computer and Communication, 2024, 5(1), 83-96
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Secure Encryption System for USV Trajectory Tracking Based on MPC

Di Liu

School of Mechanical Engineering, University of Shanghai for Science and Technology, Shanghai, China.

How to cite this paper: Di Liu. (2024) Secure Encryption System for USV Trajectory Tracking Based on MPC. *Advances in Computer and Communication*, 5(1), 83-96.
DOI: 10.26855/acc.2024.02.014

Received: February 16, 2024
Accepted: March 13, 2024
Published: April 10, 2024

***Corresponding author:** Di Liu, School of Mechanical Engineering, University of Shanghai for Science and Technology, Shanghai, China.

Abstract

Unmanned surface vehicles (USVs) are more and more widely used in marine resources exploration and marine military activities. This paper studies the security encryption of information transmission between the USV and the mothership under the malicious attack of hackers. The USV transmits useful information such as posture status and position to the mother ship. A trajectory tracking controller implemented in the mother ship will generate the optimal control signal to the USV so that the USV will follow the preset path. To ensure the security of information transmission between the mother ship and the USV, the Paillier encryption algorithm is introduced into the MPC-based trajectory tracking controller to prevent malicious attackers from eroding the security of information transmission. To make the encryption algorithm compatible with the trajectory tracking controller, two compatibility designs are added: realize the conversion from floating point numbers to integer sequences and achieve subtraction operations. Through the simulation of trajectory tracking, the effectiveness of the proposed safety control framework is proved.

Keywords

Unmanned surface vehicles (USVs), model predictive control, security encryption algorithm, marine information security

1. Introduction

About two-thirds of the earth is covered by oceans [1], which led to a strong demand from the commercial, scientific, and military communities to develop innovative unmanned surface vehicles (USVs). The current USV market has formed a multi-billion-dollar industry and will grow significantly in the coming years [2]. Due to its high mobility, versatility, flexibility, and affordable maintenance, the USV has been widely applied in scientific and military fields, such as anti-submarine operations [3], naval military reconnaissance [4], shipping [5], exploration of Marine Resources [6], and monitoring of the Marine Environment [7]. The USV has attracted many researchers to develop advanced control algorithms such as trajectory tracking, artificial intelligence, and navigation control. Trajectory tracking is essential for the autonomous control of USVs. The current control algorithms to solve the path-following problem mainly include the backstepping method [8, 9], sliding mode control [10, 11], model predictive control (MPC) [12, 13], fault-tolerant tracking control [14, 15], adaptive control [16, 17], and intelligent method [18]. Among these methods mentioned above, MPC has been one of the most promising methods for its great ability to deal with optimization and system constraints through the rolling optimization process.

Information transmission also plays an important role in the unmanned control of USVs. Network control systems (NCS) are the major choice for USV communication [19]. However, NCS is inherently insecure and vulnerable to network attacks [20]. For example, USVs can be illegally controlled by intercepting and modifying control signals, which will result in goods and USVs lost [21]. Many researchers have focused on the network security of USVs.

According to different objectives, the existing security control algorithms are mainly divided into two categories, one is to prevent information alteration [22-24], and the other is to prevent information interception [25-27]. The first type mainly solves the attack of modification, permissions modification, which will result in the loss of authenticity. S. Amin et al. introduced a control method to deal with information tampering [28]. A. Teixeira et al. summarized and classified the countermeasure mechanism according to the different tampering effects of handling attacks [29]. J. Wang et al adopted an MPC-based security control framework to deal with tampering attacks [30]. The second type is mainly used to prevent hackers from invading the information transmission system, stealing important information, and using this information to threaten property security. Z.-H. Pang et al. used symmetric encryption to protect information from disclosure [31]. To further improve security, F. Farokhi et al. introduced an asymmetric cryptographic control framework to achieve almost absolute information security with its strong homomorphism [32]. A. B. Q. Sun et al. applied some asymmetric encryption methods to MPC to achieve better control performance [33]. Due to the significance of the transmitted information between the USV and the mother ship, it is a challenge to design an effective encryption algorithm that can keep information transmission safe from malicious attacks. To the best of our knowledge, there are rarely research results on dealing with security for the USV.

To ensure the security of information transmission between the USV and the mother ship, in this paper, the Paillier encryption scheme [34] and two compatibility designs are introduced in the trajectory tracking control frame. In the wireless communication network environment, the USV trajectory tracking security control system is composed of a USV, mother ship controller, and communication link. The traditional encryption technology generally adopts the symmetric key encryption mode, which needs to decrypt the data before calculating and operating. In contrast, the Paillier encryption scheme is a homomorphic encryption technique, which can be calculated in the case of encryption to avoid the risk of data leakage during the error reporting process. Paillier encryption is one of the most commonly used instantiation homomorphic encryption algorithms in privacy computing scenarios because of its high efficiency and complete security proof. Compared with the existing methods, the designed security encryption framework can realize the complicated encryption/decryption process in the process of information transmission, and ensure the information security in the process of data transmission between the USV and the mother ship.

The main contributions of this paper are as follows:

(1) This paper designs a USV trajectory tracking control framework based on MPC. The control signal is generated by the encryption controller on the mother ship and sent to the USV through the network. After receiving and decrypting the control signal, the USV applies the control signal to the trajectory tracking, and the USV sends the position information, attitude information, and acquired data to the mother ship.

(2) Based on the trajectory tracking framework, an encryption method based on the Paillier homologous encryption scheme is proposed to protect the security of information transmission between the USV and the mother ship. The designed encryption method not only ensures the real-time performance required for trajectory tracking but also protects the communication between the mother ship and USV.

The rest of this paper is as follows: the second part is the hydrodynamic modeling, and the fluid dynamics model is determined; In the third part, the main trajectory tracking control framework of MPC is presented. The fourth part introduces the security control framework and the optimal compatible design method in detail. In Section 5, the effectiveness of the proposed method is verified by simulation experiments. The sixth part summarizes the conclusion of this paper.

2. Hydrodynamic Modeling of the USV

The USV has six degrees of freedom in the motion space, namely sway, surge, heave, roll, pitch, and yaw. To quantitatively describe the spatial state of USV, define the body coordinate system $B=\{x_b, y_b, z_b\}$, and define the inertial coordinate system $G=\{x_g, y_g, z_g\}$. The USV six-degree-of-freedom motion model is shown in Fig. 1. To reduce the complexity of the system, only surge, yaw, and sway in the horizontal motion of the USV are considered, as shown in Fig. 2.

Define the velocity vector in the body coordinate system $b=[u,v,w]^T$, where u denotes the forward velocity, v indicates the transverse velocity, and w represents the yawing angular velocity. Define the position vector in the inertial coordinate system $g=[i,j,\theta]^T$, where i denotes the X-axis position, j indicates the Y-axis position, and θ represents the yaw angle. The conversion formula from the body coordinate system to the inertial coordinate

system is as follows:

$$\dot{g} = T(\theta)b \tag{2-1}$$

Where $T(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix}$ represents the transformation matrix.

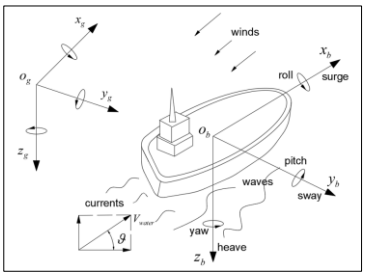

Figure 1. Six degrees of freedom model of USV.

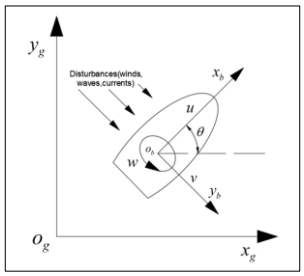

Figure 2. Three-degrees-of-freedom model of USVs horizontal plane.

In this paper, the Fossen hydrodynamic model [35] is adopted, assuming that the hull material is uniform and symmetrical. The forces on the hull are divided into propulsive force, rigid force, fluid force, and interference force. The hydrodynamic model of the USV can be established as:

$$M_{rb}\dot{b} + M_a\dot{b} + C_{rb}(b)b + C_a(b)b + D(b)b = \tau' + \tau_e \tag{2-2}$$

Where M_{rb} represents rigid body inertia matrix, M_a denotes additional mass matrix, C_{rb} indicates Centrifugal force matrix, $C_a(b)$ represents centrifugal force matrix due to rotation of body coordinate system, $D(b)$ denotes damping matrix. Define the total thrust on the USV $\tau' = [f_u, f_v, t_w]$, where f_u indicates forward force, f_v denotes transverse displacement force, and t_w represents the yawing moment. The total environmental disturbance τ_e can be described as:

$$\tau_e = \left[f_{ue}, f_{ve}, t_{we}\right]^T = \left[a_1 rand\ wind \quad a_2 rand\ wave \quad a_3 rand\ current\right]^T \tag{2-3}$$

Where f_{ue} denotes the forward force caused by environmental disturbances, f_{ve} indicates the transverse force caused by environmental disturbances (wind, waves, currents), and t_{we} represents the yawing torque caused by environmental disturbance. a_1, a_2 and a_3 represent the weight of wind, wave, and current, respectively. $randwind$, $randwave$, and $randcurrent$ are random numbers within $[-1, 1]$.

Ocean current velocity can be accurately measured with the help of a velocimeter. The water velocity is defined as V_{water} in the inertial coordinate system, the direction angle is ϑ. In the body coordinate system, the USV relative velocity $b_r = b - b_{water}$, where $b_{water} = T(\theta)^T \begin{bmatrix} V_{water}\cos\vartheta \\ V_{water}\sin\vartheta \\ 0 \end{bmatrix}$ denotes the velocity of water flow in the body coordinate system.

Considering the under-actuation of the system, the system input changes from three degrees of freedom input to two degrees of freedom input $\tau = [f_u, t_w]^T$. The hydrodynamic model (2-2) is optimized to:

$$M_{rb}\dot{b} + M_a\dot{b}_r + C_{rb}(b)b + C_a(b_r)b_r + D(b_r)b_r = \tau + \tau_e \tag{2-4}$$

3. Controller Design

The trajectory tracking controller is carried out on the mother ship's control system, and the encryption and decryption are carried out on the USV controller. The mother ship receives the encrypted status information from the USV, gets

the optimal control sequence after a series of optimization, and sends it to the USV through the network; USV applies the decrypted control signal to its own system. At the same time, the USV encrypts the information obtained by the sensor (water velocity V_{water}, the direction angle ϑ, yaw angle θ, X-axis position i, and Y-axis position j) and sends them to the mother ship through the network. Keep repeating until the entire process is completed. The MPC controller of mothership includes reference trajectory generation, roll optimization, model prediction, and control law introduction. The MPC framework under the security control framework built is shown in Fig. 3, where $U(k)$ denotes the optimal control output, $U_m(k)$ indicates the system prediction output, and $\varepsilon(k)$ represents the deviation of $U(k)$ and $U_m(k)$.

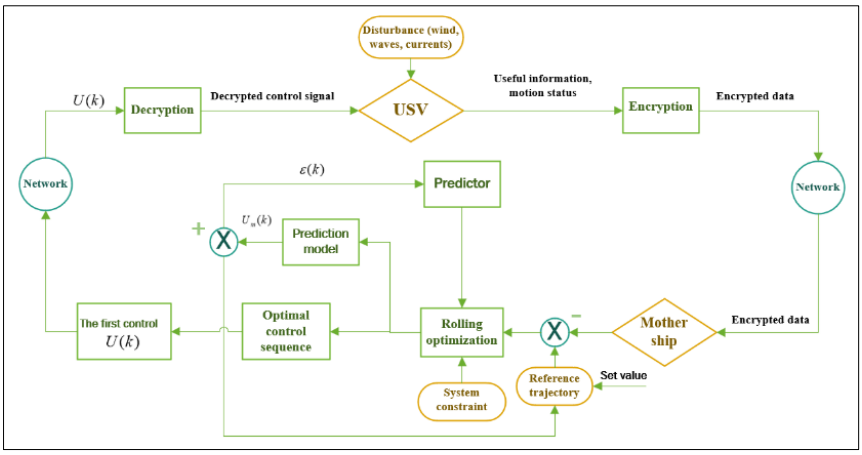

Figure 3. MPC framework under the security control framework.

The controller flow chart proposed in this paper is shown in Fig. 4. below:

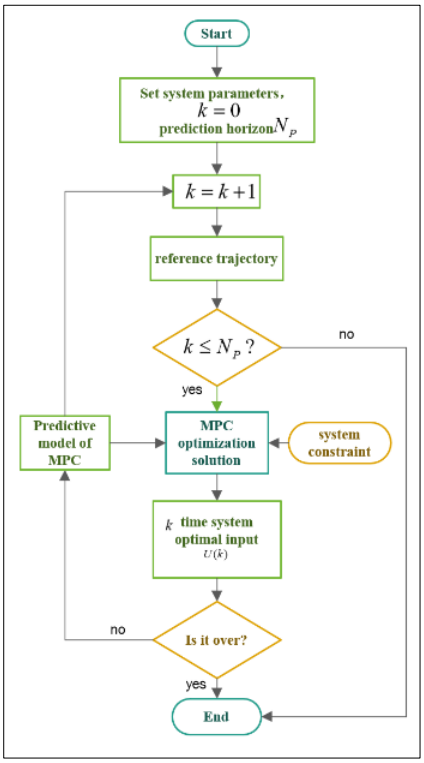

Figure 4. The flow chart of MPC.

3.1 Trajectory Tracking Framework Based on MPC

Define the system state variable $\zeta=[i, j, \theta, u, v, w]^T$, control input $\tau=[f_u, t_w]^T$, system output $h=[i, j]^T$, The USVs hydrodynamic model can be described as:

$$\begin{aligned}\dot{\zeta} &= f(\zeta,\tau)=\begin{bmatrix} T(\theta)b \\ (M_{rb}+M_a)^{-1}(I_a\tau+\tau_e+M_a\dot{b}_{water}-C_{rb}(b)b-C_a(b_r)b_r-D(b_r)b_r)\end{bmatrix} \\ h &= I_b\zeta\end{aligned} \tag{3-1}$$

Where $I_a=\begin{bmatrix}1&0&0\\0&0&1\end{bmatrix}^T$, $I_b=\begin{bmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\end{bmatrix}$, The parameter definition of $T(\theta)$ is the same as (2-1).

The system equation under the reference trajectory is as follows:

$$\dot{\zeta}_{refer}=f(\zeta_{refer},\tau_{refer}) \tag{3-2}$$

The first-order Taylor formula is used to expand point $(\zeta_{refer},\tau_{refer})$:

$$\dot{\zeta}=f(\zeta_{refer},\tau_{refer})+\frac{\partial f}{\partial\zeta}(\zeta-\zeta_{refer})+\frac{\partial f}{\partial\tau}(\tau-\tau_{refer}) \tag{3-3}$$

A new system state space model can be obtained by subtracting the two formulas （3-2）and (3-3):

$$\dot{\tilde{\zeta}}=M\tilde{\zeta}+N\tilde{\tau} \tag{3-4}$$

Where $\tilde{\zeta}=\zeta-\zeta_{refer}$, $\tilde{\tau}=\tau-\tau_{refer}$, time-varying matrix $M=\frac{\partial f}{\partial\zeta}$, time-varying matrix $N=\frac{\partial f}{\partial\tau}$.

The Euler method is used to discretize (3-4):

$$\begin{cases}\tilde{\zeta}(k+1)=M_k\tilde{\zeta}(k)+N_k\tilde{\tau}(k)\\ \tilde{h}(k)=I_b\tilde{\zeta}(k)\end{cases} \tag{3-5}$$

Where $M_k=T\cdot M+I$ and $N_k=T\cdot N$ represent the discretized system matrix. Where T denotes the discrete time step, and I indicates the identity matrix.

To deal with constraints, define a new system state variable $\xi(k)=\begin{bmatrix}\tilde{\zeta}(k)\\ \tilde{\tau}(k-1)\end{bmatrix}$,

Combine (3-5), we can have:

$$\begin{cases}\xi(k+1)=\tilde{M}_k\xi(k)+\tilde{N}_k\Delta\tau(k)\\ \tilde{h}(k)=\tilde{\mathrm{P}}_k\xi(k)\end{cases} \tag{3-6}$$

Where $\tilde{M}_k=\begin{bmatrix}M_k&N_k\\0_{c*d}&I_c\end{bmatrix}$, $\tilde{N}_k=\begin{bmatrix}N_k\\I_c\end{bmatrix}$, $\tilde{P}_k=[I_b\ 0_{2*c}]$, c denotes the control dimension, d indicates the state dimension. To simplify system design, set $M_{k+t}=M_k$, $N_{k+t}=N_k$. The predictive output expression is established as follow:

$$\tilde{H}(k)=\Phi_k\xi(k)+\Psi_k\Delta U(k) \tag{3-7}$$

Where $\tilde{H}(k)=\left[\tilde{h}(k+1),\tilde{h}(k+2),\tilde{h}(k+3)\cdots\tilde{h}(k+N_C)\cdots\tilde{h}(k+N_P)\right]^T$ denotes output prediction,

$U(k)=\left[\Delta\tau(k),\Delta\tau(k+1),\Delta\tau(k+2)\cdots\Delta\tau(k+N_C)\right]^T$ indicates input prediction,

$\Phi_k = \left[\tilde{P}_k \tilde{M}_k, \tilde{P}_k \tilde{M}_k{}^2, \tilde{P}_k \tilde{M}_k{}^3 \cdots \tilde{P}_k \tilde{M}_k{}^{N_C} \cdots \tilde{P}_k \tilde{M}_k{}^{N_P} \right]^T$ represents system matrix,

$$\Psi_k = \begin{bmatrix} \tilde{P}_k \tilde{N}_k & 0 & \cdots & 0 \\ \vdots & \tilde{P}_k \tilde{N}_k & \vdots & \vdots \\ \tilde{P}_k \tilde{M}_k{}^{N_C} \tilde{N}_k & \vdots & 0 & \tilde{P}_k \tilde{M}_k \tilde{N}_k \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{P}_k \tilde{M}_k{}^{N_{P-1}} \tilde{N}_k & \cdots & \tilde{P}_k \tilde{M}_k{}^{N_P - N_C + 1} \tilde{N}_k & \tilde{P}_k \tilde{M}_k{}^{N_P - N_C} \tilde{N}_k \end{bmatrix}$$ denotes system matrix.

To ensure the USV to track the desired trajectory quickly and smoothly, we construct the objective function with the state quantity deviation, control quantity and control quantity increment. Objective functional can be defined as:

$$\begin{aligned} &\arg\min_{\Delta\tau(k)} \left\{ J(k) = \sum_{\ell=0}^{N_P-1} \left\| \tilde{h}(k+\ell) \right\|_Q^2 + \sum_{\ell=0}^{N_C} \left\| \Delta\tau(k+\ell) \right\|_R^2 \right\} \\ &s.t. \\ &\Delta\tau_{\min} \le \Delta\tau(k+t) \le \Delta\tau_{\max} \qquad t \in [0, N_C - 1] \\ &\tau_{\min} \le \tau(k+t) \le \tau_{\max} \qquad t \in [0, N_C - 1] \\ &h_{\min} \le h(k+t) \le h_{\max} \qquad t \in [1, N_P] \end{aligned} \tag{3-8}$$

Where N_P denotes the prediction horizon, N_C indicates the control horizon, Q and R are positive-definite matrices. $\arg\min\{\ \}$ is a function that returns the smallest element, $\Delta\tau_{\min}$ represents the constraint under input increment, $\Delta\tau_{\max}$ indicates the constraint on input increment, $\tau_{\min}$ denotes the constraint under the control input, $\tau_{\max}$ represents the constraint on the control input, $h_{\min}$ denotes the constraint under the output, $h_{\max}$ indicates the constraint on the output.

4. The Architecture of Security Control

During the operation of the USV, the data transmission between it and the mother ship may be attacked, these attacks may include attacks on the network transmission between the mother ship and the USV, or hackers using malicious viruses, software, etc. to hijack the USV. To ensure the safety of data transmission in harsh environments, it is necessary to design a secure encryption scheme to meet the following requirements: 1. The data transmission process of the trajectory tracking control scheme can be encrypted. 2. Encryption/decryption process is safe enough. 3. The implementation of the encryption scheme is efficient enough to make the encryption scheme be implemented in real-time in the USV trajectory tracking environment.

4.1 Paillier Encryption Scheme

To completely solve the above three problems, we design the Paillier homomorphic encryption scheme to protect the optimal control sequence obtained in the previous section. Paillier cryptosystem is a semi-homomorphic encryption algorithm (PHE) first proposed by Paillier at EUROCRYPT in 1999. Among many PHE schemes, Paillier scheme is widely used in major conferences and practical applications due to its high efficiency and complete security proof. It is one of the most commonly used PHE instantiation schemes in private computing scenarios. This advantage is brought by the inherent hardness of computing the residue classes under the large prime numbers. Using this encryption scheme can very reliably protect the data transmission between the USV and the mother ship. The principle of the Paillier encryption algorithm is simply divided into three steps: (1) Generate public key (K_n) and private key (K_e, K_f); (2) The public key will be used to encrypt the original information into ciphertext (c); (3) Restore the ciphertext to the cleartext (m) with the private key. The detailed process of the Paillier encryption scheme is shown in Table 1.

Table 1. Paillier optimization encryption principle

	Key generation
1.	Set the length of the message to be encrypted to M_{key}. Two large prime numbers α and β of length M_{key} are randomly selected. And $\alpha=\beta=3\bmod 4$, $\gcd(\alpha-1,\beta-1)=2$. Select a random number $a \leftarrow Z_{K_n}^*$, define $g=-a^2$, $K_n=\alpha\beta$
2.	$g_a = g^{K_n} \bmod K_n^2$ (4-1) $\chi=\frac{(\alpha-1)(\beta-1)}{2}$ (4-2)
3.	Output public key K_n and g_a, private key χ
	Encryption
1.	Enter plaintext message m, and request $m\in[0,K_n)$, Select a random number $b \leftarrow Z_{2^{\frac{\lvert K_n\rvert}{2}}}$
2.	Computational ciphertext $c(m,r)=(K_n+1)^m \cdot g_a{}^b \bmod K_n^2$ (4-3)
3.	Output ciphertext c
	Decryption
1.	Enter ciphertext c
2.	Cleartext $m=F(c^{K_e} \bmod K_n^2)\cdot\chi \bmod K_n$ (4-4)
3.	Output cleartext m

Where mod stands for modular exponential operation.

4.2 Compatibility Design

By using the Paillier encryption scheme designed in the previous section, the transmission of information between the mother ship and the USV is well protected, no matter how powerful malicious attackers and network hackers are. But we found in our experiments that there are two other challenges to combining trajectory tracking controllers with encryption algorithms. First, because the encryption algorithm runs in integer form and the track-tracking signal is transmitted in floating-point numbers, the analog signal must be converted to digital form. However, the traditional IEEE floating point standard cannot satisfy the matrix operation format necessary for cryptographic systems. Second, the Paillier encryption scheme has only addition and scalar multiplication operations. But the MPC controller requires subtraction.

We designed two compatibility designs. By introducing an encoding for data type conversion, the analog signal is converted to digital form, while maintaining the matrix operations required by the encryption system. A chain addition algorithm is designed to support MPC in subtraction operation.

4.2.1 Data Type Conversion

Since the Paillier encryption scheme is calculated in integer form, it must pass through a linear matrix to maintain security. The transmission process of the unmanned boat track tracking signal is floating-point type. The floating-point number must be converted into an integer sequence, an algorithm is inserted here to complete the conversion, the algorithm is shown as follows:

$$x = f(\kappa) = \sum_{\ell=0}^{M_{code}-1} i_\ell 10^{\ell - M_{offest}} + \varepsilon_x \tag{4-5}$$

Where κ indicates the sequence of encoded integers, $\kappa=[\kappa_0,\kappa_1,\kappa_2\cdots\kappa_{E_{code}}]$, $\kappa_\ell\in[0,9]$, ε_x indicates the sequence of encoded integers, M_{code} is the maximum digit length of the encoded integer, and $M_{code}\le M_{key}$, M_{offest} is the offset length of the precision.

$$Dec = sign(\kappa)\sum_{\ell=0}^{M_{code}-1}\kappa_\ell 10^\ell \tag{4-6}$$

Where Dec denotes the converted coded decimal number, $sign(x)$ represents the function used to determine the symbol of the data. This method can not only complete the data conversion, and simplify the coding task, but also ensure the necessary matrix operation of the cryptographic system.

4.2.2 Implement Subtraction Operations

To make the Paillier encryption scheme implement subtraction operation, we design an algorithm based on chain addition mechanism. The signed decimal number is first converted to a representation of an unsigned decimal number, and then the final result is computed using only the addition operation. The algorithm that supports the subtraction by a chain addition mechanism is as follows (Table 2).

Table 2. The algorithm that supports the subtraction by a chain-plus mechanism

1.	Input the coded decimal number Dec, and maximum digit length of the encoded integer M_{code}. Define the complement number p. If $Dec > 0$,then $p = Dec$; else $p = 10^{M_{code}} + Dec$ where, $10^{M_{code}}$ indicates the offset value. Output: a series of complement numbers $p_1, p_2, \cdots p_M$.
2.	Input the series of complement numbers $p_1, p_2, \cdots p_M$, the maximum digit length of the encoded integer M_{code}. Set $\Sigma = 0$; For ($i = 1; i \le M; i++$) do { $\Sigma = \Sigma + p_i$ } Output the sum of complements Σ.
3.	Input the sum of complements Σ, the maximum digit length of the encoded integer M_{code}. Set $\Sigma_A = \Sigma$; While $\Sigma_A \ge 9 \cdot 10^{M_{code}-1}$, do $\Sigma_A = \Sigma_A - 10^{M_{code}}$; Output the original sum Σ_A.

5. Simulation

To evaluate the operation of unmanned vehicle trajectory tracking under encrypted conditions, we designed a simulation experiment and put the simulation results and conclusions in this chapter. In this paper, Cyber Ship II is used as a USV simulation model.

5.1 Parameter Setting

Model parameter setting: The model is a fully driven ship equipped with longitudinal thrusters, transverse thrusters, and steering gear. The object considered in this paper is an underdriven USV, and the transverse thrusters should be ignored in the model. Maximum longitudinal thrust is $f_u = 2N$, the maximum longitudinal thrust corresponding to the real ship is $686kN$; the maximum yaw torque is $t_w = 1.5N \cdot m$, the maximum yaw torque corresponds to the real ship is $36015kN \cdot m$; maximum speed is $0.2m/s$, corresponding to the real ship is $1.7m/s$. model quality $m = 23.8kg$, gravity constant $g = 9.81kg/s^2$, water density $\rho = 1.01g/cm^3$, The uncertainty of parameter perturbation effect in the simulation is estimated as 5%.

For the state-space equation described in (3-1), according to the kinetic parameters of Cyber Ship II, we can obtain:

$$M_{\text{rb}} = \begin{bmatrix} 23.8 & 0 & 0 \\ 0 & 23.8 & 1 \\ 0 & 1 & 1.8 \end{bmatrix}, \quad M_a = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$C_{rb}(b)=\begin{bmatrix}0 & 0 & -1.1r-23.8b\\ 0 & 0 & 23.8\tau\\ 1.1r+23.8b & -23.8\tau & 0\end{bmatrix},\ C_a(b_r)=\begin{bmatrix}0 & 0 & -10b_r\\ 0 & 0 & 2\tau_r\\ 10b_r & -2\tau_r & 0\end{bmatrix},$$

$$D(b_r)=\begin{bmatrix}0.7+1.3|\tau_r|+5.9\tau_r^{\,2} & 0 & 0\\ 0 & 0.9+36.3|b_r|+0.8|r_r| & -0.1+0.8|b_r|+3.5|r_r|\\ 0 & -0.1-5|b_r|-0.1|r_r| & 1.9-0.1|b_r|+0.8|r_r|\end{bmatrix}$$

5.2 Simulation Parameters Setting

Circular reference track of USV: $\begin{cases}\zeta(t)=2\sin(0.01t)\\ \tau(t)=2(1-\cos(0.01t))\end{cases}$

The reference trajectories are discretized to form a series of reference points $(\zeta_{refer},\tau_{refer})$:

$$\begin{cases}\zeta_{refer}=2\sin(0.01nT)\\ \tau_{refer}=2(1-\cos(0.01nT))\end{cases}\ n\in\left[0,N_{refer}\right]$$

Where N_{refer} represents the number of reference points, T indicates the one-step simulation duration, set $T=1s$. The linearization of (3-2) takes $(\zeta_{refer},\tau_{refer})$ as a reference, set $\zeta_{refer}=\left[i_{refer},j_{refer},\theta_{refer},u_{refer},v_{refer},w_{refer}\right]^T$, $\tau_{refer}=\left[0.075,0.015\right]^T$, where $\theta_{refer}=0.01nT$, $\left[u_{refer},v_{refer},w_{refer}\right]^T=T\left(\theta_{refer}\right)^T\left[\dot{\zeta}_{refer}(nT),\dot{\tau}_{refer}(nT),0.01\right]^T$. In (3-8), Q and R are set as: $Q=\begin{bmatrix}80 & 0\\ 0 & 80\end{bmatrix}$, $R=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}$, prediction horizon $N_P=12$, control horizon $N_C=10$.

Environmental interference parameter setting: The interference of model (3-1) can be divided into two types, one is the ship force caused by environmental interference (τ_e), and the other is the speed change caused by the presence of water flow (V_{water}). Reference formula (2-3), $\tau_e=\left[f_{ue},f_{ve},f_{we}\right]^T=H\begin{bmatrix}rand\\ rand\\ rand\end{bmatrix}$ $H\geq 0$, where H is the weight parameter, $rand$ is a uniform random number in the range $[-1,1]$. The speed and direction of the water flow in the inertial coordinate system $\{g\}$ during navigation usually remain constant and can be measured by the voyage data recorder (VDR), so V_{water} is assumed to be known.

Constraint Parameter setting: Input constraint: $A\begin{bmatrix}-1\\ -0.2\end{bmatrix}\leq\tau\leq A\begin{bmatrix}1\\ 0.2\end{bmatrix}$, input increment constraint: $B\begin{bmatrix}-1\\ -0.2\end{bmatrix}\leq\Delta\tau\leq B\begin{bmatrix}1\\ 0.2\end{bmatrix}$, Output constraints: $C\begin{bmatrix}-5\\ -6\end{bmatrix}\leq h\leq C\begin{bmatrix}5\\ 6\end{bmatrix}$. Where A,B,C are weights greater than zero.

Security encryption scheme parameter settings: According to Table 4, the key length $M_{key}=256bits$. The two large prime numbers α and β of length M_{key} are presented as follows:

$\alpha=$ 87400697748627000500418982062125720145083595286290689356511561050034589378249, $\beta=$ 92833132186568426198749835897197910518523286423616088832223047227419760673703. The public and private keys are then generated using the algorithm in Table 4. In compatibility design, the maximum digit length of the encoded integer $M_{code}=20$, and the offset value of the precision $M_{offest}=6$.

5.3 Experimental Results and Analysis

In the absence of environmental interference: the flow velocity $V_{water}=0m/s$, environmental interference force

weight $H=0$, constraint parameter set to $A=1$, $B=1$, $C=1$. Only track tracking results are shown in Fig. 6. The track tracking results of adding the security encryption module are shown in Fig. 6.

The real track points in the simulation process are (x_{rea}, y_{rea}), trajectory tracking deviation is defined as $E=\sqrt{\left(x_{rea}-x_{refer}\right)^2+\left(y_{rea}-y_{refer}\right)^2}$. Fig. 7 shows the trajectory tracking error without adding the secure encryption module, and Fig. 8 shows the trajectory tracking error with adding the secure encryption module.

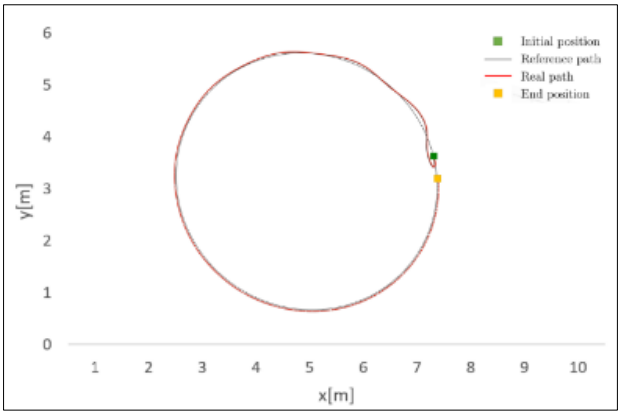

Figure 5. Results of circular path tracking (No environmental disturbance).

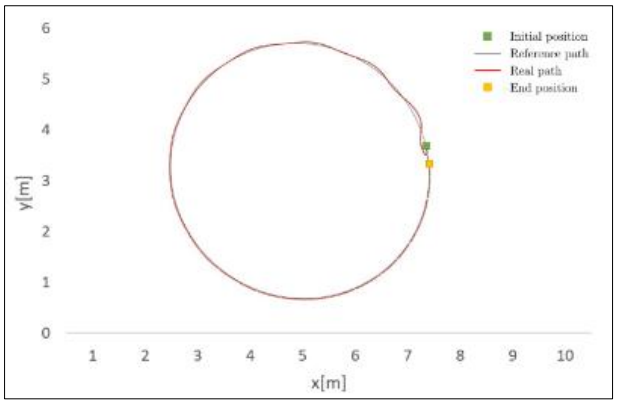

Figure 6. Results of circular path tracking under the security control framework (No environmental disturbance).

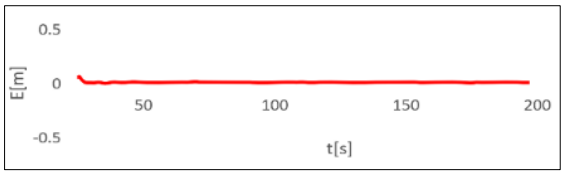

Figure 7. USV tracking error under the circular path.

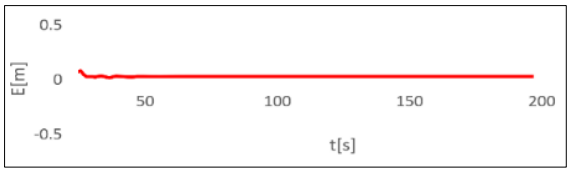

Figure 8. Tracking error of circular path under security control framework.

As can be seen from the figures, despite the uncertainty and quantification effects, the position of the USV can always follow the expected path of tolerable error, whether it is encrypted or not. It has an excellent tracking effect.

Compared with Fig. 7 and Fig. 8, the degree of deviation between them is similar, which indicates that the introduction of the secure encryption module has little interference with the trajectory tracking in the absence of environmental interference.

In the presence of environmental interference, we set $V_{water} = 0.1m/s$, $H = 0.05$. The simulation results of track tracking only are shown in Fig. 9, and the simulation results of track tracking under the secure encryption framework are shown in Fig. 10.

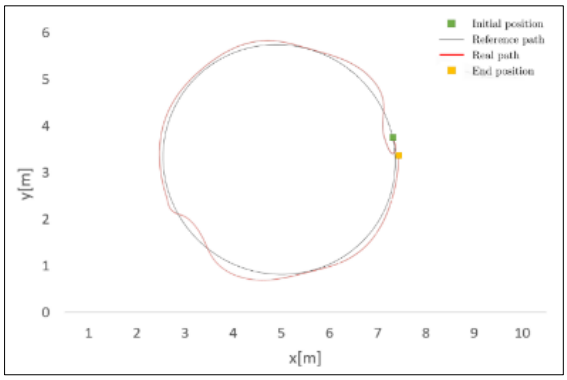

Figure 9. Results of circular path tracking ($V_{water} = 0.1m/s$, $H = 0.05$).

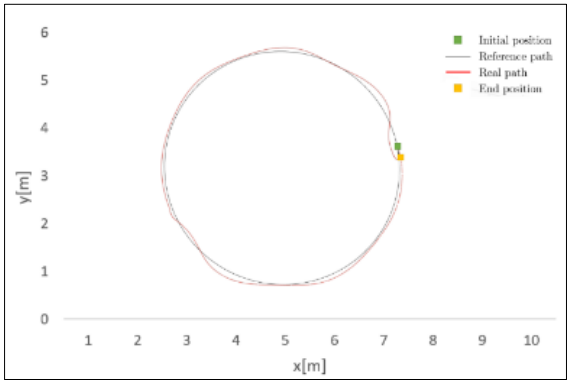

Figure 10. Results of circular path tracking under the security control framework ($V_{water} = 0.1m/s$, $H = 0.05$).

As can be seen from the comparison results of Fig. 9 and Fig. 10, although the deviation between the real trajectory and the expected trajectory increases under environmental interference, the deviation degree of the two graphs is almost the same, indicating that the introduction of security encryption module has little interference on trajectory tracking under environmental interference.

For the universality of the experiment, we set the environmental disturbance as $V_{water} = 0.02m/s$, $H = 0.01$, constraint parameter is set to $A = 1$, $B = 1$, $C = 1$. Under secure encryption conditions, linear, double-circle, and S-shape were used as reference trajectories for simulation experiments. Simulation results are shown in Fig 11. Fig 12. and Fig. 13.

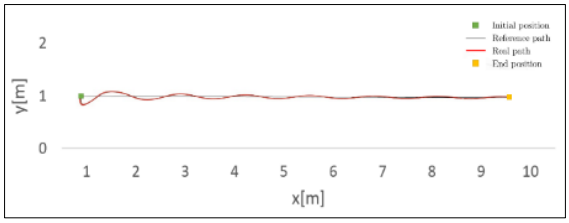

Figure 11. Results of linear path tracking under the security control framework ($V_{water} = 0.02m/s$, $H = 0.01$).

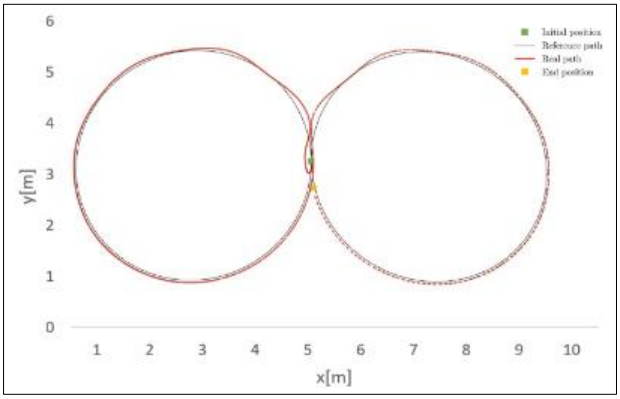

Figure 12. Results of double circular path tracking under the security control framework ($V_{water} = 0.02m/s$, $H = 0.01$).

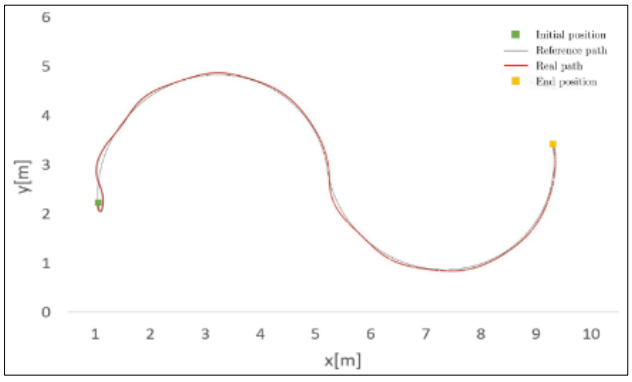

Figure 13. Results of S-shaped path tracking under the security control framework ($V_{water} = 0.02m/s$, $H = 0.01$).

The results show that the USV with an encryption algorithm can always follow the expected trajectory on the three reference trajectories. Our proposed secure encryption framework for USV trajectory tracking has been proven.

The main computation of trajectory tracking security control comes from encoding and encryption, decoding and decryption. According to the Paillier optimization encryption principle in Table 3, 128 bits, 256 bits, 384 bits, 512 bits, and 1024 bits were selected as the bit length of the experiment. Table 4 shows the processing time required for encryption/decryption with different key sizes in the security control implementation. This is what we got when we averaged the results of a hundred experiments. As can be seen from the table. Although the encryption effect can still be maintained when the key length keeps increasing, the time consumption also increases sharply. This is an expected result. It can be seen from Table 4 that the encryption/decryption process is based on the calculation of public and private keys. The larger the key length, the larger the calculation will be. According to the need for trajectory tracking simulation and NIST recommendations, we use a 256-bit key as the sampling period to perform the calculation task. At the same time, to obtain better security, a larger key must be used in the control, so the sampling frequency must be reduced.

To ensure the accuracy of the data, the standard deviation of calculation amount addition/decryption time in this paper is shown in Table 4. It can be seen from the table that the standard deviation is very small, indicating that the results of these 100 experiments are very stable.

Table 3. The statistics on encryption/decryption time

	128 bits	256 bits	384 bits	512 bits	1024 bits
Encryption time/s	0.002872	0.020141	0.064816	0.106346	0.625357
Decryption time/s	0.000723	0.005552	0.017706	0.040334	0.212336

Table 4. The standard deviation of Encryption /decryption time

	128 bits	256 bits	384 bits	512 bits	1024 bits
Standard deviation of encryption	0.000394	0.000616	0.001196	0.007303	0.012483
Standard deviation of decryption	0.000443	0.000502	0.000684	0.001163	0.004479

6. Conclusion

This paper presents a safety control framework for unmanned vehicle trajectory tracking based on MPC. To realize synchronous information encryption in trajectory tracking, we introduce the Paillier homomorphic encryption algorithm into the control framework. Data such as USV status information and control signals can be prevented from malicious interception and eavesdropping. Because Paillier homomorphic encryption does not support subtraction operations, and the encryption scheme and the trajectory tracking control algorithm have different data types. We introduce two simple algorithms to solve the compatibility problem between them. Through these efforts, data such as control signals and USV status information cannot be maliciously modified, intercepted, and eavesdropped. Then, the proposed safety control framework is applied to the simulation of underactuated unmanned vehicle, and the effectiveness of the proposed method is verified. The method proposed in this paper can not only be applied to the security protection of information transmission between the unmanned boat and the mother ship, but also has broad application space for the application scenarios such as the collaborative task execution of sea and air robots. In the future, we will focus on applying the proposed framework to more control schemes and working on developing more efficient encryption methods.

References

[1] Yuh J, Marani G, Blidberg D R. Applications of marine robotic vehicles. Intelligent service robotics, 2011, 4: 221-231.

[2] Jadhav, A. & Mutreja, S. Autonomous ships market. Allied Market Research-Freight & Logistics. Portland, Oregon, USA. 2020.

[3] Woo J, Park J, Yu C, et al. Dynamic model identification of unmanned surface vehicles using deep learning network. Applied Ocean Research, 2018, 78: 123-133.

[4] Faris Elasha, Matthew Greaves, David Mba, Abdulmajid Addali. Application of Acoustic Emission in Diagnostic of Bearing Faults within a Helicopter Gearbox, Procedia CIR, 2015, ISSN 2212-8271.

[5] O. Levander. Autonomous ships on the high seas. IEEE Spectrum. 54 (2), (2017), 26-31.

[6] Majohr J, Buch T. Modelling, simulation and control of an autonomous surface marine vehicle for surveying applications Measuring Dolphin MESSIN. IEE Control Engineering Series, 2006, 69: 329.

[7] Naeem W, Xu T, Sutton R, et al. The design of a navigation, guidance, and control system for an unmanned surface vehicle for environmental monitoring. Proceedings of the Institution of Mechanical Engineers, 2008, 222(2): 67-79.

[8] Dong, Z., Wan, L., Li, Y., Liu, T., Zhang, G. Trajectory tracking control of underactuated USV based on modifed backstepping approach. Int. J. Naval Architecture Ocean Eng., 7(5), 817-832 (2015).

[9] Wen, G., et al. Adaptive tracking control of surface vessel using optimized backstepping technique. IEEE Trans. Cybern., 49(9), 3420-3431 (2019).

[10] Zhang, J., Yu, S., Wu, D., Yan, Y. Nonsingular fixed-time terminal sliding mode trajectory tracking control for marine surface vessels with anti-disturbances. Ocean Eng., 217, 108158 (2020).

[11] Qiu, B., Wang, G., Fan, Y., Mu D., Sun, X.: Adaptive sliding mode trajectory tracking control for unmanned surface vehicle with modeling uncertainties and input saturation. Appl. Sci. 9(6), 1240 (2019)

[12] Zhao B, Zhang X, Liang C, et al. An improved model predictive control for path-following of USV based on global course constraint and event-triggered mechanism. IEEE Access, 2021, 9: 79725-79734.

[13] Yao, X., Wang, X., Zhang, L., Jiang, X. Model predictive and adaptive neural sliding mode control for three-dimensional path following of autonomous underwater vehicle with input saturation. Neural Computer. Appl., 32(22), 16875-16889 (2020).

[14] Zhang, J., Yang, G. Fault-tolerant fixed-time trajectory tracking control of autonomous surface vessels with specified accuracy. IEEE Trans. Industr. Electron., 67(6), 4889 (2020).

[15] Wang, N., Pan, X., Su, S.-F. Finite-time fault-tolerant trajectory tracking control of an autonomous surface vehicle. J. Franklin

Inst., 357(16), 11114-11135 (2020).

[16] Deng, Y., Zhang, X., Im, N., Zhang, G., Zhang, Q. Adaptive fuzzy tracking control for underactuated surface vessels with unmodeled dynamics and input saturation. ISA Trans., 103, 52-62 (2020).

[17] Dong, C., Ye, Q., Dai, S.-L. Neural-network-based adaptive output-feedback formation tracking control of USVs under collision avoidance and connectivity maintenance constraints. Neurocomputing, 401, 101-112 (2020).

[18] Zheng, Z., Ruan, L., Zhu, M., Guo, X. Reinforcement learning control for underactuated surface vessel with output error constraints and uncertainties. Neurocomputing, 399, 479-490 (2020).

[19] Zhang, X., Han, Q., Ge, X., Ding, D., Ding, L., Yue, D., & Peng, C. Networked control systems: A survey of trends and techniques. IEEE/CAA Journal of Automatica Sinica, 7(1), (2020), 1-17.

[20] Teixeira, A., Pérez, D., Sandberg, H., & Johansson, K.H. Attack models and scenarios for networked control systems. In: Proceedings of the 1st international conference on high confidence networked systems HiCoNS'12, Beijing, China. New York, NY: Association for Computing Machinery, (2012), pp. 55-64.

[21] Vinnem, J.E. & Utne, I.B. Risk from cyberattacks on autonomous ships. In: Haugen, S., Barros, A., van Gulijk, C., Kongsvik, T. & Vinnem, J.E. (Eds.) Safety and reliability—safe societies in a changing world: Proceedings of the ESREL 2018 June 17-21, 2018, Trondheim, Norway, 1st edition. London: CRC Press, pp. 1485-1492.

[22] Amin S, Schwartz G A, Sastry S S. Security of interdependent and identical networked control systems. Automatica, 2013, 49(1): 186-192.

[23] André Teixeira, Iman Shames, Henrik Sandberg, Karl Henrik Johansson. A secure control framework for resource-limited adversaries. Automatica, Volume 51, 2015.

[24] Huanhuan Yuan, Yuanqing Xia. Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework, Information Sciences, Volumes 454-455, 2018.

[25] Pang Z H, Liu G P. Design and implementation of secure networked predictive control systems under deception attacks. IEEE Transactions on Control Systems Technology, 2011, 20(5): 1334-1342.

[26] Farhad Farokhi, Iman Shames, Nathan Batterham. Secure and private control using semi-homomorphic encryption, Control Engineering Practice, Volume 67, 2017.

[27] Sun Q, Shi Y. Model Predictive Control as a Secure Service for Cyber-Physical Systems: A Cloud-Edge Framework. IEEE Internet of Things Journal, 2021, 9(22): 22194-22203.

[28] S. Amin, G. A. Schwartz, and S. S. Sastry. Security of interdependent and identical networked control systems. Automatica, vol. 49, no. 1, pp. 186-192, 2013.

[29] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. A secure control framework for resource-limited adversaries. Automatica, vol. 51, pp. 135-148, 2015.

[30] J. Wang, B. Ding, and J. Hu. Security control for LPV system with deception attacks via model predictive control: A dynamic output feedback approach. IEEE Transactions on Automatic Control, vol. 66, no. 2, pp. 760-767, 2021.

[31] Z.-H. Pang and G.-P. Liu. Design and implementation of secure networked predictive control systems under deception attacks. IEEE Transactions on Control Systems Technology, vol. 20, no. 5, pp. 1334-1342, 2012.

[32] F. Farokhi, I. Shames, and N. Batterham. Secure and private control using semi-homomorphic encryption. Control Engineering Practice, vol. 67, pp. 13-20, 2017.

[33] Q. Sun and Y. Shi. Model predictive control as a secure service for cyber-physical systems: A cloud-edge framework. IEEE Internet of Things Journal, 2021.

[34] Paillier, Pascal. Public-key cryptosystems based on composite degree residuosity classes. Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2-6, 1999 Proceedings 18. Springer Berlin Heidelberg, 1999.

[35] Fossen, Thor I. Handbook of marine craft hydrodynamics and motion control. John Wiley & Sons, 2011.