IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 25, 2020, accepted December 18, 2020, date of publication December 22, 2020, date of current version April 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3046483

Optimal Jamming Attack System Against Remote State Estimation in Wireless Network Control Systems

LI YANG[1] AND CHENGLIN WEN[2]
[1]School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
[2]System Modeling and Information Processing Laboratory, Hangzhou Dianzi University, Hangzhou 310018, China

Corresponding author: Chenglin Wen (wencl@hdu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61751304, Grant 61933013, Grant U1664264, and Grant 61673160.

ABSTRACT Recently, public attention is thoroughly aroused as to the security threats of Wireless Network Control System (WNCS), which can seriously disrupt the system operation. In order to achieve the attack effect that each sensor is damaged and maximize the terminal estimation error covariance, it is necessary to study an attack system from the attacker's perspective. In this paper, we establish an attack system, which includes: the multi-sensor importance evaluation model, the time allocation of jamming attack, and the attack rules. Specifically, we firstly establish the wireless network control system model and the jamming attack model. Then, according to the transmission data and channel parameter information which is intercepted by the attackers, we establish an evaluation model of sensor based on the Mean Impact Value (MIV) algorithm. Then, based on the evaluation results of each sensor, we establish a distribution model of the number of attacks on each sensor. Then, we perform two jamming attack rules(continuous attack rule and good-sensor-late-attack rule)to attack each sensor. Finally, we use the attack system to conduct digital simulation experiments in first-order and high-order system. There is no different between the MIV-based sensor evaluation method in the multi-sensor importance evaluation experiment and sensor performance evaluation based on estimation error. In the jamming attack time allocation experiment, effect that every sensor was attacked had been achieved. In the attack rule experiment, we compare the experimental results of ''continuous attack'' and '' discontinuous attack'', and the result shows that the effect of ''continuous attack'' is better than that of ''intermittent attack''. Similarly, we have conducted comparative experiments on all attack strategies, and the results show that '' good-sensor-late-attack '' strategy has the best effect. The effectiveness of the attack system is proved by digital simulation experiment.

INDEX TERMS Wireless networked control systems, jamming attack system, mean impact value algorithm, CMIV evaluation model, terminal estimation error.

I. INTRODUCTION

Wireless networked control systems (WNCS) are defined as a spatial distributed system which connects sensors, remote estimators and controllers by wireless communication network [1], [2].With the rapid development of Internet technology, WNCS have been extensively used, such as smart grid, smart logistics, smart transportation and smart home [3], [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

At present, WNCSs have been increasingly important in industrial systems. Due to their ''openness'' characteristics [5], they are prone to be attacked. As a result, the security issues of WNCSs have aroused so much interest from researchers [6], [7]. Attackers study how to attack WNCSs, while defenders study how to detect attacks [8], [9]. Generally speaking, there are four types of network attacks [10]: space hiding-time hiding attacks, such as system simulation attacks, Stuxnet-type replay attacks, etc.; space non-hidden-time hiding attacks, such as zero dynamic attacks, zero-dynamic induced attacks, etc.; space hiding-time non-hiding attacks, such as data Injection attacks, topological attacks, etc.;

space does not hide-time does not hide attacks, such as DoS attacks, general replay attacks, etc.

Based on the above categories, the most common attack methods mainly include: false data injection attack, replay attack and DoS attack. The false data injection attack is defined as modifying the integrity data of data packets transmitted between components in the system [11]. Further, the researcher defines a stealthy fake data injection attack [12], [13]. As for the replay attack, it first records data from the system, and then injects the recorded data into the system to perform the attack [14], [15]. The DoS attack exploits limited network resources by constantly sending excess data to attack network. Jamming attack is a typical Dos attack which can block the transmission of information. Therefore, this paper mainly considers jamming attack.In the paper [16], based on the defender's perspective, the researcher proposed a scheme, which can detect node compromise attack without having the need to share a key ring. However, there are few research results on jamming attacks from the perspective of attackers. In the paper [17], the attacker studied the Dos attack strategy that maximizes the LOG cost function under energy constraints. Because the state estimate is obtained on the sensor, and the state estimation value and the estimated error covariance are transmitted to the remote estimator through the wireless network channel. Therefore, it leads to increase the pressure of network bandwidth, and the sensor must be a smart sensor. In [18], a necessary and sufficient condition is established for the scenario where the attacks are undetectable by the detector of the multi-sensor system. But the point is that it's difficult to get sensor parameters. In the paper [19], researcher established a multivariate evaluation model. Based on this evaluation model, the suitable number of sensors can be obtained. The work in [20] applies the idea of cooperative game to design an optimal power allocation strategy when there are multiple attackers. The authors in [21] present a probabilistic attack method that the attacker perceives the channel state and execute the DoS attack only when the channel is idle. The authors in [22] investigate optimal attack schedule problems of the wireless Cyber-Physical Systems with two sensors under DoS attack. However, the researchers didn't take it into consideration that the allocated attack time of each sensor is different because of the different relative importance. In addition, they also didn't take account of the ''universality'' of the attack.

This paper studies the scenario where multiple sensors transmit measured values to remote estimators through wireless channels. We should ensure every sensor being attacked. Meanwhile, each sensor has a different contribution to the physical device, and relative importance of each sensor is different, so the attack time is also different. Therefore, in order to maximize the terminal estimated error covariance, the purpose of this article is to design an optimal attack system from the attacker's point of view based on the different importance of each sensor under the constraints of the attacker. The main contributions of this article are as follows:

(1) We firstly establish a complete jamming attack system, including multi-sensor importance evaluation model, the time allocation of jamming attack and two attack rules.

(2) Then, in the multi-sensor importance evaluation model, we use the idea of MIV algorithm to analyze the relative importance of each sensor.

(3) Then, based on the results of sensor importance analysis, we allocate the attack time of each sensor. We guarantee that every sensor is attacked, and the relatively important sensor will be attacked for more time.

(4) Then, with the goal of maximizing the terminal estimated error covariance, we formulate two attack rules.

(5) Finally, this paper proves the validity of the conclusion through digital simulation experiment.

The rest of this paper is organized as follows. Section II presents the system model and attack model, and proposes a method for the identification of sensor structure parameter, and formulates the optimal jamming attack scheduling problem. Section III constructs an attack system, which includes multi-sensor importance evaluation, the time allocation of jamming attack and attack rules. In Section IV, we provide several numerical examples to validate our theoretical results. Section V draws conclusions.

Notations: In the whole paper, Z are the sets of all integers. R^n represents the Euclidean space with n-dimension. $P[X]$ and $E[X]$ refer to probability and expectation for a random variable X, whose spectral radius is presented by $\rho(X)$.

II. PROBLEM FORMULATION

A. SYSTEM EQUATIONS AND OBSERVATION EQUATIONS

As shown in Figure 1, a wireless network control system is composed of physical devices, multiple sensors and remote estimators. It has broader application because of its characteristics of cheapness, easy deployment and easy expandability [23].

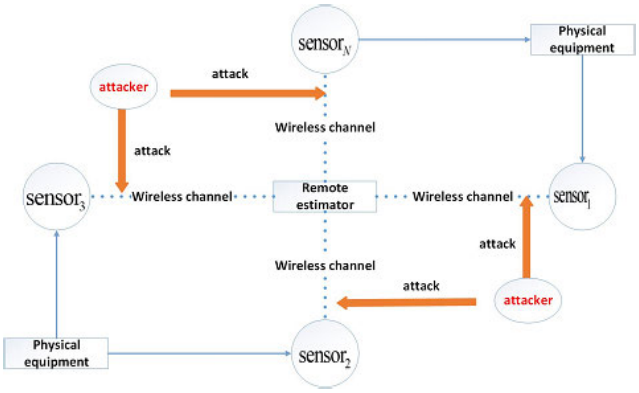

FIGURE 1. Wireless network control system.

Taking the discrete-time linear time-invariant system as an example, this paper constructs the system equation and observation equation of the wireless network control system, as shown below [24]:

$$\begin{aligned} x(k+1) &= Ax(k) + \omega(k) \\ y_i(k) &= Hx_i(k) + v_i(k) \quad i = 1, 2, 3, \ldots \end{aligned} \tag{1}$$

where $k \in Z$ is a discrete time series, $x(k) \in R^{n_x}$ is the state value of the system, assuming that the initial state of the system is $x(0)$, $y_i(k) \in R^{m_y}$ is the measured value of the ith sensor, $\omega(k)$is the process noise, assuming it is Gaussian white noise, the mean is 0, and the variance is $Q \geq 0$, $v_i(k) \in R^{n_y}$ is the measurement noise, assuming it is Gaussian white noise, the mean is 0, and the variance is $R_i \geq 0$, $A \in R^{n\times n}$, $H \in R^{m\times n}$, $x(k)$, $\omega(k)$, and $v_i(k)$ are mutually independent.

B. THE IDENTIFICATION OF SENSOR STRUCTURE PARAMETER

This paper assumes that there are N sensors in total and the attacker cannot know the structural parameter information of the sensor,which means that the measurement matrix H in formula (1) cannot be known, but the attacker can obtain the data set y as follows by monitoring and recording the measurement value of each sensor:

$$\begin{aligned} y &= [y_1, y_2, \ldots, y_i, \ldots y_N] \\ y_i &= [y_{i1}, y_{i2}, \ldots\ldots, y_{ik}] \end{aligned} \tag{2}$$

where y_i represents the ith sensor and y_{ik} represents the measured value of the ith sensor at the kth moment.

It is assumed that the attacker is aware of the knowledge of system dynamics, that is, the attacker can use the existing priori knowledge to analyze the measurement equation and determine model structure. This paper adopted ''Maximum Exponential Square State Estimator'' which was proposed in the papers [25], [26] and [27]. So the objective function is as follows:

$$\min_H \sum_{i=1}^{k} -\omega_i \exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}) \tag{3}$$

where ω_i is the weight; $\sigma$is the Parzen window width.

Let $F = \sum_{i=1}^{k} -\omega_i \exp(-\frac{(y_i-Hx_i)^2}{2\sigma^2})$, where i represents the ith sensor. The derivative of F to H is obtained:

$$\begin{aligned} \frac{\partial F}{\partial H} &= \sum_{i=1}^{k} -\omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(-\frac{2(y_i - Hx_i)(-x_i)}{2\sigma^2}) \\ &= -\frac{1}{\sigma^2}\sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))((y_i - Hx_i)x_i) \\ &= -\frac{1}{\sigma^2}\sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(y_i x_i) \\ &\quad -\omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(H(x_i)^2) \end{aligned} \tag{4}$$

Let $\frac{\partial F}{\partial H} = 0$, then the closed-form solution of H is as follows:

$$\begin{aligned} &\Rightarrow 0 = \sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(y_i x_i) \\ &\quad -\omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(H(x_i)^2) \\ &\Rightarrow 0 = \sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(y_i x_i) \\ &\quad -\sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(H(x_i)^2) \\ &\Rightarrow \sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(y_i x_i) \\ &\quad = \sum_{i=1}^{k} \omega_i(\exp(-\frac{(y_i - Hx_i)^2}{2\sigma^2}))(H(x_i)^2) \\ &\Rightarrow \sum_{i=1}^{k} y_i x_i = H\sum_{i=1}^{k} (x_i)^2 \\ &\Rightarrow H = \frac{\sum_{i=1}^{k} y_i x_i}{\sum_{i=1}^{k} (x_i)^2} \end{aligned} \tag{5}$$

C. THE REMOTE ESTIMATOR

The attacker monitors the wireless communication network and launches a jamming attack to block measurement value of transmission $y_i, i \in \{1, 2, \ldots, N\}$. This paper use variable θ to describe the attacker's attack status, as shown below:

$$\theta = \begin{cases} 1, & \text{Attacker launches an attack} \\ 0, & \text{other} \end{cases} \tag{6}$$

Therefore, the function $y_a^*(k)$ represents the data received by the remote estimator, as shown below:

$$y_a^*(k) = \theta f(y^*(k)) + (1 - \theta)y^*(k) \tag{7}$$

where $f(y^*(k)) = [y_1(k)y_2(k)\ldots y_{i+1}(k)y_{i-1}(k)\ldots y_N(k)]^T$.

According to the modified Kalman filter [28], [29], the optimal estimated value $\hat{x}_a(k)$ is obtained in the remote estimator, as shown below:

$$\hat{x}_a(k|k-1) = A\hat{x}_a(k-1) \tag{8}$$

$$\hat{P}_a(k|k-1) = A\hat{P}_a(k-1)A^T + Q \tag{9}$$

$$\hat{P}_a^{-1}(k) = \hat{P}_a^{-1}(k|k-1) + \sum_{i\in s} (H_a^*)^T R_i^{-1} H_a^* \tag{10}$$

$$\hat{K}_a(k) = \hat{P}_a(k)(H_a^*)^T[R_i^{-1}, i \in s] \tag{11}$$

$$\hat{x}_a(k) = \hat{x}_a(k|k-1) + \hat{K}_a(k)(y_a^*(k) - H_a^*\hat{x}_a(k|k-1)) \tag{12}$$

where s represents the attack scheduling of the attacker, namely: $s = (\xi(1), \xi(2), \ldots, \xi(T))$, $\xi(k) = i$ means that the attacker attacks the ith sensor at k time, $\hat{K}_a(k)$ refers to the gain of the Kalman filter, $H_a^* = H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_N]^T$.

D. THE JAMMING ATTACK MODEL

There is an attacker in the scenario considered in this paper. Since wireless communication signals can only be transmitted over one channel at a time, the attacker can only attack one channel at once [30]. $\xi(k) = i$ means that the attacker

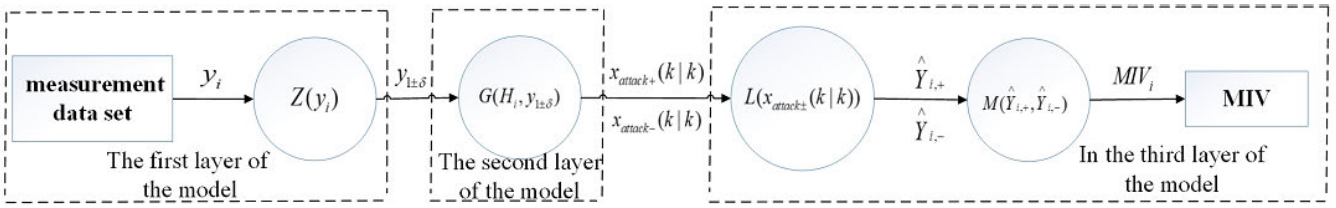

FIGURE 2. CMIV model.

attacks the communication channel of sensor i at the time kth, so $1_{\xi(k)=1} + 1_{\xi(k)=2} + \cdots + 1_{\xi(k)=N} \leq 1$ [31].

In order to make the attack broader, it is required that each sensor must be subject to jamming attacks, namely:

$$\tau_1 > 0, \tau_2 > 0, \tau_3 > 0, \ldots\ldots, \tau_N > 0 \tag{13}$$

where τ_i represents the attack time of the ith sensor.

The accuracy of the measurement data varies because of the quality differences of sensors. Therefore, the assigned attack time is relevant to the relative importance of each sensor. In this paper, the relatively important sensors get more jamming attack time, and the relatively less important sensors get less jamming attack time, namely:

$$\eta_i > \eta_j \Rightarrow \tau_i > \tau_j \tag{14}$$

where η_i represents the relative importance of the ith sensor and τ_i represents the attack time of the ith sensor.

Due to $\hat{P}_a(k) = E[(x(k) - \hat{x}_a(k))(x(k) - \hat{x}_a(k))^T]$ [32], as mentioned in [34], the estimation error $\hat{P}_a(T)$ at the end time T is an important indicator to measure the estimation performance. Therefore, this paper solves the following problems:

Problem 2.1.

$$\max \ \mathrm{Tr}[J_T(s)] \tag{15}$$
$$s.t.\ 1_{\xi(k)=1} + 1_{\xi(k)=2} + \cdots + 1_{\xi(k)=N} \leq 1 \tag{16}$$
$$\tau_1 > 0, \quad \tau_2 > 0, \quad \tau_3 > 0, \ldots\ldots, \tau_N > 0 \tag{17}$$
$$\eta_i > \eta_j \Rightarrow \tau_i > \tau_j \tag{18}$$

where $J_T(s) = \hat{P}_a(T)$ is the estimated error at the end time under the attack strategy s.

III. THE SYSTEM OF JAMMING ATTACK

A. MULTI-SENSOR IMPORTANCE EVALUATION BASED ON CMIV MODEL

This paper establishes a CMIV (Centralized-Mean-Impact-Value) model. This model is used to evaluate the relative importance of multi-sensor. And the model employs the Mean Impact Value (MIV) algorithm, as shown in Figure 2. The MIV algorithm was first applied to Neural Network to reflect the influence of feature input in each dimension, on at the output of Neural Network. Later, the researcher uses the MIV algorithm to evaluate the influence weight of the network feature input on the network output [33].

Assuming that there are N sensors. The first layer of the model, input the data of sensor measurement y_i and get $y_{1\pm\delta}$ through the function $Z(y_i)$, as shown below:

$$\begin{aligned} Z(y_i) = y_{1\pm\delta} &= [y_1, y_2, \ldots\ldots (1 \pm \delta) y_i] \\ y_i &= [y_i(1), y_i(2), \ldots, y_i(k)] \end{aligned} \tag{19}$$

where $Z(y_i)$ represents the self-increment and self-decrement of the measured value of the evaluated ith sensor.

The second layer of the model takes the output $y_{1\pm\delta}$ of the first layer as input, and get $x_{attack+}(k|k)$ and $x_{attack-}(k|k)$ through the function $G(y_{1\pm\delta})$, as shown below:

$$G(y_{1\pm\delta}) = \begin{cases} x_{attack}(k|k-1) = A x_{attack}(k-1|k-1) \\ P_{attack}(k|k-1) = A P_{attack}(k|k-1) A^T + Q \\ x_{attack\pm}(k|k) = x_{attack}(k|k-1) + \\ K_{attack}[y_{1\pm\delta} - h x_{attack}(k|k-1)] \\ K_{attack} = \dfrac{P_{attack}(k|k-1) h^T}{(h P_{attack}(k|k-1) h^T + R)} \\ P_{attack}(k|k) = (I - \mathrm{K}_{attack} h) P_{attack}(k|k-1) \end{cases} \tag{20}$$

where I represents the identity matrix, h^T represents the transpose of matrix h and A^T represents the transpose of matrix A.

In the third layer of the model, the outputs $x_{attack+}(k|k)$ and $x_{attack-}(k|k)$ of the second layer are used as inputs, and the outputs $\hat{Y}_{i,+}$ and $\hat{Y}_{i,-}$ are generated through the function $L(x_{attack\pm}(k|k))$ first, and then the output MIV_i can be obtained by the function $M(\hat{Y}_{i,+}, \hat{Y}_{i,-})$, as follows:

$$\begin{aligned} \hat{Y}_{i,+} &= \frac{1}{K} * \sum_{k=1}^{K} \left\| x_{i,attack+}(k|k) - x_{attack}(k) \right\|_2 \\ \hat{Y}_{i,-} &= \frac{1}{K} * \sum_{k=1}^{K} \left\| x_{i,attack-}(k|k) - x_{attack}(k) \right\|_2 \end{aligned} \tag{21}$$

$$\begin{aligned} MIV_i &= (\hat{Y}_{i,+}) - (\hat{Y}_{i,-}) \\ &= \frac{1}{K} * \Big(\sum_{k=1}^{K} \left\| x_{i,attack+}(k|k) - x_{attack}(k) \right\|_2 \\ &\quad - \sum_{k=1}^{K} \left\| x_{i,attack-}(k|k) - x_{attack}(k) \right\|_2 \Big) \end{aligned} \tag{22}$$

where $\|.\|_2$ represents the two-dimensional norm, let $0.1 \leq \delta \leq 0.3, i = 1, 2, \ldots\ldots N$.

In summary, the final output MIV_i of the model is the average impact value of the ith sensor which need to be evaluated. In the same way, the average influence value $MIV = [MIV_1, MIV_2, \ldots\ldots, MIV_N]$ of each sample in the data set $y = [y_1(k), y_2(k), \ldots\ldots y_N(k)]$ could be calculated according to the above steps. The absolute value of MIV_i is regarded as the relative importance of each sensor, namely:

$$\begin{cases} \eta_i > \eta_j & |MIV_i| > |MIV_j| \\ \eta_i < \eta_j & |MIV_i| < |MIV_j| \end{cases} \tag{23}$$

where η_i represents the importance of the ith sensor, and $|.|$ represents the absolute value.

B. THE TIME ALLOCATION OF JAMMING ATTACK

From the perspective of the attacker, the allocation of attack time is relevant to the relative importance of each sensor. The attack time of the relatively important sensor should be more than the attack time of the relatively unimportant sensor. At the same time, in order to ensure each sensor being attacked, this paper allocates the attack time of each sensor based on the sensor evaluation result of the CMIV model, as shown below:

$$\tau_i = \frac{MIV_i}{\sum_{j=1}^{N} MIV_j} * \tau' \tag{24}$$

where τ' represents the total attack time allocated by the attacker, τ_i represents the attack time allocated by the ith sensor and N means there is a total of N sensors.

C. JAMMING ATTACK RULE

As described in formula 1:

$$\begin{aligned} x(k+1) &= Ax(k) + w(k) \\ y_i(k) &= Hx(k) + v_i(k) \end{aligned} \tag{25}$$

where $w(k)$ and $v_i(k)$ are zero-mean Gaussian white noise, and their variances are Q and R_i respectively, and they are independent of each other.

Rewrite Equation (10) as:

$$\hat{P}(k+1) = \frac{1}{h^{-1} + g} \tag{26}$$

where $h = A\hat{P}(k)A^T + Q$, $g = \sum_{i \in s} H^T R_i^{-1} H$.

Theorem 1: With the goal of maximizing the estimated error $\hat{P}(T)$ at the terminal, the optimal strategy for solving problem 2.1 is: continuous attack is better than discontinuous attack.

Proof: Suppose that the attacker has T attack time, attack strategy 1 is $s_1 = \{1, 1, 1, 1, \ldots, 1\}$, $number(1) = T$ and attack strategy 2 is $s_2 = \{1, 0, 1, 0, 1, 0, \ldots, 1\}$, $number(1) = T$. When the first attack is completed, the estimation error of attack strategy 1 is the same as attack strategy 2, namely: $\hat{P}_{s_1}(1) = \hat{P}_{s_2}(1)$;When the second attack is completed, the estimated error of attack strategy 1 is $\hat{P}_{s_1}(2)$, attack strategy 2 did not attack at this time: $g(1_0)_{s_2} > g_{s_1}(2)$, $h_{s_2}(1_0) = h_{s_1}(2)$, as shown in formula (26), $\hat{P}(k+1)$ is proportional to h and inversely proportional to g, so $\hat{P}_{s_1}(2) > \hat{P}_{s_2}(1_0)$. When attack strategy 2 completes the second attack, $\hat{P}_{s_1}(2) > \hat{P}_{s_2}(1_0)$, so $h_{s_1}(2) > h_{s_2}(2)$ and $g(2)_{s_2} > g_{s_1}(2)$. Similarly, we get: $\hat{P}_{s_1}(2) > \hat{P}_{s_2}(2)$; We can get $\hat{P}_{s_1}(T) > \hat{P}_{s_2}(T)$ in a similar way.

Theorem 2: With the goal of maximizing the estimated error $\hat{P}(T)$ at the terminal, the optimal strategy to solve problem 2.1 is: the attacker follows the "good-sensor-late-attack" strategy.

Proof: The smaller the measurement noise in formula (26), the more accurate the sensor's measurement value generally is. Suppose the variances of the measurement noises of the three sensors are r_1, r_2, r_3 and $r_1 < r_3$, so $\frac{1}{r_1} + \frac{1}{r_2} > \frac{1}{r_3} + \frac{1}{r_2}$,then get $H^T(\frac{1}{r_1} + \frac{1}{r_2})H > H^T(\frac{1}{r_3} + \frac{1}{r_2})H = (H^T\frac{1}{r_1}H + H^T\frac{1}{r_2}H) > (H^T\frac{1}{r_3}H + H^T\frac{1}{r_2}H)$, namely $g_{r1r2} > g_{r3r2}$. As shown in formula (26), $\hat{P}(k+1)$ is inversely proportional to g, so $\hat{P}_{r1r2}(k+1) < \hat{P}_{r3r2}(k+1)$. Therefore, the attacker follows the " good-sensor-late-attack " strategy to maximize $\hat{P}(T)$.

IV. ILLUSTRATIVE EXAMPLES

A. SIMULATION ANALYSIS OF MULTI-SENSOR IMPORTANCE EVALUATION

Assuming that the wireless network control system consists of three sensors. The followings are measured values of the three sensors in Figure 3-5. In these figures, the x-axis represents time in seconds, and the y-axis represents the measured value of the sensor.

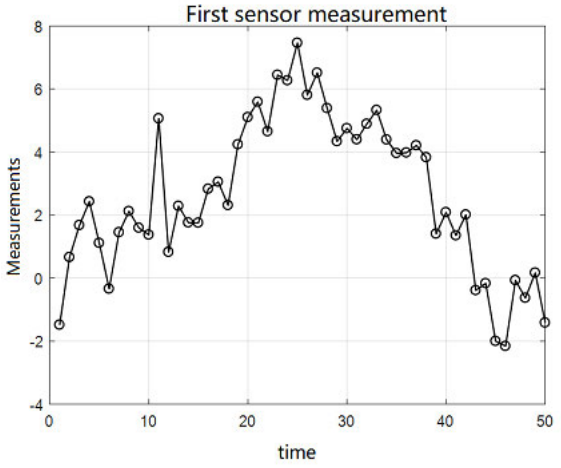

FIGURE 3. The first sensor measurement.

1) THE SIMULATION OF IMPORTANCE EVALUATION OF SENSORS BASED ON CMIV MODEL

This paper evaluates relative importance of 3 sensors according to the CMIV sensor evaluation model proposed earlier in the paper. The main parameters of the CMIV sensor

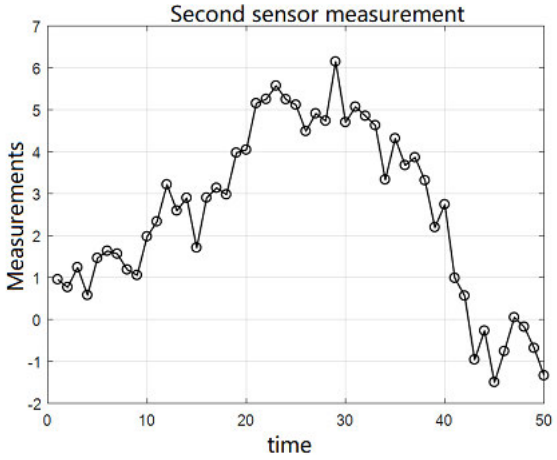

FIGURE 4. The second sensor measurement.

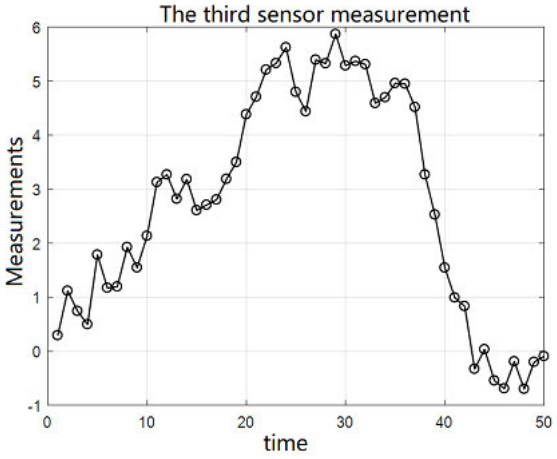

FIGURE 5. The third sensor measurement.

evaluation model are as follows: $A = 1$, $Q = 0.5$, $x_0 = 0$, $k = 50$, $\delta = 0.2$. The measured values of the three sensors (Figure 3-Figure 5) are taken as the model input, and the output of the model is obtained in turn: MIV_1, MIV_2, MIV_3,as shown in the following table:

Table 1 shows, the MIV_1 is 0.0467, the MIV_2 is 0.0912, the MIV_3 is 0.1375. The MIV_1 is smaller than the MIV_2 and the MIV_2 is smaller than the MIV_3.

TABLE 1. CMIV model output MIV value.

Sensor	$\hat{Y}_{N,+}$	$\hat{Y}_{N,-}$	MIV
1	0.1951	0.1484	0.0467
2	0.2508	0.1596	0.0912
3	0.3314	0.1939	0.1375

2) THE SIMULATION OF IMPORTANCE EVALUATION OF SENSOR BASED ON REAL SYSTEM MODEL

The system state equation parameters and the measurement equation parameters of these three sensors are as follows:

$$A = 1, Q = 0.5, \quad H_1 = H_2 = H_3 = 1,$$
$$R_1 = 1,\ R_2 = 0.5,\ R_3 = 0.2, \delta = 0.2$$

Use the MIV algorithm to evaluate the relative importance of the three sensors and obtain successively: MIV_1, MIV_2, MIV_3, as shown in the following table:

TABLE 2. MIV value based on real system.

Sensor	$\hat{Y}_{N,+}$	$\hat{Y}_{N,-}$	MIV
1	0.2012	0.1465	0.0547
2	0.2753	0.1587	0.1166
3	0.3489	0.1947	0.1542

The table 2 shows, the MIV_1 is 0.0547, the MIV_2 is 0.1166, MIV_3 is 0.1542.The MIV_1 is smaller than the MIV_2, and the MIV_2 is smaller than the MIV_3.

3) THE SIMULATION OF SENSOR IMPORTANCE EVALUATION BASED ON ESTIMATION ERROR OF REAL SYSTEM

The system state equation parameters and the measurement equation parameters of the three sensors are as follows:

$$A = 1, Q = 0.5, \quad H_1 = H_2 = H_3 = 1,$$
$$R_1 = 1,\ R_2 = 0.5,\ R_3 = 0.2$$

Use the Kalman filter algorithm to simulate the three sensors, and obtain the one-dimensional norm of the estimated errors of three sensors in turn, as follows:

TABLE 3. Estimated error based on real system.

Sensor	The average estimation error
1	0.4420
2	0.3174
3	0.1795

According to Table 3, the average estimation error of sensor 1 is greater than that of sensor 2, and the average estimation error of sensor 2 is greater than that of sensor 3.

The comparison of the simulation results in Table 1 and Table 2 shows that the sensor importance evaluation method based on sensor structure parameter identification, and the sensor importance evaluation method based on the real system have the same MIV value order of the three sensors. According to Kalman filtering algorithm, the smaller the estimation error, the better the performance of the sensor. From Table 3, it can be concluded that the performance of sensor 3 is better than that of sensor 2, and the performance of sensor 2 is better than that of sensor 1. The importance of the sensors obtained by the MIV value sorting is the same as the sensor performance evaluation results obtained in Table 3.

B. THE SIMULATION ANALYSIS OF OPTIMAL JAMMING ATTACK

1) THE TIME ALLOCATION OF JAMMING ATTACK

Assume that the attack time provided by the attacker is $\tau' = 15$, and according to formula 24 the calculated attack time of the three sensors is as follows:

$$\tau_1 = \frac{0.0467}{0.0467 + 0.0912 + 0.1375} \times 15 = 3$$

$$\tau_2 = \frac{0.0912}{0.0467 + 0.0912 + 0.1375} \times 15 = 5$$
$$\tau_3 = \frac{0.1375}{0.0467 + 0.0912 + 0.1375} \times 15 = 7$$

2) COMPARATIVE SIMULATION ANALYSIS OF CONTINUOUS ATTACK AND DISCONTINUOUS ATTACK

Considering only to attack sensor 3, assume that the attack strategy 1 is a continuous attack, namely: $r_1 = \{1\ 1\ 1\ 1\ 1\ 1\ 1\}$ and suppose attack strategy 2 is an intermittent attack, namely:

$$r_2 = \{1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\}.$$

where {.} is attack rule, "1" means to launch an attack, "0" means no attack.

Figure 6 shows the variation curve of the estimation error, "O" represents attack strategy1 and "*" represents attack strategy2. In attack strategy 1, when the attack is completed, the estimation error is 0.2287. In attack strategy 2, when the attack is completed, the estimated error is 0.2151. The estimation error of terminal time in attack strategy 1 is larger than that in strategy 2.

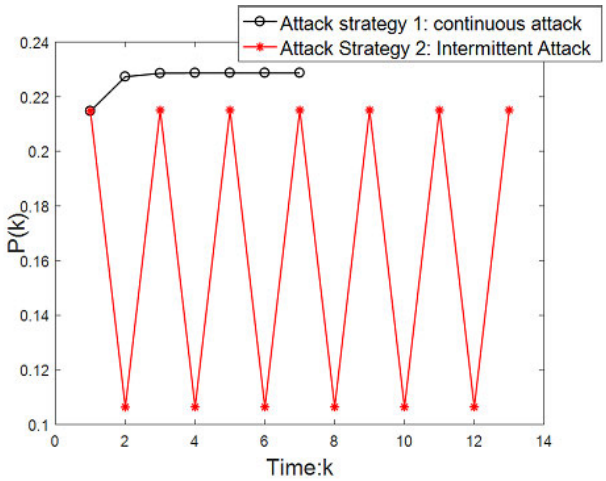

FIGURE 6. Comparison of continuous and intermittent attacks.

3) SIMULATION ANALYSIS OF "attacking GOOD SENSOR LATER" STRATEGY

For three sensors, there are six feasible attack strategies. According to the attack time allocated by B.1, as shown below:

$$s_1 = \left\{\begin{matrix} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1 \end{matrix}\right\}$$
$$s_2 = \left\{\begin{matrix} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1&1 \\ 0&0&0&1&1&1&1&1&1&1&0&0&0&0&0 \end{matrix}\right\}$$
$$s_3 = \left\{\begin{matrix} 0&0&0&0&0&1&1&1&0&0&0&0&0&0&0 \\ 1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1 \end{matrix}\right\}$$
$$s_4 = \left\{\begin{matrix} 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&1&1&1&1&1&1&0&0&0 \end{matrix}\right\}$$
$$s_5 = \left\{\begin{matrix} 0&0&0&0&0&0&0&1&1&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1&1 \\ 1&1&1&1&1&1&1&0&0&0&0&0&0&0&0 \end{matrix}\right\}$$
$$s_6 = \left\{\begin{matrix} 1&1&1&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&1&1&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \end{matrix}\right\}$$

where {.} is attack rule, the first line represents the attack strategy for the first sensor, the second line represents the attack strategy against the second sensor, and the third line represents the attack strategy against the third sensor, "1" means to launch an attack, "0" means no attack.

Figure 7 shows the changes of estimated error of six attack strategies. The figures show that the attack strategies with the largest estimated error performance at the end time $k = 60$ are attacking strategy s_1 and attack strategy s_3. When the estimated error performance at the end point of the two attack strategies is the same, we reversely compare the estimated error at each point from the end point. In the time period $k = 54$ to $k = 60$, the estimation error of attack strategy s_1 and attack strategy s_3 is the same. When $k = 53$,the estimated error performance of attack strategy s_1 is greater than that of attack strategy s_3, so one of the optimal attack rules for problem 2.1 is s_1.

C. SIMULATION ANALYSIS OF MULTI-SENSOR IMPORTANCE EVALUATION BASE ON HIGH-ORDER SYSTEM

1) THE SIMULATION OF IMPORTANCE EVALUATION OF SENSORS BASED ON CMIV MODEL

This paper evaluates the relative importance of 2 sensors according to the CMIV sensor evaluation model proposed earlier in the paper. Consider the system (1) with

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 0.5 & 1 \end{bmatrix},$$
$$Q = 0.5, \quad R_1 = 10, \ R_2 = 2$$

Use the MIV algorithm to evaluate the relative importance of the two sensors and obtain successively: MIV_1, MIV_2, as shown in the following table:

TABLE 4. MIV value based on high-order system.

Sensor	$\hat{Y}_{N,+}$	$\hat{Y}_{N,-}$	MIV
1	2.9726	2.7552	0.2174
2	3.0621	2.7042	0.3579

Table 4 shows, the MIV_1 is 0.2174, the MIV_2 is 0.3579. The MIV_1 is smaller than the MIV_2.

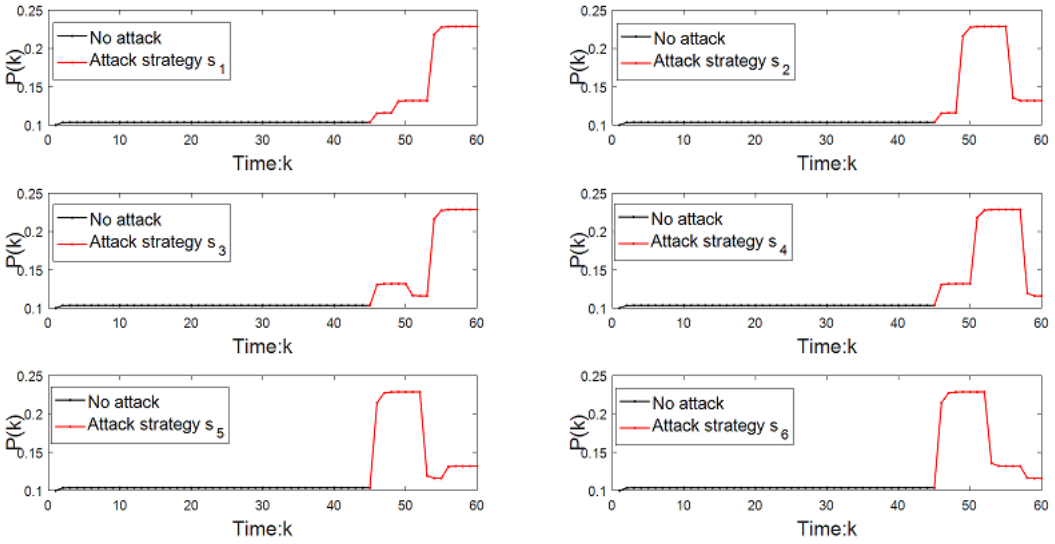

FIGURE 7. Comparison of estimation error performance of 6 attack strategies.

2) THE SIMULATION OF SENSOR IMPORTANCE EVALUATION BASED ON THE ESTIMATION ERROR

Use the Kalman filter algorithm to simulate the two sensors, and obtain the one-dimensional norm of the estimated errors of two sensors in turn, as follows:

TABLE 5. Estimated error.

Sensor	The average estimation error
1	4.7232
2	1.7671

According to Table 5, the average estimation error of sensor 1 is greater than that of sensor 2.

According to Kalman filtering algorithm, the smaller the estimation error, the better the performance of the sensor. According to Table 5, the performance of sensor 2 is better than that of sensor 1. The sensor importance obtained by sorting the *MIV* value in Table 4 is the same as the sensor performance evaluation result obtained in Table 5.

D. THE SIMULATION ANALYSIS OF JAMMING ATTACK RULE BASE ON HIGH-ORDER SYSTEM

1) THE TIME ALLOCATION OF JAMMING ATTACK

Assume that the attack time provided by the attacker is $\tau' = 15$, and according to formula 24 the calculated attack time of the two sensors is as follows:

$$\tau_1 = \frac{0.2174}{0.2174 + 0.3579} \times 15 = 6$$
$$\tau_2 = \frac{0.3579}{0.2174 + 0.3579} \times 15 = 9$$

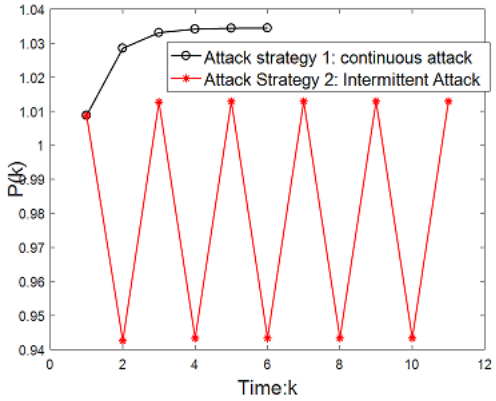

FIGURE 8. Comparison of continuous and intermittent attacks in the high-order system.

2) COMPARATIVE SIMULATION ANALYSIS OF CONTINUOUS ATTACK AND DISCONTINUOUS ATTACK

Considering only to attack sensor 2, assume that the attack strategy 1 is a continuous attack, namely: $v_1 = \{111111\}$ and suppose the attack strategy 2 is an intermittent attack, namely:

$$v_2 = \{1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1\}.$$

where {.} is attack rule, "1" means to launch an attack, "0" means no attack.

Figure 8 shows the variation curve of the estimation error. "O" is attack strategy 1 and "*" is attack strategy 2. In attack strategy 1, when the attack is completed, the estimated error is 1.0345. In attack strategy 2, when the attack is completed, the estimated error is 1.0129. The estimation error of terminal time in attack strategy 1 is larger than that in strategy 2. So, one of the optimal attack rules for problem 2.1 is v_1.

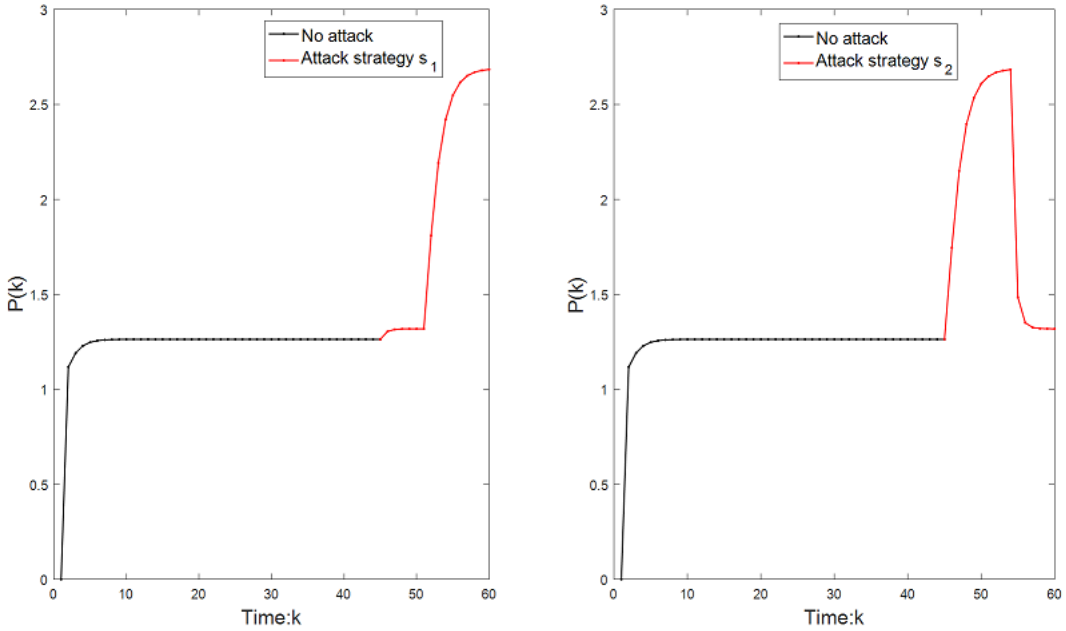

FIGURE 9. Comparison of estimation error performance of 2 attack strategies.

Therefore, the validity of theorem 3.1 in this paper can be proved.

3) SIMULATION ANALYSIS OF "attacking GOOD SENSOR LATER" STRATEGY BASE ON HIGH-ORDER SYSTEM

According to the attack time allocated by D.1, there is a total of 2 attack strategies, as shown below:

$$m_1 = \left\{ \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix} \right\}$$

$$m_2 = \left\{ \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} \right\}$$

where {.} is attack rule, the first line represents the attack strategy for the first sensor, the second line represents the attack strategy against the second sensor, "1" means to launch an attack, "0" means no attack.

Figure 9 shows the curve of estimation error covariance over time. As can be seen from the figure, the attacker did not launch attack from $k = 1$ to $k = 45$. From $k = 46$ to $k = 60$, attacker launched attack. Comparing the estimation error covariance of the two attack strategies, the estimation error covariance of attack strategy 1 is 2.684 at the end point $k = 60$, and that of attack strategy 2 is 1.319. At the end point, the estimation error covariance of attack strategy 1 is larger than that of attack strategy 2.

V. CONCLUSION

In this paper, we establish an attack system. Specifically, the attack system consists of three layers: the multi-sensor importance evaluation based on CMIV model, the time allocation of Jamming attack and attack rules. The sensor importance evaluation model based on CMIV can accurately evaluate the relative importance of each sensor. The allocation model of the number of sensor attacks can ensure that each sensor is attacked and the more important sensors are attacked for more time. The attack criterion can ensure that the estimation error covariance of the remote estimator is maximized at the end point, when sensor is attacked. We proved its effectiveness by simulation experiments. Future works include the study of attack rules for maximizing the average estimation error of remote estimator, jamming attack rules for wireless networked control systems with network delay, and jamming attack rules for non-Gaussian white noise scenarios [35].

REFERENCES

[1] D. Zhang, P. Shi, Q.-G. Wang, and L. Yu, "Analysis and synthesis of networked control systems: A survey of recent advances and challenges," *ISA Trans.*, vol. 66, pp. 376–392, Jan. 2017.

[2] H. Wang, S. Tan, Y. Zhu, and M. Li, "Deterministic scheduling with optimization of average transmission delays in industrial wireless sensor networks," *IEEE Access*, vol. 8, pp. 18852–18862, 2020.

[3] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang, "Distributed event-triggered estimation over sensor networks: A survey," *IEEE Trans. Cybern.*, vol. 50, no. 3, pp. 1306–1320, Mar. 2020.

[4] Xian-Ming, Zhang, Qing-Long, Han, Xiaohua, Ge, Derui, Ding, and Lei, "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Automatica Sinica*, vol. v.7, no. 01, pp. 4–20, 2020.

[5] T. Wen, C. Constantinou, L. Chen, Z. Tian, and C. Roberts, "Access point deployment optimization in cbtc data communication system," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 6, pp. 1985–1995, Jun. 2018.

[6] Y. Wang, S. X. Ding, D. Xu, B. Shen, "An fault estimation scheme of wireless networked control systems for industrial real-time applications," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 6, pp. 2073–2086, May 2014.

[7] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020.

[8] H. Yang, M. Shi, Y. Xia, and P. Zhang, "Security research on wireless networked control systems subject to jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 6, pp. 2022–2031, Jun. 2019.
[9] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.
[10] T. Liu, J. Tian, J. Z. Wang, H. Y. Wu, X. H. Guan, "Integrated security threats and defense of cyber-physical systems," *Zidonghua Xuebao/Acta Automatica Sinica*, vol. 45, no. 1, pp. 5–24, 2019.
[11] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.
[12] Z.-H. Pang, L.-Z. Fan, J. Sun, K. Liu, and G.-P. Liu, "Detection of stealthy false data injection attacks against networked control systems via active data modification," *Inf. Sci.*, vol. 546, pp. 192–205, Feb. 2021.
[13] Y.-G. Li and G.-H. Yang, "Optimal stealthy false data injection attacks in cyber-physical systems," *Inf. Sci.*, vol. 481, pp. 474–490, May 2019.
[14] M. S. Mahmoud, M. M. Hamdan, U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, Apr. 2019.
[15] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, "Optimal periodic watermarking schedule for replay attack detection in cyberïcphysical systems," *Automatica*, vol. 112, p. 108698, 2020.
[16] C. Aggarwal and B. B. Gupta, "Energy efficient key pre distribution scheme in WSN," in *Proc. 3rd IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2018, pp. 2480–2484.
[17] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.
[18] H. Song, P. Shi, C. C. Lim, W. A. Zhang, and L. Yu, "Attack and estimator design for multi-sensor systems with undetectable adversary," *Automatica*, vol. 109, Dec. 2019, Art. no. 108545.
[19] N. Cao, P. Liu, G. Li, C. Zhang, S. Cao, G. Cao, M. Yan, and B. B. Gupta, "Evaluation models for the nearest closer routing protocol in wireless sensor networks," *IEEE Access*, vol. 6, pp. 77043–77054, 2018.
[20] L. Zhao, Y. Li, Y. Yuan, and H. Yuan, "Optimal power allocation for multiple DoS attackers in wireless networked control systems," *ISA Trans.*, vol. 104, pp. 204–211, Sep. 2020.
[21] X. Cao, C. Sun, "Probabilistic denial of service attack against remote state estimation over a Markov channel in cyber-physical systems," in *Proc. 11th Asian Control Conf. (ASCC)*, 2017, pp. 946–951.
[22] Z. Ai, L. Peng, and M. Cao, "Optimal attack schedule for two sensors state estimation under jamming attack," *IEEE Access*, vol. 7, pp. 75741–75748, 2019.
[23] A. Ulusoy, A. Onat, O. Gurbuz, Wireless model based predictive networked control system, *IFAC Proc.*, vol. 42, no. 3, pp. 40–47, 2009.
[24] X. Su and C. T. Wen Wen, "High-order Extended Kalman Filter design for a class of complex dynamic systems with polynomial nonlinearities," *Chin. J. Electron.*, vol. 1, no. 1, pp. 1–8, 2021.
[25] Y. Chen, J. Ma, P. Zhang, F. Liu, and S. Mei, "Robust state estimator based on maximum exponential absolute value," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1537–1544, Jul. 2017.
[26] Y. Chen, F. Liu, S. Mei, and J. Ma, "A robust WLAV state estimation using optimal transformations," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 2190–2191, Jul. 2015.
[27] W. Wu, Y. Guo, B. Zhang, A. Bose, and S. Hongbin, "Robust state estimation method based on maximum exponential square," *IET Generat., Transmiss. Distrib.*, vol. 5, no. 11, pp. 1165–1172, Nov. 2011.
[28] Q. S. Jia, L. Shi, Y. Mo, B. Sinopoli, "On optimal partial broadcasting of wireless sensor networks for Kalman filtering," *IEEE Trans. Autom. Control*, vol. 57, no. 3, pp. 715–721, Aug. 2012.
[29] C. Wen, Z. Wang, Q. Liu, and F. E. Alsaadi, "Recursive distributed filtering for a class of state-saturated systems with fading measurements and quantization effects," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 6, pp. 930–941, Jun. 2018.
[30] L. Peng, X. Cao, C. Sun, Y. Cheng, and S. Jin, "Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems," *Neurocomputing*, vol. 272, pp. 571–583, Jan. 2018.
[31] L. Wu, S. Su, and J. Yan, "Optimal jamming attack scheduling of interactive channels," *IEEE Access*, vol. 8, pp. 95540–95546, 2020.
[32] J. Xu, C. Wen, and D. Xu, "Optimal control data scheduling with limited controller-plant communication," *Sci. China Inf. Sci.*, vol. 61, no. 1, Jan. 2018, Art. no. 012202.
[33] S. Ji, X. Xu, and C. Wen, "A kind of K—Nearest neighbor fault diagnosis method based on MIV data transformation," in *Proc. Chin. Automat. Congr.*, 2017, pp. 6306–6310.
[34] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal Denial-of-Service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
[35] C. Wen, X. Cheng, D. Xu, and C. Wen, "Filter design based on characteristic functions for one class of multi-dimensional nonlinear non-Gaussian systems," *Automatica*, vol. 82, pp. 171–180, Aug. 2017.

LI YANG is currently pursuing the Ph.D. degree with the Cyberspace College, Hangzhou Dianzi University. His research interests include wireless sensor network security and cyber-physical system attack methods.

CHENGLIN WEN received the Ph.D. degree in control science and engineering from Tsinghua University. He is currently pursuing the Ph.D. degree in control theory and control engineering with Northwestern Polytechnical University. He is also a Visiting Professor with Hong Kong Baptist University. He is also a Visiting Professor with Kent University, U.K. His main research interests include multi-source information fusion and target detection and identification and tracking, fault diagnosis and health management, complex engineering system safety assessment, and safe operation theory and methods.