Non-Fragile Set-Membership Filtering for Networked Systems under Protocol Scheduling and Hybrid Attacks

Chaoqun Zhu, Xiaolan Zhu, Bin Yang, and Pan Zhang

Institute of College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou, 730050, China (e-mail: chaoqunzhu@yeah.net).

Abstract: This paper investigates the non-fragile set-membership filtering problem for a class of discrete time-varying networked systems with protocol scheduling and hybrid cyber attacks. Firstly, Weighted Try-Once-Discard (WTOD) and Stochastic Communication (SC) protocols are utilized to allocate limited communication resources for the sensors of networked systems, and then two independent stochastic variables that follow Bernoulli distribution are introduced to characterize the replay attacks and deception attacks, respectively. Secondly, a non-fragile set-membership filter is provided by considering the impact of filtering gain perturbation on system performance. Sufficient conditions are derived in term of mathematical induction to ensure that the filtering error can be constrained within the ellipsoidal domain, and the minimum ellipsoidal domain in the sense of matrix trace is obtained by solving two optimization problems. Finally, the effectiveness of the proposed non-fragile set-membership filtering algorithm is demonstrated through two simulation examples.

Keywords: Networked control systems, non-fragile set-membership filter, communication protocols, hybrid cyber attacks

1. INTRODUCTION

Networked Control Systems (NCSs) are closed-loop control systems composed of sensors, controllers, and actuators interconnected through real-time networks. NCSs provide many advantages, such as flexibility, ease of installation, and cost savings, and they have found successful applications in a wide range of areas including power, chemical, manufacturing, and other key infrastructure areas, see, e.g., (Ge et al., 2019; Rahmanpour and Esfanjani, 2019; Fort et al., 2017; Cuong et al., 2018) and references therein. Due to the increasing of NCSs' scale and complexity, it is difficult to directly obtain the internal state of networked systems. Therefore, there are urgent needs to estimate the systems' state, which has significantly propelled the development of filtering theory concerning the NCSs. Currently, there have been generally three types filtering methods that are frequently used in addressing the problem of state estimation, i.e., Kalman filtering (Stojanovic and Nedic, 2016; Chen et al., 2021; Wang et al., 2021), H_∞ filtering (Shen et al., 2019; Chen et al., 2021), and H_2 filtering technology (Lee and Huang, 2008; Wang and Han, 2021). As we all know, Kalman filtering methods are effective for linear (or nonlinear) systems with Gaussian noise, while H_∞ filtering and H_2 filtering mothed are only applicable to dealing with so-called norm bounded noise. However, in most practical applications, it is impossible to know the probability and statistical properties of the system noise, and only the bounds of the noise can be obtained. In such a situation, the set-membership filtering technology has been proposed, which can effectively handle unknown but bounded (UBB) noise, and provide an estimated set of the system state (Ge et al., 2017, Wei et al., 2016). The set-membership filtering can reduce the negative impact of measurement inaccuracy to a certain extent, and meet certain system requirements with lower sensor precision. In recent years, the issue of set-membership filtering for networked systems has garnered widespread attention (Zhang et al., 2020; Han et al., 2023). In (Zhang et al., 2020), the set-membership filtering problem is discussed for networked systems with UBB noise, and a global ellipsoidal estimation method is provided. In (Han et al., 2023), the design problem of set-membership filtering algorithm is investigated for a class of time-varying networked systems under incomplete measurements and Round-Robin (RR) scheduling protocol. In the aforementioned research on set-membership filtering method, it is usually assumed that the designed filters can be fully implemented. However, in most practical applications, this assumption often does not hold. Due to the effects of rounding errors and finite word length during the process of numerical computation, there may be fluctuations in filtering parameters, which is referred to as the non-fragility of the filter. Even if the error of filtering gains is relatively small, it still can lead to the degradation of filtering performance. For this reason, it is more practically significant to take into full account the non-fragility when designing a set-membership filtering algorithm.

Due to the limited bandwidth of communication network, when all sensor nodes attempt to transmit information simultaneously, it may lead to channel congestion, and potentially cause that partial data packets are incomplete or even lost entirely. Therefore, in order to fully use of communication resources, various scheduling protocols have been introduced to guarantee that network nodes transmit information in an orderly manner. Up to data, popular communication protocols could be generally classified into three categories, namely, Round-Robin (RR) protocol, Weighted Try-Once-Discard (WTOD) protocol, and Stochastic Communication (SC) protocol. Among them, the RR protocol is a class of communication protocol that allocates the network access right in a recycling mode. The WTOD protocol is a kind of dynamic scheduling protocol that determines which node requires data transmission based on the difference between the last data sent by the communication network and the current data. While the SC protocol is a type of stochastic scheduling protocol, where communication nodes can choose whether to access the network at any time. The introduction of communication protocols brings great challenges to the dynamic analysis and synthesis of NCSs. Accordingly, the filtering problem of NCSs under communication protocols has attracted the considerable attention. In (Chen et al., 2020), a distributed set-membership filtering algorithm is proposed for the nonlinear systems with UBB noise under the condition of both RR scheduling protocol and SC scheduling protocol. The set-membership filtering problem is investigated in (Li et al., 2018) for a class of time-varying state-saturated systems with mixed time delays and the WTOD protocol. However, these available results only address the design problem of filtering algorithms under various communication scheduling protocols, but ignore the impact of malicious cyber attacks in an open network environment.

On the other hand, due to the openness and sharing characteristic of communication networks, NCSs are more susceptible to external malicious attacks, which may lead to a significant degradation in system performance even causing system instability. As a result, the issue of cyber security has recently attracted considerable research attention in the control community. For example, a distributed secure set-membership filtering algorithm is developed for a class of time-varying sensor networks subject to replay attacks and bandwidth limitations in (Liu et al., 2020b). For the two-dimensional uncertain systems with redundant channels in an insecure network environment, a set-membership filtering algorithm has been proposed by taking into account the randomly occurring deception attacks in (Li and Liang, 2023). A distributed filter scheduled by the RR protocol is designed in (Liu et al., 2020a) to ensure the security performance of networked systems under bounded disturbances and deception attacks. In the aforementioned results, the focus has been primarily on secure filtering design under specific types of cyber attacks. However, in order to ensure the success rate of cyber attacks and increase their destructive power, attackers often combine multiple different types of single attack to launch the so-called hybrid cyber attacks in the practical application of NCSs. Hybrid cyber attacks, due to their diverse attack modes and complex spatiotemporal interaction characteristics, pose great challenges to system stability analysis and control synthesis, and have attracted much research interest. For example, the design problem of recursive resilient filter is discussed for discrete-time nonlinear dynamic networks subject to randomly switching topologies and DoS attacks as well as deception attacks in (Ding et al., 2022). The set-membership filtering algorithms is developed in (Qu and Pang, 2020) for delayed artificial neural networks under DoS attacks and deception attacks. Although the aforementioned literature has some achievements in the filtering design of networked systems under the influence of cyber attacks, there are still some interesting problems that deserve further research.

In response to the aforementioned discussion, we aim to explore the non-fragile set-membership filtering problem for the networked systems under hybrid cyber attacks. More specifically, the objective of this paper is to design the non-fragile set-membership filter for the NCSs with hybrid cyber attacks and scheduling protocol whose sensors access the network governed by WTOD and SC protocols to guarantee the filtering error within the ellipsoidal domain. The main contributions of this paper can be summarized as follows.

(1) The comprehensive integration of the non-fragile set-membership filter design and hybrid cyber attacks is investigated for the networked systems.

(2) The WTOD scheduling protocol and SC scheduling protocol characterized by Markov stochastic process has been allowed to occur with hybrid cyber attacks, simultaneously, in the framework of non-fragile set-membership filter design.

(3) The calculation procedure of set-membership filtering gain matrices is presented by employing mathematical induction, and the filtering error is minimized in term of the convex optimization method.

The rest of this paper is organized as follows. Section 2 describes the NCSs framework, and the models of communication scheduling protocols and hybrid cyber attacks. In Section 3, we solve the designing problem of the non-fragile set-membership filter. Numerical example is presented in Section 4 to show the effectiveness of our results. Finally, we give some concluding remarks and discuss future research directions in Section 5.

Notations: The following notations will be used throughout the paper. R^n and $R^{m\times n}$ denote the n-dimensional Euclidean space and the set of $m\times n$ real matrices, respectively. $\mathbb{N}^+$ denotes the set of nonnegative integers. $P>0$ (≥ 0) means that P is real symmetric and positive definite (semi-definite). $\mathrm{E}(v)$ stands for the mathematical expectation of the stochastic variable v, and $\Pr(\kappa)$ means the occurrence probability of the event κ. X^T and X^{-1} represent the transpose and the inverse of matrix X, and $\mathrm{tr}(X)$ denotes the trace of the matrix X. $\{X_i\}_{i=1}^N$ denotes the set of the matrix X_1, $X_2, \cdots, X_N$.

2. PROBLEM FORMULATION

The structure diagram of the set-membership filtering problem for networked systems subjected to communication scheduling protocols and hybrid cyber attacks is depicted in Figure 1. The discrete time-varying nonlinear systems considered in this paper can be described as

$$\begin{cases} x_{k+1} = A_k x_k + B_k f(x_k) + D_k \omega_k \\ y_k = C_k x_k + v_k \end{cases}, \tag{1}$$

where $x_k \in R^n$ is the system state, $y_k \in R^m$ is the measurement output. A_k, B_k, C_k and D_k are known time-varying matrices with appropriate dimensions. $\omega_k \in R^r$ and $v_k \in R^m$ are the UUB system noise and measurement noise, respectively, which satisfy the following given ellipsoidal set constraints:

$$\begin{cases} W_k = \{\omega_k : \omega_k^T S_k^{-1} \omega_k \le 1\} \\ V_k = \{v_k : v_k^T R_k^{-1} v_k \le 1\} \end{cases}, \tag{2}$$

where $S_k > 0$ and $R_k > 0$ are known positive definite matrices with appropriate dimensions.

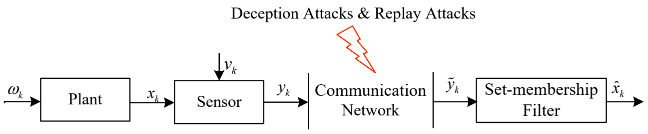

Fig. 1. NCSs architecture under protocol scheduling and hybrid attacks.

The nonlinear function $f(x_k)$ satisfies the following boundedness condition:

$$f^T(x_k) f(x_k) \le x_k^T M^T M x_k , \tag{3}$$

where M is a known real matrix with appropriate dimension.

2.1 Communication Protocol

In networked filtering systems with a large number of sensors, the scenario of freely exchanging measured information from the sensors to the filter can only be realized in an ideal network environment. In engineering practice, the limited bandwidth of communication network often leads to information conflicts or transmission congestion. In light of this, it is necessary to design effective communication strategies to schedule the limited communication resources according to certain scheduling protocols. Without loss of generality, it is assumed that only one sensor could be allowed to access the network channel to transmit information at one sampling period. Let $\xi_k \in \{1,2,\ldots,m\}$ denote the sensor that gains access to the communication network and transmits data to the filter at time instant k. Then, the value of ξ_k will be determined by the communication scheduling protocol with the specific rules as follows.

(1) WTOD Protocol

The WTOD protocol is a typical dynamic scheduling protocol that determines which sensor requires transmission data based on the difference between the last data sent by the communication node and the current data. Under the WTOD protocol, the value of ξ_k can be determined according to the following rules:

$$\xi_k \triangleq \arg\max_{1\le i\le N} (y_{i,k} - \hat{y}_{i,k})^T Q_i (y_{i,k} - \hat{y}_{i,k}) , \tag{4}$$

where $\hat{y}_{i,k}$ represents the most recent signal sent by sensor i before time instant k, and Q_i $(i \in \{1,2,\ldots,m\})$ is a known positive definite matrix that represents the weight matrix for the i-th sensor. Then, we define y_k, $\hat{y}_k$ and $\bar{Q}$ as

$$\begin{cases} y_k = \begin{bmatrix} y_{1,k}^T & y_{2,k}^T & \cdots & y_{m,k}^T \end{bmatrix}^T \\ \hat{y}_k = \begin{bmatrix} \hat{y}_{1,k}^T & \hat{y}_{2,k}^T & \cdots & \hat{y}_{m,k}^T \end{bmatrix}^T \end{cases}, \ \bar{Q} = diag\{Q_1, Q_2, \ldots, Q_m\} .$$

Correspondingly, the value of ξ_k can be redefined as follows:

$$\xi_k \triangleq \arg\max_{1\le i\le N} (y_k - \hat{y}_k)^T \bar{Q}_i (y_k - \hat{y}_k) , \tag{5}$$

where $\bar{Q}_i = \bar{Q}\Phi_i$, $\Phi_i = diag\{\delta(i-1)I, \delta(i-2)I, \ldots, \delta(i-m)I\}$.

(2) SC Protocol

The SC protocol is characterized by the fact that all of the sensors can choose whether they need to access the network at any time. Under the SC protocol, $\xi_k \in \{1,2,\ldots,m\}$ is a stochastic variable that obeys a Markov stochastic distribution with the following conditional probability:

$$\Pr\{\xi_k = i\} = \pi_i(k), \ \Pr\{\xi_{k+1} = j \mid \xi_k = i\} = \pi_{ij}(k) \ ,$$

where $\pi_i(k)$ represents the probability that the i-th sensor gains access to the communication network at time instant k. $\pi_{ij}(k) > 0$ represents the transition probability that from the sensor i gaining access to the communication network at time instant k to the sensor j gaining access to the communication network at time instant $k+1$, and it is satisfied that $\sum_{j=1}^{m} \pi_{ij}(k) = 1$.

We could represent the measurement output of the sensors after network transmission as

$$\bar{y}_k = \begin{bmatrix} \bar{y}_{1,k}^T & \bar{y}_{2,k}^T & \cdots & \bar{y}_{N,k}^T \end{bmatrix}^T . \tag{6}$$

It is assumed the initial state of $\bar{y}_k$ is taken as $\bar{y}_j = \varphi_0 (j < 0)$, where φ_0 is a known vector. Then, the update rule for $\bar{y}_{i,k}$ $(k \in \mathbb{N}^+, i \in \{1,2,\ldots m\})$ can be expressed as

$$\bar{y}_{i,k} = \begin{cases} y_{i,k} & if \ i = \xi_k \\ \bar{y}_{i,k-1} & \text{otherwise} \end{cases} . \tag{7}$$

According to the update rule (7) of the measurement output, one has

$$\begin{cases} \bar{y}_k = \Phi_{\xi_k} y_k + (I - \Phi_{\xi_k}) \bar{y}_{k-1} \\ \bar{y}_j = \varphi_0 , \ \ j < 0 \end{cases} . \tag{8}$$

2.2 Deception Attacks and Replay Attacks

Due to the openness of communication network, NCSs are more susceptible to malicious attacks, which may lead to data loss or tampering, and seriously affect the filtering performance of networked systems. Therefore, it is necessary to investigate the characteristics of cyber attacks and model them for better addressing the issue of security filtering. In this paper, we consider the scenario that the networked systems are subject to deception attacks and replay attacks, simultaneously.

Two mutually independent and identically distributed random variables $\alpha_k \in \{0,1\}$ and $\beta_k \in \{0,1\}$ are employed to describe whether the deception attacks and replay attacks occur or not, respectively. The probability distributions of random variables α_k and β_k satisfy the following conditions:

$$\Pr\{\alpha_k = 1\} = \bar{\alpha}\,,\ \Pr\{\alpha_k = 0\} = 1-\bar{\alpha}\,,$$

$$\Pr\{\beta_k = 1\} = \bar{\beta}\,,\ \Pr\{\beta_k = 0\} = 1-\bar{\beta}\,. \tag{9}$$

Then, the measurement output impacted by the hybrid cyber attacks can be described as follows:

$$\tilde{y}_k = \beta_k \bar{y}_{k-\tau_k} + (1-\beta_k)\vec{y}_k \tag{10}$$

where $\tilde{y}_k$ represents the measurement signal suffered the hybrid cyber attacks. τ_k satisfy the condition $0 < \tau_m \le \tau_k \le \tau_M$, where τ_m and τ_M are the known upper and lower bounds of the replay delay, respectively. $\vec{y}_k$ is the measurement signal affected by deception attack, which can be represented as

$$\vec{y}_k = \alpha_k \delta_k + (1-\alpha_k)\bar{y}_k\,, \tag{11}$$

where δ_k represents the false signal injected by the attacker, which satisfies the following given ellipsoidal constraints:

$$\mathrm{E}\{\delta_k^T \Theta_k^{-1} \delta_k\} \le 1\,, \tag{12}$$

where $\Theta_k > 0$ is a known positive definite matrix.

Remark 1. When $\beta_k = 1$, it indicates that the networked system is subject to replay attacks, and the filter receives the measurement data as $\tilde{y}_k = \beta_k \bar{y}_{k-\tau_k}$. When $\beta_k = 0$ and $\alpha_k = 1$, it indicates that the networked system is subject to deception attacks, and the filter receives the measurement data as $\vec{y}_k = \tilde{y}_k$. When $\beta_k = 0$ and $\alpha_k = 0$, it indicates that the networked system is free from any cyber attacks, and the filter receives the system's normal measurement data as $\tilde{y}_k = \bar{y}_k$.

2.3 Model Description

Considering the discrete time-varying nonlinear system (1) with various communication protocols and hybrid cyber attacks, we define the augmented state variable as $\tilde{x}_k = \begin{bmatrix} x_k^T & \bar{y}_{k-1}^T \end{bmatrix}^T$. By combining (1), (5), (8), (10) and (11), the following augmented system model can be obtained:

$$\begin{cases} \tilde{x}_{k+1} = \tilde{A}_k \tilde{x}_k + \tilde{B}_{0k}\tilde{x}_{k-d} + \tilde{B}_{1k}\tilde{f}(\tilde{x}_k) + \tilde{D}_k \tilde{\omega}_k \\ \tilde{y}_k = \tilde{C}_k \tilde{x}_k + \tilde{C}_{1k}\tilde{x}_{k-d} + \tilde{D}_{1k}\tilde{v}_k + \tilde{E}_k \tilde{\delta}_k \end{cases}, \tag{13}$$

where $\tilde{A}_k = \begin{bmatrix} A_k & 0 \\ (1-\alpha_k)(1-\beta_k)\Phi_{\xi_k} C_k & (1-\alpha_k)(1-\beta_k)(I-\Phi_{\xi_k}) \end{bmatrix}$

$=\tilde{A}_{0k} + \varsigma_1 \tilde{A}_{1k} + \varsigma_2 \tilde{A}_{2k} + \varsigma_3 \tilde{A}_{3k}$, $\tilde{A}_{0k} = \begin{bmatrix} A_k & 0 \\ \varsigma_5 \Phi_{\xi_k} C_k & \varsigma_5 (I-\Phi_{\xi_k}) \end{bmatrix}$,

$\tilde{A}_{1k} = \begin{bmatrix} 0 & 0 \\ \Phi_{\xi_k} C_k & (I-\Phi_{\xi_k}) \end{bmatrix}$, $\tilde{A}_{2k} = \begin{bmatrix} 0 & 0 \\ \Phi_{\xi_k} C_k & (I-\Phi_{\xi_k}) \end{bmatrix}$,

$\tilde{A}_{3k} = \begin{bmatrix} 0 & 0 \\ \Phi_{\xi_k} C_k & (I-\Phi_{\xi_k}) \end{bmatrix}$, $\tilde{B}_{0k} = \begin{bmatrix} 0 & 0 \\ \beta_k & 0 \end{bmatrix} = \tilde{B}_{2k} - \varsigma_1 \tilde{B}_{3k}$,

$\tilde{B}_{2k} = \begin{bmatrix} 0 & 0 \\ \bar{\beta} & 0 \end{bmatrix}$, $\tilde{B}_{3k} = \begin{bmatrix} 0 & 0 \\ -I & 0 \end{bmatrix}$, $\tilde{B}_{1k} = \begin{bmatrix} B_k & 0 \\ 0 & 0 \end{bmatrix}$, $\tilde{D}_k = \begin{bmatrix} D_k & 0 \\ 0 & 0 \end{bmatrix}$,

$\tilde{C}_{0k} = \begin{bmatrix} \varsigma_5 \Phi_{\xi_k} C_k & \varsigma_5 (I-\Phi_{\xi_k}) \end{bmatrix}$, $\tilde{C}_{2k} = \begin{bmatrix} \Phi_{\xi_k} C_k & I-\Phi_{\xi_k} \end{bmatrix}$,

$\tilde{C}_k = \begin{bmatrix} (1-\alpha_k)(1-\beta_k)\Phi_{\xi_k} C_k & (1-\alpha_k)(1-\beta_k)(I-\Phi_{\xi_k}) \end{bmatrix}$

$= \tilde{C}_{0k} + \varsigma_1 \tilde{C}_{2k} + \varsigma_2 \tilde{C}_{3k} + \varsigma_3 \tilde{C}_{4k}$

$\tilde{C}_{3k} = \begin{bmatrix} \Phi_{\xi_k} C_k & I-\Phi_{\xi_k} \end{bmatrix}$, $\tilde{C}_{4k} = \begin{bmatrix} \Phi_{\xi_k} C_k & I-\Phi_{\xi_k} \end{bmatrix}$,

$\tilde{C}_{1k} = \begin{bmatrix} \beta_k & 0 \end{bmatrix} = \tilde{C}_{5k} - \varsigma_1 \tilde{C}_{6k}$, $\tilde{C}_{5k} = \begin{bmatrix} \bar{\beta} & 0 \end{bmatrix}$, $\tilde{C}_{6k} = \begin{bmatrix} -I & 0 \end{bmatrix}$,

$\tilde{D}_{1k} = \begin{bmatrix} (1-\alpha_k)(1-\beta_k)\Phi_{\xi_k} & 0 \end{bmatrix} = \tilde{D}_{2k} + \varsigma_1 \tilde{D}_{3k} + \varsigma_2 \tilde{D}_{4k} + \varsigma_3 \tilde{D}_{5k}$,

$\tilde{D}_{2k} = \begin{bmatrix} \varsigma_5 \Phi_{\xi_k} & 0 \end{bmatrix}$, $\tilde{D}_{3k} = \begin{bmatrix} \Phi_{\xi_k} & 0 \end{bmatrix}$, $\tilde{D}_{4k} = \begin{bmatrix} \Phi_{\xi_k} & 0 \end{bmatrix}$, $\tilde{D}_{5k} = \begin{bmatrix} \Phi_{\xi_k} & 0 \end{bmatrix}$,

$\tilde{E}_k = \begin{bmatrix} \alpha_k (1-\beta_k) I & 0 \end{bmatrix} = \tilde{E}_{1k} - \varsigma_2 \tilde{E}_{2k} - \varsigma_3 \tilde{E}_{3k}$, $\tilde{E}_{1k} = \begin{bmatrix} \varsigma_4 I & 0 \end{bmatrix}$,

$\tilde{E}_{2k} = \begin{bmatrix} I & 0 \end{bmatrix}$, $\tilde{E}_{3k} = \begin{bmatrix} I & 0 \end{bmatrix}$, $\varsigma_1 = (\bar{\beta} - \beta_k)$, $\varsigma_2 = (\bar{\alpha} - \alpha_k)$,

$\varsigma_3 = (\alpha_k \beta_k - \bar{\alpha}\bar{\beta})$, $\varsigma_4 = (\bar{\alpha} - \bar{\alpha}\bar{\beta})$, $\varsigma_5 = (1 - \bar{\beta} - \bar{\alpha} + \bar{\alpha}\bar{\beta})$.

Based on the augmented system (13), a non-fragile set-membership filter is constructed with the following structure:

$$\hat{x}_{k+1} = \tilde{A}_k \hat{x}_k + \tilde{B}_{0k}\hat{x}_{k-d} + \tilde{B}_{1k}\tilde{f}(\hat{x}_k) + (\hat{L}_k + \Delta\hat{L}_k)(\tilde{y}_k - \tilde{C}_k \hat{x}_k)\,, \tag{14}$$

where $\hat{x}_k$ is the estimated value of the system state $\tilde{x}_k$. $\hat{L}_k$ is the filtering gain matrix to be determined. $\Delta\hat{L}_k$ is an unknown gain perturbation that satisfies the following norm-bounded uncertainty:

$$\Delta\hat{L}_k = \hat{M}\hat{F}_k \hat{N}\,, \tag{15}$$

where $\hat{M}$ and $\hat{N}$ are known real matrices, and the unknown time-varying matrix $\hat{F}_k$ satisfies the condition $\hat{F}_k^T \hat{F}_k \le I$.

Define the filtering error as $e_k = \tilde{x}_k - \hat{x}_k$. By considering (13) and (14), the filtering error system can be given as follows:

$$\begin{aligned}
e_{k+1} &= \tilde{x}_{k+1} - \hat{x}_{k+1} \\
&= \tilde{A}_k \tilde{x}_k + \tilde{B}_{0k}\tilde{x}_{k-d} + \tilde{B}_{1k}\tilde{f}(\tilde{x}_k) + \tilde{D}_k \tilde{\omega}_k - (\tilde{A}_k \hat{x}_k + \tilde{B}_{0k}\hat{x}_{k-d} + \tilde{B}_{1k}\tilde{f}(\hat{x}_k) \\
&\quad + (\hat{L}_k + \Delta\hat{L}_k)(\tilde{y}_k - \tilde{C}_k \hat{x}_k)) \\
&= \tilde{A}_k \tilde{x}_k + \tilde{B}_{0k}\tilde{x}_{k-d} + \tilde{B}_{1k}\tilde{f}(\tilde{x}_k) + \tilde{D}_k \tilde{\omega}_k - \tilde{A}_k \hat{x}_k - \tilde{B}_{0k}\hat{x}_{k-d} - \tilde{B}_{1k}\tilde{f}(\hat{x}_k) \\
&\quad - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_k \tilde{x}_k - (\hat{L}_k + \Delta\hat{L}_k)\tilde{D}_{1k}\tilde{v}_k \\
&\quad - (\hat{L}_k + \Delta\hat{L}_k)\tilde{E}_k \tilde{\delta}_k + (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_k \hat{x}_k \\
&= (\tilde{A}_k - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_k)\tilde{x}_k - (\tilde{A}_k - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_k)\hat{x}_k + \tilde{B}_{0k}\tilde{x}_{k-d} \\
&\quad + \tilde{B}_{1k}\tilde{f}(\tilde{x}_k) + \tilde{D}_k \tilde{\omega}_k - \tilde{B}_{0k}\hat{x}_{k-d} - \tilde{B}_{1k}\tilde{f}(\hat{x}_k)
\end{aligned}$$

$$-(\hat{L}_k+\Delta\hat{L}_k)\tilde{D}_{1k}\tilde{v}_k-(\hat{L}_k+\Delta\hat{L}_k)\tilde{E}_k\tilde{\delta}_k$$
$$=(\tilde{A}_k-(\hat{L}_k+\Delta\hat{L}_k)\tilde{C}_k)e_k+\tilde{B}_{0k}e_{k-d}+\tilde{B}_{1k}\tilde{f}(e_k)+\tilde{D}_k\tilde{\omega}_k$$
$$-(\hat{L}_k+\Delta\hat{L}_k)\tilde{D}_{1k}\tilde{v}_k-(\hat{L}_k+\Delta\hat{L}_k)\tilde{E}_k\tilde{\delta}_k, \tag{16}$$

where $\tilde{f}(e_k)=\tilde{f}(\tilde{x}_k)-\tilde{f}(\hat{x}_k)$.

Additionally, in order to accelerate the presentation of subsequent results, the several statistical properties regarding the hybrid cyber-attacks are given as follows:

$$\mathrm{E}\left\{(\alpha_k-\bar{\alpha})^2\right\}=\bar{\alpha}(1-\bar{\alpha}),\ \mathrm{E}\left\{(\beta_k-\bar{\beta})^2\right\}=\bar{\beta}(1-\bar{\beta}).$$

3. MAIN RESULTS

The research objective of this paper is to address the design issue of a non-fragile set-membership filter for the discrete time-varying nonlinear system (13) subject to hybrid cyber attacks and the influence of the WTOD protocol as well as the SC protocol. Specifically, we will start by defining a set of positive definite matrices P_{k+1} such that the filtering error e_{k+1} satisfies the P_{k+1}-dependent ellipsoidal constraint. Then, the optimal filtering gain matrix can be solved by minimizing the trace of matrix P_{k+1}. Before proceeding further, we introduce the following definition, assumption, and lemmas.

Definition 1: For the discrete time-varying nonlinear system (13) and the set-membership filter (14), given a set of ellipsoidal constraint matrices $P_k\in R^{n\times n}$ $(k\in\mathrm{N}^+)$, if the inequality

$$e_k^TP_k^{-1}e_k\le 1 \tag{17}$$

holds for all $k\in\mathbb{N}^+$, the filtering error e_k satisfy the P_k-dependent ellipsoidal constraint.

Remark 2. The constraint condition (17) $e_k^TP_k^{-1}e_k\le 1$ involves the nonlinear characteristic of networked systems. The nonlinear constraint produces complex interactions in the optimization process, which makes P_k fail to optimize to the ideal value, that is, the actual P_k after optimization is greater than the ideal P_k. As a result, the bound 1 imposed on constraint condition (17) is satisfied with a lot of slack under the premise condition of greater P_k.

Assumption 1: The initial condition $\tilde{x}_0=\varphi_0$ satisfy

$$\varphi_0^TP_0^{-1}\varphi_0\le 1, \tag{18}$$

where P_0 is a known positive definite matrix.

Lemma 1. (Boyd et al., 1994) Let $\phi_0(\cdot)$, $\phi_1(\cdot)$, …, $\phi_p(\cdot)$ be quadratic functions of the variable $\varsigma\in\mathbb{R}^n$: $\phi_i(\cdot)\triangleq\varsigma^TT_i\varsigma$ (i=0, 1, ⋯, p) with $T_i^T=T_i$. If there exist $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_p\ge 0$, such that

$$T_0-\sum_{i=1}^{p}\alpha_iT_i\le 0, \tag{19}$$

then the following inequalities hold

$$\phi_1(\varsigma)\le 0,\ \phi_2(\varsigma)\le 0,\ldots,\ \phi_p(\varsigma)\le 0\Rightarrow\phi_0(\varsigma)\le 0. \tag{20}$$

Lemma 2. (Petersen and Hollot, 1986) For the appropriate dimension matrices M, N and F_k satisfying $F_k^TF_k\le I$, the following inequality holds for any scalar $\varepsilon>0$

$$MF_kN+N^TF_k^TM^T\le\varepsilon^{-1}MM^T+\varepsilon N^TN. \tag{21}$$

3.1 Design of Non-fragile Set-Membership Filter

3.1.1 Non-fragile set-membership filter under the WTOD protocol

Theorem 1: For the system (1) with the WTOD protocol (5) and hybrid cyber attacks (10), let the sequence of constraint matrices $P_k>0$ $(k\in\mathbb{N}^+)$ be given, and the filtering error e_k satisfy $e_k^TP_k^{-1}e_k\le 1$. If there exist matrices $P_{k+1}>0$, filtering gain matrices $\hat{L}_k$ and positive scalars ε_j $(j\in\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\})$, the following matrix inequality holds

$$\begin{bmatrix} -\Theta_k & \hat{\Omega} & \hat{M}_1 & 0 & \hat{M}_2 & 0 & \hat{M}_3 & 0 \\ * & -P & 0 & \varepsilon_7\hat{N}_1^T & 0 & \varepsilon_8\hat{N}_2^T & 0 & \varepsilon_9\hat{N}_3^T \\ * & * & -\varepsilon_7 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -\varepsilon_7 & 0 & 0 & 0 & 0 \\ * & * & * & * & -\varepsilon_8 & 0 & 0 & 0 \\ * & * & * & * & * & -\varepsilon_8 & 0 & 0 \\ * & * & * & * & * & * & -\varepsilon_9 & 0 \\ * & * & * & * & * & * & * & -\varepsilon_9 \end{bmatrix}\le 0, \tag{22}$$

where

$$\Theta_k=diag\left\{1-\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4-\varepsilon_5-\varepsilon_6,\varepsilon_1I,\varepsilon_2I,0,\varepsilon_4S^{-1},\varepsilon_5R^{-1},\varepsilon_1Q^{-1}\right\}$$
$$+\Gamma_k^T\sum_{i=1}^{N}\lambda_{ik}(\bar{Q}(\Phi_i-\Phi_{\xi_k}))\Gamma_k+\varepsilon_3\Xi_1,$$

$$\Xi_1=diag\left\{0,H_k^TM_1^TMH_k,0,I,0,0,0\right\},$$

$$\hat{\Omega}=\begin{bmatrix}\hat{\Omega}_{1k}^T & \sqrt{\bar{\varsigma}_1}\hat{\Omega}_{2k}^T & \sqrt{\bar{\varsigma}_2}\hat{\Omega}_{3k}^T & \sqrt{\bar{\varsigma}_3}\hat{\Omega}_{4k}^T\end{bmatrix},$$

$$\hat{\Omega}_{1k}=\begin{bmatrix}0 & (\tilde{A}_{0k}-\hat{L}_k\tilde{C}_{0k})H_k & \tilde{B}_{2k}H_{k-d} & \tilde{B}_{1k} & \tilde{D}_k & -\hat{L}_k\tilde{D}_{2k} & -\hat{L}_k\tilde{E}_{1k}\end{bmatrix},$$

$$P=diag\left\{P_{k+1}\quad P_{k+1}\quad P_{k+1}\quad P_{k+1}\right\},\hat{M}_1=\begin{bmatrix}0 & \hat{M} & 0 & 0 & 0 & 0 & 0\end{bmatrix}^T,$$

$$\hat{\Omega}_{2k}=\begin{bmatrix}0 & (\tilde{A}_{1k}-\hat{L}_k\tilde{C}_{2k})H_k & \tilde{B}_{3k}H_{k-d} & 0 & 0 & \hat{L}_k\tilde{D}_{3k} & 0\end{bmatrix},$$

$$\hat{\Omega}_{3k}=\begin{bmatrix}0 & (\tilde{A}_{2k}-\hat{L}_k\tilde{C}_{3k})H_k & 0 & 0 & 0 & -\hat{L}_k\tilde{D}_{4k} & \hat{L}_k\tilde{E}_{2k}\end{bmatrix},$$

$$\hat{M}_2=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & \hat{M} & 0\end{bmatrix}^T,\hat{M}_3=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & \hat{M}\end{bmatrix}^T,$$

$$\hat{\Omega}_{4k}=\begin{bmatrix}0 & (\tilde{A}_{3k}-\hat{L}_k\tilde{C}_{4k})H_k & 0 & 0 & 0 & -\hat{L}_k\tilde{D}_{5k} & \hat{L}_k\tilde{E}_{3k}\end{bmatrix},$$

$\hat{N}_1 = \left[\hat{N}\tilde{C}_{0k}H_k \quad \sqrt{\varsigma_1}\hat{N}\tilde{C}_{2k}H_k \quad \sqrt{\varsigma_2}\hat{N}\tilde{C}_{3k}H_k \quad \sqrt{\varsigma_3}\hat{N}\tilde{C}_{4k}H_k\right]$,

$\bar{\varsigma}_1 = \bar{\beta}(1-\bar{\beta})$, $\hat{N}_2 = \left[-\hat{N}\tilde{D}_{2k} \quad \sqrt{\bar{\varsigma}_1}\hat{N}\tilde{D}_{3k} \quad -\sqrt{\bar{\varsigma}_2}\hat{N}\tilde{D}_{4k} \quad -\sqrt{\bar{\varsigma}_3}\hat{N}\tilde{D}_{5k}\right]$,

$\bar{\varsigma}_2 = \bar{\alpha}(1-\bar{\alpha})$, $\hat{N}_3 = \left[-\hat{N}\tilde{E}_{1k} \quad 0 \quad \sqrt{\bar{\varsigma}_2}\hat{N}\tilde{E}_{2k} \quad \sqrt{\bar{\varsigma}_3}\hat{N}\tilde{E}_{3k}\right]$,

$\bar{\varsigma}_3 = \bar{\alpha}\bar{\beta}(1-\bar{\alpha}\bar{\beta})$.

Then, the filtering error e_{k+1} satisfies the ellipsoid constraint $e_{k+1}^T P_{k+1}^{-1} e_{k+1} \le 1$.

Proof: The mathematical induction is employed to prove this theorem. According to Assumption 1, the initial condition satisfy

$$\varphi_0^T P_0^{-1}\varphi_0 = e_0^T P_0^{-1} e_0 \le 1. \tag{23}$$

It is assumed that $e_k^T P_k^{-1} e_k \le 1$ holds for time instant k. Then, we aim to show that $e_{k+1}^T P_{k+1}^{-1} e_{k+1} \le 1$ holds at the time instant $k+1$. From (El and Calafiore, 2001), we know that there exists a vector Z_k satisfying $e_k = H_k Z_k$ with $\mathrm{E}\left\{Z_k^T Z_k\right\} \le 1$, where H_k is a factorization of $P_{k+1} = H_k H_k^T$, $k \in \mathbb{N}^+$.

For notational simplicity, we denote

$$\eta_k = \left[1 \quad Z_k^T \quad Z_{k-d}^T \quad \tilde{f}^T(e_k) \quad \tilde{\omega}_k^T \quad \tilde{v}_k^T \quad \tilde{\delta}_k^T\right]^T.$$

Then, the filtering error system (16) is equivalent to

$$e_{k+1} = \Omega\eta_k, \tag{24}$$

where $\Omega = \left[\Omega_{1k}^T \quad \varsigma_1\Omega_{2k}^T \quad \varsigma_2\Omega_{3k}^T \quad \varsigma_3\Omega_{4k}^T\right]$,

$$\Omega_{1k} = \left[0 \quad (\tilde{A}_{0k} - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_{0k})H_k \quad \tilde{B}_{2k}H_{k-d} \quad \tilde{B}_{1k} \quad \tilde{D}_k \quad -(\hat{L}_k + \Delta\hat{L}_k)\tilde{D}_{2k} \quad -(\hat{L}_k + \Delta\hat{L}_k)\tilde{E}_{1k}\right],$$

$$\Omega_{2k} = \left[0 \quad (\tilde{A}_{1k} - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_{2k})H_k \quad \tilde{B}_{3k}H_{k-d} \quad 0 \quad 0 \quad (\hat{L}_k + \Delta\hat{L}_k)\tilde{D}_{3k} \quad 0\right],$$

$$\Omega_{3k} = \left[0 \quad (\tilde{A}_{2k} - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_{3k})H_k \quad 0 \quad 0 \quad 0 \quad -(\hat{L}_k + \Delta\hat{L}_k)\tilde{D}_{4k} \quad (\hat{L}_k + \Delta\hat{L}_k)\tilde{E}_{2k}\right],$$

$$\Omega_{4k} = \left[0 \quad (\tilde{A}_{3k} - (\hat{L}_k + \Delta\hat{L}_k)\tilde{C}_{4k})H_k \quad 0 \quad 0 \quad 0 \quad -(\hat{L}_k + \Delta\hat{L}_k)\tilde{D}_{5k} \quad (\hat{L}_k + \Delta\hat{L}_k)\tilde{E}_{3k}\right].$$

From (24), we can obtain that

$$\begin{aligned}
&\mathrm{E}\left\{e_{k+1}^T P_{k+1}^{-1} e_{k+1}\right\} - 1 \\
&= \mathrm{E}\left\{\eta_k^T \Omega P_{k+1}^{-1}\Omega\eta_k\right\} - 1 \\
&= \mathrm{E}\left\{\eta_k^T(\Omega_{1k} + \varsigma_1\Omega_{2k} + \varsigma_2\Omega_{3k} + \varsigma_3\Omega_{4k})^T P_{k+1}^{-1}\right. \\
&\quad \left.\times(\Omega_{1k} + \varsigma_1\Omega_{2k} + \varsigma_2\Omega_{3k} + \varsigma_3\Omega_{4k})\eta_k\right\} - 1 \\
&= \eta_k^T\Omega_{1k}^T P_{k+1}^{-1}\Omega_{1k}\eta_k + \bar{\varsigma}_1\eta_k^T\Omega_{2k}^T P_{k+1}^{-1}\Omega_{2k}\eta_k + \bar{\varsigma}_2\eta_k^T\Omega_{3k}^T P_{k+1}^{-1}\Omega_{3k}\eta_k \\
&\quad + \bar{\varsigma}_3\eta_k^T\Omega_{4k}^T P_{k+1}^{-1}\Omega_{4k}\eta_k - 1 \\
&= \eta_k^T(\Omega_{1k}^T P_{k+1}^{-1}\Omega_{1k} + \bar{\varsigma}_1\Omega_{2k}^T P_{k+1}^{-1}\Omega_{2k} + \bar{\varsigma}_2\Omega_{3k}^T P_{k+1}^{-1}\Omega_{3k} \\
&\quad + \bar{\varsigma}_3\Omega_{4k}^T P_{k+1}^{-1}\Omega_{4k} - diag\left\{1,0,0,0,0,0,0\right\})\eta_k.
\end{aligned}$$

Based on (3), one has

$$\tilde{f}^T(e_k)\tilde{f}(e_k) - e_k^T M_1^T M_1 e_k \le 0. \tag{25}$$

Then, (25) can further be expressed as

$$\eta_k^T \Xi_1 \eta_k \le 0, \tag{26}$$

where $\Xi_1 = diag\left\{0,\ H_k^T M_1^T M H_k,\ 0,\ I,\ 0,\ 0,\ 0\right\}$.

From (2), Assumption 1 and the update rule of WTOD protocol (5), we can obtain

$$\begin{cases}
\mathrm{E}\left\{Z_k^T Z_k\right\} \le 1 \\
\mathrm{E}\left\{Z_{k-\tau}^T Z_{k-\tau}\right\} \le 1 \\
\omega_k^T S_k^{-1}\omega_k \le 1 \\
v_k^T R_k^{-1} v_k \le 1 \\
(y_k - \bar{y}_{k-1})^T \bar{Q}(\Phi_i - \Phi_{\xi_k})(y_k - \bar{y}_{k-1}) \le 0,\ i = 1,2,\ldots,m
\end{cases}. \tag{27}$$

Rearrange (26) and (27), which yields

$$\begin{cases}
\eta_k^T diag\left\{-1,I,0,0,0,0,0\right\}\eta_k \le 0 \\
\eta_k^T diag\left\{-1,0,I,0,0,0,0\right\}\eta_k \le 0 \\
\eta_k^T diag\left\{-1,0,0,0,S^{-1},0,0\right\}\eta_k \le 0 \\
\eta_k^T diag\left\{-1,0,0,0,0,R^{-1},0\right\}\eta_k \le 0 \\
\eta_k^T diag\left\{-1,0,0,0,0,0,Q^{-1}\right\}\eta_k \le 0 \\
\eta_k^T \Gamma_k^T \bar{Q}(\Phi_i - \Phi_{\xi_k})\Gamma_k\eta_k \le 0 \\
\eta_k^T diag\left\{0,H_k^T M_1^T M H_k,0,I,0,0,0\right\}\eta_k \le 0
\end{cases}. \tag{28}$$

According to Lemma 1, if there exist positive scalars ε_1, ε_2, ε_3, ε_4, ε_5 and ε_6, such that

$$\begin{aligned}
&\eta_k^T(\Omega^T P_{k+1}^{-1}\Omega - diag\left\{1,0,0,0,0,0,0\right\})\eta_k \\
&-\eta_k^T\Gamma_k^T\sum_{i=1}^{N}\lambda_{ik}(\bar{Q}(\Phi_i - \Phi_{\xi_k}))\Gamma_k\eta_k - \varepsilon_1\eta_k^T diag\left\{-1,I,0,0,0,0,0\right\}\eta_k \\
&-\varepsilon_2\eta_k^T diag\left\{-1,0,I,0,0,0,0\right\}\eta_k - \varepsilon_3\eta_k^T\Xi_1\eta_k - \varepsilon_4\eta_k^T diag\left\{-1,0,0,0,S^{-1},0,0\right\}\eta_k \\
&-\varepsilon_5\eta_k^T diag\left\{-1,0,0,0,0,R^{-1},0\right\}\eta_k - \varepsilon_6\eta_k^T diag\left\{-1,0,0,0,0,0,Q^{-1}\right\}\eta_k \le 0.
\end{aligned} \tag{29}$$

Accordingly, (29) can be rewritten as follows:

$$\Omega^T P_{k+1}^{-1}\Omega - diag\left\{1-\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4-\varepsilon_5-\varepsilon_6,\varepsilon_1 I,\varepsilon_2 I,0,\varepsilon_4 S^{-1},\varepsilon_5 R^{-1},\varepsilon_1 Q^{-1}\right\}$$

$$-\Gamma_k^T \sum_{i=1}^{N} \lambda_{ik} (\bar{Q}(\Phi_i - \Phi_{\xi_k}))\Gamma_k - \varepsilon_3 \Xi_1 \le 0 . \tag{30}$$

We denote that

$$\Theta(k) = diag\left\{1-\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4-\varepsilon_5-\varepsilon_6, \varepsilon_1 I, \varepsilon_2 I, 0, \varepsilon_4 S^{-1}, \varepsilon_5 R^{-1}, \varepsilon_1 Q^{-1}\right\}$$
$$+\Gamma_k^T \sum_{i=1}^{N} \lambda_{ik} (\bar{Q}(\Phi_i - \Phi_{\xi_k}))\Gamma_k + \varepsilon_3 \Xi_1 . \tag{31}$$

Then, (30) is equivalent to

$$\Omega^T P_{k+1}^{-1} \Omega - \Theta_k \le 0 . \tag{32}$$

Applying the Schur complement lemma to (32), it is obtained that

$$\begin{bmatrix} -\Theta_k & \Omega^T \\ * & -P \end{bmatrix} \le 0 . \tag{33}$$

Due to the presence of the matrix with parametric uncertainty, (33) can be decomposed into

$$\Upsilon_1 + \begin{bmatrix} 0 & \tilde{\Omega}^T \\ * & 0 \end{bmatrix} \le 0 , \tag{34}$$

where $\Upsilon_1 = \begin{bmatrix} -\Theta_k & \hat{\Omega}^T \\ * & -P \end{bmatrix}$, $\tilde{\Omega} = \begin{bmatrix} \tilde{\Omega}_{1k}^T & \sqrt{\varsigma_1}\tilde{\Omega}_{2k}^T & \sqrt{\varsigma_2}\tilde{\Omega}_{3k}^T & \sqrt{\varsigma_3}\tilde{\Omega}_{4k}^T \end{bmatrix}$,

$$\tilde{\Omega}_{1k} = \begin{bmatrix} 0 & \Delta\hat{L}_k \tilde{C}_{0k} H_k & \tilde{B}_{2k} H_{k-d} & \tilde{B}_{1k} & \tilde{D}_k & -\Delta\hat{L}_k \tilde{D}_{2k} & -\Delta\hat{L}_k \tilde{E}_{1k} \end{bmatrix},$$

$$\tilde{\Omega}_{2k} = \begin{bmatrix} 0 & \Delta\hat{L}_k \tilde{C}_{2k} H_k & \tilde{B}_{3k} H_{k-d} & 0 & 0 & \Delta\hat{L}_k \tilde{D}_{3k} & 0 \end{bmatrix},$$

$$\tilde{\Omega}_{3k} = \begin{bmatrix} 0 & \Delta\hat{L}_k \tilde{C}_{3k} H_k & 0 & 0 & 0 & -\Delta\hat{L}_k \tilde{D}_{4k} & \Delta\hat{L}_k \tilde{E}_{2k} \end{bmatrix},$$

$$\tilde{\Omega}_{4k} = \begin{bmatrix} 0 & \Delta\hat{L}_k \tilde{C}_{4k} H_k & 0 & 0 & 0 & -\Delta\hat{L}_k) \tilde{D}_{5k} & \Delta\hat{L}_k \tilde{E}_{3k} \end{bmatrix}.$$

From (15) and (34), one has

$$\Upsilon_1 + \hat{M}_1 F_k \hat{N}_1 + \hat{N}_1^T F_k^T \hat{M}_1^T + \hat{M}_2 F_k \hat{N}_2 + \hat{N}_2^T \hat{F}_k^T \hat{M}_2^T$$
$$+\hat{M}_3 F_k \hat{N}_3 + \hat{N}_3^T F_k^T \hat{M}_3^T \le 0 , \tag{35}$$

where $\hat{M}_1 = \begin{bmatrix} 0 & \hat{M} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T$,

$$\hat{N}_1 = \begin{bmatrix} \hat{N}\tilde{C}_{0k} H_k & \sqrt{\varsigma_1}\hat{N}\tilde{C}_{2k} H_k & \sqrt{\varsigma_2}\hat{N}\tilde{C}_{3k} H_k & \sqrt{\varsigma_3}\hat{N}\tilde{C}_{4k} H_k \end{bmatrix},$$

$$\hat{M}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \hat{M} & 0 \end{bmatrix}^T,$$

$$\hat{N}_2 = \begin{bmatrix} -\hat{N}\tilde{D}_{2k} & \sqrt{\varsigma_1}\hat{N}\tilde{D}_{3k} & -\sqrt{\varsigma_2}\hat{N}\tilde{D}_{4k} & -\sqrt{\varsigma_3}\hat{N}\tilde{D}_{5k} \end{bmatrix},$$

$$\hat{M}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \hat{M} \end{bmatrix}^T,$$

$$\hat{N}_3 = \begin{bmatrix} -\hat{N}\tilde{E}_{1k} & 0 & \sqrt{\varsigma_2}\hat{N}\tilde{E}_{2k} & \sqrt{\varsigma_3}\hat{N}\tilde{E}_{3k} \end{bmatrix}.$$

According to Lemma 1, if there exist positive scalars ε_7, ε_8 and ε_9, such that

$$\Upsilon_1 + \varepsilon_7 \hat{M}_1 \hat{M}_1^T + \varepsilon_7 \hat{N}_1^T \hat{N}_1 + \varepsilon_8 \hat{M}_2 \hat{M}_2^T + \varepsilon_8 \hat{N}_2^T \hat{N}_2 + \varepsilon_9 \hat{M}_3 \hat{M}_3^T + \varepsilon_9 \hat{N}_3^T \hat{N}_3 \le 0 . \tag{36}$$

By applying the Schur complement lemma to (36), we have (22). Thus, it can be obtained from (22) that $e_{k+1}^T P_{k+1}^{-1} e_{k+1} \le 1$ holds. By mathematical induction, it is shown that the addressed proposition holds for all $k \in \mathbb{N}^+$, which means that the filtering error system (16) with the conditions of the WTOD protocol and hybrid cyber attacks satisfies the P_k-dependent ellipsoidal constraint with the filtering gain matrix $\hat{L}_k$. This completes the proof.

3.1.2 Non-fragile set-membership filter under the SC-protocol

Theorem 2: For the system (1) with the SC protocol (8) and hybrid cyber attacks (10), let the sequence of constraint matrices $P_k > 0$ ($k \in \mathbb{N}^+$) be given, and the filtering error e_k satisfy $e_k^T P_k^{-1} e_k \le 1$. If there exist matrices $P_{k+1} > 0$, filtering gain matrices $\hat{L}_k$ and positive scalars ε_j ($j \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$), the following matrix inequality holds

$$\begin{bmatrix} -\bar{\Theta}_k & \hat{\Omega} & \hat{M}_1 & 0 & \hat{M}_2 & 0 & \hat{M}_3 & 0 \\ * & -P & 0 & \varepsilon_7 \hat{N}_1^T & 0 & \varepsilon_8 \hat{N}_2^T & 0 & \varepsilon_9 \hat{N}_3^T \\ * & * & -\varepsilon_7 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & -\varepsilon_7 & 0 & 0 & 0 & 0 \\ * & * & * & * & -\varepsilon_8 & 0 & 0 & 0 \\ * & * & * & * & * & -\varepsilon_8 & 0 & 0 \\ * & * & * & * & * & * & -\varepsilon_9 & 0 \\ * & * & * & * & * & * & * & -\varepsilon_9 \end{bmatrix} \le 0 , \tag{37}$$

where

$$\bar{\Theta}_k == diag\left\{1-\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4-\varepsilon_5-\varepsilon_6, \varepsilon_1 I, \varepsilon_2 I, 0, \varepsilon_4 S^{-1}, \varepsilon_5 R^{-1}, \varepsilon_1 Q^{-1}\right\} + \varepsilon_3 \Xi_1 ,$$

and matrices $\hat{\Omega}$, P, $\hat{M}_1$, $\hat{M}_2$, $\hat{M}_3$, $\hat{N}_1$, $\hat{N}_2$ as well as $\hat{N}_3$ have been explicitly defined in Theorem 1. Then, the filtering error e_{k+1} satisfies the ellipsoid constraint $e_{k+1}^T P_{k+1}^{-1} e_{k+1} \le 1$.

Proof: The proof process of Theorem 2 is similar to that of Theorem 1, so we present an abbreviated proof process below.

By considering (2), (18), and the scheduling rule of the SC protocol (8) comprehensively, one has

$$\begin{cases} \mathrm{E}\left\{Z_k^T Z_k\right\} \le 1 \\ \mathrm{E}\left\{Z_{k-\tau}^T Z_{k-\tau}\right\} \le 1 \\ \omega_k^T S_k^{-1} \omega_k \le 1 \\ v_k^T R_k^{-1} v_k \le 1 \end{cases} . \tag{38}$$

Rearrange (26) and (38), which yields

$$\begin{cases} \eta_k^T diag\{-1, I, 0,0,0,0,0\}\eta_k \le 0 \\ \eta_k^T diag\{-1,0,I,0,0,0,0\}\eta_k \le 0 \\ \eta_k^T diag\{-1,0,0,0,S^{-1},0,0\}\eta_k \le 0 \\ \eta_k^T diag\{-1,0,0,0,0,R^{-1},0\}\eta_k \le 0 \\ \eta_k^T diag\{-1,0,0,0,0,0,Q^{-1}\}\eta_k \le 0 \\ \eta_k^T diag\{0, H_k^T M_1^T M H_k, 0, I, 0,0,0\}\eta_k \le 0 \end{cases} . \quad (39)$$

According to Lemma 1, if there exist positive scalars ε_1, ε_2, ε_3, ε_4, ε_5 and ε_6, such that

$$\eta_k^T(\Omega^T P_{k+1}^{-1}\Omega - diag\{1,0,0,0,0,0,0\})\eta_k - \varepsilon_1\eta_k^T diag\{-1,I,0,0,0,0,0\}\eta_k$$
$$-\varepsilon_2\eta_k^T diag\{-1,0,I,0,0,0,0\}\eta_k$$
$$-\varepsilon_3\eta_k^T\Xi_1\eta_k - \varepsilon_4\eta_k^T diag\{-1,0,0,0,S^{-1},0,0\}\eta_k - \varepsilon_5\eta_k^T diag\{-1,0,0,0,0,R^{-1},0\}\eta_k$$
$$-\varepsilon_6\eta_k^T diag\{-1,0,0,0,0,0,Q^{-1}\}\eta_k \le 0 . \quad (40)$$

Accordingly, (40) can be rewritten as

$$\Omega^T P_{k+1}^{-1}\Omega - diag\{1-\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4-\varepsilon_5-\varepsilon_6, \varepsilon_1 I, \varepsilon_2 I, 0, \varepsilon_4 S^{-1}, \varepsilon_5 R^{-1}, \varepsilon_1 Q^{-1}\}$$
$$-\varepsilon_3\Xi_1 \le 0 . \quad (41)$$

We denote that

$$\bar{\Theta}(k) = diag\{1-\varepsilon_1-\varepsilon_2-\varepsilon_3-\varepsilon_4-\varepsilon_5-\varepsilon_6, \varepsilon_1 I, \varepsilon_2 I, 0, \varepsilon_4 S^{-1}, \varepsilon_5 R^{-1}, \varepsilon_1 Q^{-1}\}$$
$$+\varepsilon_3\Xi_1 . \quad (42)$$

Then, (41) is equivalent to

$$\Omega^T P_{k+1}^{-1}\Omega - \bar{\Theta}_k \le 0 . \quad (43)$$

Applying the Schur complement lemma to (43), we can obtain

$$\begin{bmatrix} -\bar{\Theta}_k & \Omega^T \\ * & -P \end{bmatrix} \le 0 . \quad (44)$$

Due to the presence of a matrix with parametric uncertainty, (44) can be decomposed into

$$\Upsilon_2 + \begin{bmatrix} 0 & \tilde{\Omega}^T \\ * & 0 \end{bmatrix} \le 0 , \quad (45)$$

where $\Upsilon_2 = \begin{bmatrix} -\bar{\Theta}_k & \hat{\Omega}^T \\ * & -P \end{bmatrix}$.

From (15) and (45), it is obtained that

$$\Upsilon_2 + \hat{M}_1\hat{F}_k\hat{N}_1 + \hat{N}_1^T\hat{F}_k^T\hat{M}_1^T + \hat{M}_2\hat{F}_k\hat{N}_2 + \hat{N}_2^T\hat{F}_k^T\hat{M}_2^T$$
$$+\hat{M}_3\hat{F}_k\hat{N}_3 + \hat{N}_3^T\hat{F}_k^T\hat{M}_3^T \le 0 . \quad (46)$$

According to Lemma 2, if there exist positive scalars ε_7, ε_8 and ε_9, such that

$$\Upsilon_2 + \varepsilon_7\hat{M}_1\hat{M}_1^T + \varepsilon_7\hat{N}_1^T\hat{N}_1 + \varepsilon_8\hat{M}_2\hat{M}_2^T + \varepsilon_8\hat{N}_2^T\hat{N}_2$$
$$+\varepsilon_9\hat{M}_3\hat{M}_3^T + \varepsilon_9\hat{N}_3^T\hat{N}_3 \le 0 . \quad (47)$$

By applying the Schur complement lemma to (47), we have (37). Thus, it can be obtained from (37) that $e_{k+1}^T P_{k+1}^{-1} e_{k+1} \le 1$ holds. By mathematical induction, it is shown that the addressed proposition holds for all $k \in \mathbb{N}^+$, which means that the filtering error system (16) with the conditions of the SC protocol and hybrid cyber attacks satisfies the P_k-dependent ellipsoidal constraint with the filtering gain matrix $\hat{L}_k$. This completes the proof.

Remark 3. It can be seen from (Shen et al., 2011) that solving algorithms based on standard LMI systems have polynomial time complexity. For example, define the computational complexity of LMI as $\lambda(\eta\iota^3\log(\kappa\lambda^{-1}))$, where η is the row size, ι is the number of scalar decision variables, κ is a data-related scaling factor, and λ is the relative precision setting of the algorithm. In our work, the parameters η, ι, κ, and λ increase with the increase of system dimension, which increases the computational complexity of LMI system to a certain extent. In spite of this, because the unknown variables of the matrix inequality (37) have linear relationship and powerful computing power of software, the feasible solutions of matrix inequality (37) could be obtained in time by utilizing well developed LMI toolbox.

Corollary 1. Considering the system (1) with the WTOD protocol (5) and hybrid cyber attacks (10), and the set-membership filter (14), the ellipsoid constraint matrices P_k on the filtering error e_k is minimized in the sense of the matrix trace if there exist positive definite matrix P_{k+1}, filtering gain matrix $\hat{L}_k$ and positive scalars ε_j $(1 \le j \le 9)$ solving the following optimization problem:

$$\min_{\hat{L}_k, P_{k+1}, \varepsilon_j > 0} \operatorname{tr}(P_{k+1}) \quad (48)$$

subject to (22).

Corollary 2. Considering the system (1) with the SC protocol (8) and hybrid cyber attacks (10), and the set-membership filter (14), the ellipsoid constraint matrices P_k on the filtering error e_k is minimized in the sense of the matrix trace if there exist positive definite matrix P_{k+1}, filtering gain matrix $\hat{L}_k$ and positive scalars ε_j $(1 \le j \le 9)$ solving the following optimization problem:

$$\min_{\hat{L}_k, P_{k+1}, \varepsilon_j > 0} \operatorname{tr}(P_{k+1}) \quad (49)$$

subject to (37).

4. ILLUSTRATIVE EXAMPLES

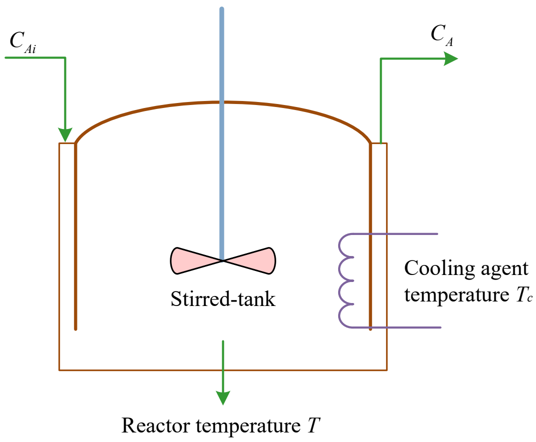

Fig. 2. Diagram of an industrial continuous stirred-tank reactor.

Example 1: In this case, we will show the effectiveness of the presented non-fragile set-membership filtering algorithm by an industrial continuous stirred-tank reactor in (Lehman et al., 1994). As shown in Figure 2, the reactor system involves a nonlinear process that transforms chemical substance A into substance B, where C_{Ai} represents the inlet concentration of material A, C_A is the outlet concentration of material A, T is the temperature of the reactor system, and T_C is the temperature of the cooling agent. In control practice, due to the unpredictable nature of environmental changes, the parameters of the reactor system may be subject to some degree of variation. In this system, the state variables of the system are the temperature $x_1(k)=T$ in the reactor and the temperature $x_2(k)=T_j$ in the jacket; the input is the feed concentration $u(k)=C_{Ai}$; the output is the discharge concentration $y(k)=C_A$. The system parameter matrices are time-varying, which are given as follows:

$$A_k=\begin{bmatrix}-1.34 & 0.7\\ -1.25 & 0.2+\sin(0.05k)\end{bmatrix},$$

$$B_k=\begin{bmatrix}0.6 & 1.2\\ 0.95 & 0.01+0.05\sin(0.01k)\end{bmatrix},$$

$$C_k=\begin{bmatrix}-0.8 & 0.2\\ 0.8 & -0.05\end{bmatrix},$$

$$D_k=\begin{bmatrix}0.05 & 0.8\\ 1 & 0.03+0.5\sin(0.1k)\end{bmatrix}.$$

The nonlinear function $f(x_k)$ of the reactor system is selected as follows:

$$f(x_k)=0.5+0.3\sin(x_k).$$

It is assumed that the reactor system is subject to deception attacks and replay attacks with the probabilities of $\bar{\alpha}=0.3$ and $\bar{\beta}=0.4$, respectively. The deception attack signal is denoted by $\delta_k=2.5I$, and the replay delay $\tau_k\in[1,2]$ is a random variable. The bounded system noise and measurement noise in the reactor system are given by $\omega(k)=0.4*[sin(0.6k)\ sin(0.6k)]^T$ and $v(k)=0.05*[sin(k)\ sin(k)]^T$ with the covariance matrices $S_k=R_k=0.75I$, respectively. The given perturbation of the filtering gain is $\Delta\hat{L}_k=\hat{M}\hat{F}_k\hat{N}$, where $\hat{M}=\begin{bmatrix}0.25 & 0.25 & 0.25 & 0.25\\ 0.25 & 0.25 & 0.25 & 0.25\end{bmatrix}^T$, $\hat{N}=\begin{bmatrix}0.1 & 0.1 & 0.1 & 0.1\\ 0.1 & 0.1 & 0.1 & 0.1\end{bmatrix}$, $\hat{F}_k=\begin{bmatrix}\sin(0.1k) & 1 & 0 & 1\\ 1 & 0 & 0 & \sin(0.1k)\end{bmatrix}$. The weight matrix for the WTOD protocol is selected as $Q_1=Q_2=0.6$, and the SC protocol obeys the Markov transition probabilities as follows:

$$\pi=\begin{bmatrix}0.2735 & 0.7265\\ 0.6986 & 0.3014\end{bmatrix}.$$

Based on Theorem 1, Theorem 2, Corollary 1, and Corollary 2, the optimization problems (48) and (49) are solved by utilizing the LMI Toolbox of Matlab software. The resulting filtering gain matrices $\hat{L}_k$ are presented in Table 1 for the WTOD protocol and in Table 2 for the SC protocol, respectively.

Table 1. Filtering gain matrices under the WTOD Protocol.

K	0	1	…	99
$\hat{L}_k$	$\begin{bmatrix}-0.17 & 0\\ -0.42 & -0.99\\ 1.33 & 0\\ 0 & 0.25\end{bmatrix}$	$\begin{bmatrix}0 & 0.19\\ 0 & 0.47\\ 0.259 & 0\\ 0.04 & 1.15\end{bmatrix}$	…	$\begin{bmatrix}1 & 0.19\\ 0 & 0.61\\ -0.249 & 0\\ 0 & -0.15\end{bmatrix}$

Table 2 Filtering gain matrices under the SC Protocol

K	0	1	…	99
$\hat{L}_k$	$\begin{bmatrix}-0.16 & 0\\ -0.51 & 0.76\\ 1.27 & 0\\ 0 & -0.24\end{bmatrix}$	$\begin{bmatrix}0 & 0.18\\ 1.3 & 0.61\\ 0 & -0.15\\ 0.53 & 0\end{bmatrix}$	…	$\begin{bmatrix}-0.22 & 0.47\\ 0.02 & 0\\ 0.93 & 0\\ 0 & 1.39\end{bmatrix}$

It is assumed that the initial state and constraint matrix are given as $x_0=[0.1\ 0.1]^T$ and $P_0=diag\{1.17,1.17,1.17,1.17\}$, respectively. The simulation results are shown in Figure 3-11. Figure 3 depicts the communication sequence subject to the WTOD scheduling protocol, where ‘1’ in the y-axis represents sensor 1 obtains the access authority to communication network; similarly, ‘2’ in the y-axis represents sensor 2 obtains the access authority to communication network. Figure 4 depicts the communication sequence subject to the SC scheduling protocol. In such a communication protocol, which sensor obtains network access authority is determined by Markov chain with the given transition probability. Figure 5 depicts the occurrence time of replay attacks and deception attacks, where ‘0’ in the y-axis indicates that the system does not suffer any cyber attacks at that instant, and ‘1’ in the y-axis indicates that the system is subjected to cyber attacks at that time instant. Figure 6 and Figure 7 depict the trajectories of system states $x_1(k)$ and $x_2(k)$, as well as their estimations $\hat{x}_1(k)$ and $\hat{x}_2(k)$ under the influence of hybrid cyber attacks and various scheduling protocols. Figure 8 and Figure 9 plot the trajectories of the filtering error $e_1(k)$ and $e_2(k)$ with respect to the WTOD protocol and the SC protocol. Figure 10 and Figure 11 depict the trajectories of $e_1(k+1)^T P^{-1} e_1(k+1)$ and $e_2(k+1)^T P^{-1} e_2(k+1)$ under the WTOD protocol, respectively. It can be seen from Figure 6-11 that filtering performance is well achieved and the proposed non-fragile set-membership filter algorithm is indeed effective for the reactor system under both hybrid cyber attacks and WTOD protocol/SC protocol.

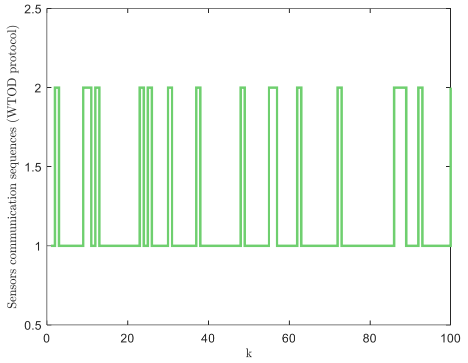

Fig. 3. The communication sequence of sensors under the WTOD protocol.

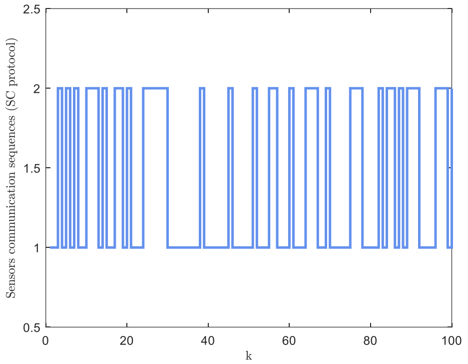

Fig. 4. The communication sequence of sensors under the SC protocol.

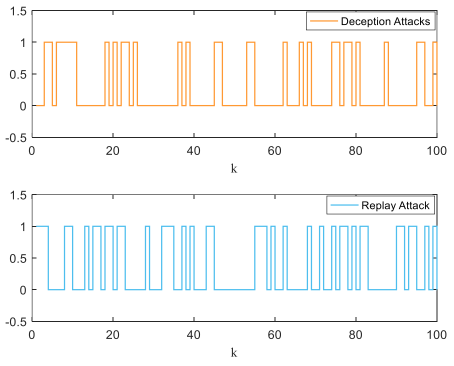

Fig. 5. The occurrence time of hybrid cyber attacks.

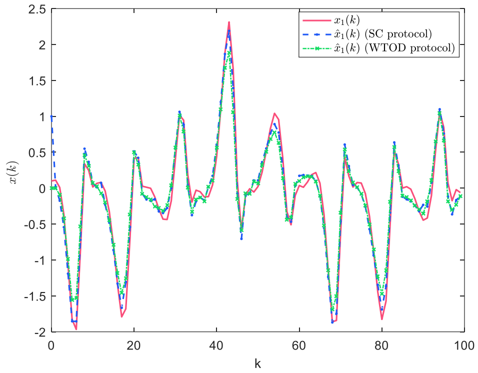

Fig. 6. The state trajectories of $x_1(k)$ and its estimation $\hat{x}_1(k)$.

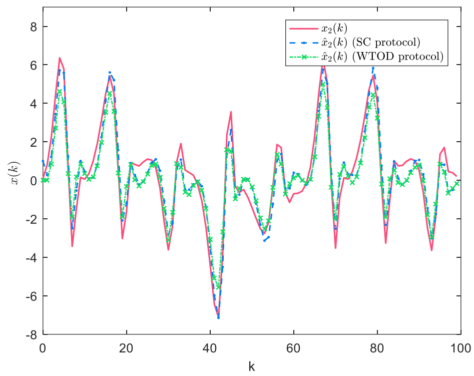

Fig. 7. The state trajectories of $x_2(k)$ and its estimation $\hat{x}_2(k)$.

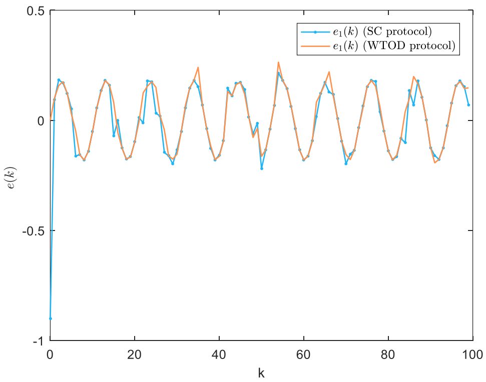

Fig. 8. The filtering error trajectories of $e_1(k)$.

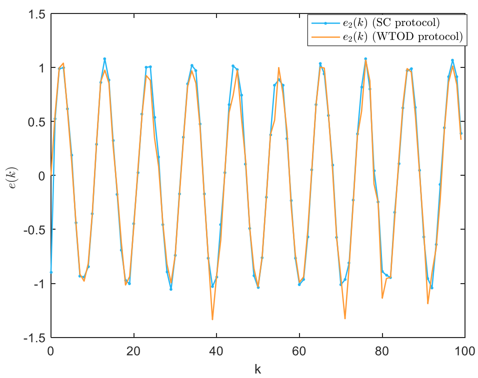

Fig. 9. The filtering error trajectories of $e_2(k)$.

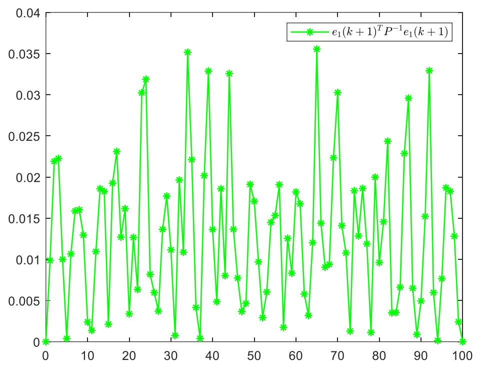

Fig. 10. The trajectories of $e_1(k+1)^T P^{-1} e_1(k+1)$ under the WTOD protocol.

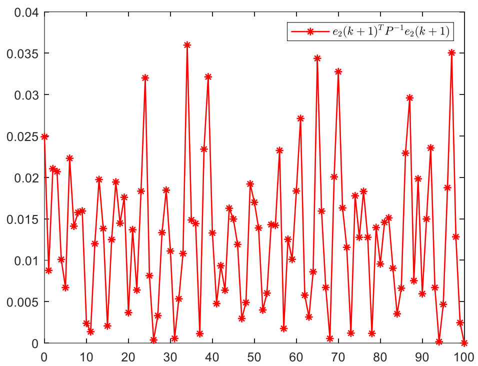

Fig. 11. The trajectories of $e_2(k+1)^T P^{-1} e_2(k+1)$ under the WTOD protocol.

Example 2: Another simulation example is presented to illustrate the effectiveness of the presented non-fragile set-membership filtering algorithm. Consider the system (1) with

$$A_k = \begin{bmatrix} -0.66 & 0.54 & 0.2 \\ -1.12 & 0.8 & 1.05 \\ 0.82 & 0.47 & 0.8+\sin(0.6k) \end{bmatrix},$$

$$B_k = \begin{bmatrix} 0.12 & 0.52 & 0.34 \\ 0.43 & 0.56 & 0.75 \\ 0.32 & 0.67 & 0.05+\sin(0.2k) \end{bmatrix},$$

$$C_k = \begin{bmatrix} -0.5 & 0.37 & 0.3 \\ -.12 & -0.3 & 0.8 \\ 0.45 & 0.47 & -0.11 \end{bmatrix},$$

$$D_k = \begin{bmatrix} 0.2 & 0.23 & 0.34 \\ 1.5 & 0.5 & 0.52 \\ 0.22 & 0.37 & 0.1+\sin(0.2k) \end{bmatrix}.$$

The system noise and measurement noise are given by $\omega(k) = 0.4*[sin(0.6k)\ \ sin(0.6k)\ \ sin(0.6k)\ ]^T$ and $v(k) = 0.05*[sin(k)\ \ sin(k)\ \ sin(k)]^T$ with the covariance matrices $S_k = R_k = 0.6I$, respectively. The given perturbation of the filtering gain is $\Delta\hat{L}_k = \hat{M}\hat{F}_k\hat{N}$, where

$$\hat{M} = \begin{bmatrix} 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.23 & 0.23 & 0.23 & 0.23 & 0.23 & 0.23 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \end{bmatrix}^T,$$

$$\hat{N} = \begin{bmatrix} 0.18 & 0.18 & 0.18 & 0.18 & 0.18 & 0.18 \\ 0.15 & 0.15 & 0.15 & 0.15 & 0.15 & 0.15 \\ 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 \end{bmatrix},$$

$$\hat{F}_k = \begin{bmatrix} \sin(0.2k) & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & \sin(0.2k) & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & \sin(0.1k) \end{bmatrix}.$$

The weight matrix of the WTOD protocol is selected as $Q_1 = Q_2 = 0.55$, and the SC protocol obeys the following Markov transition probability:

$$\pi = \begin{bmatrix} 0.3125 & 0.2654 & 0.4221 \\ 0.2673 & 0.4794 & 0.2533 \\ 0.3825 & 0.2736 & 0.3439 \end{bmatrix}.$$

Other parameters are selected to be the same as in Example 1.

We utilized an Intel Core i7 CPU for simulation, with a total time consumption of 3.24 seconds. It is assumed that the initial state is given as $x_0 = \begin{bmatrix} 2 & -1 & 2.2 \end{bmatrix}^T$. Figure 12-14 depict the trajectories of system states $x_1(k)$, $x_2(k)$ and $x_3(k)$, as well as their estimations $\hat{x}_1(k)$, $\hat{x}_2(k)$ and $\hat{x}_3(k)$ under the influence of hybrid cyber attacks and various scheduling protocols. It can be seen from Figure 12-14 that the proposed non-fragile set-membership filtering algorithm demonstrates excellent filtering performance, even in the presence of hybrid cyber attacks and WTOD/SC scheduling protocols.

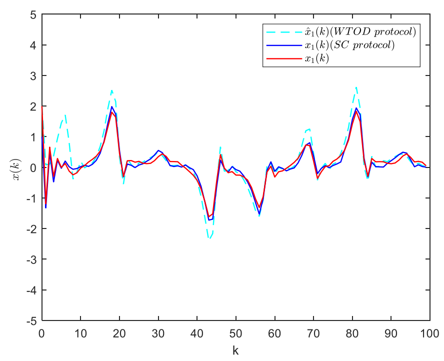

Fig. 12. The trajectories of $x_1(k)$ and its estimation $\hat{x}_1(k)$.

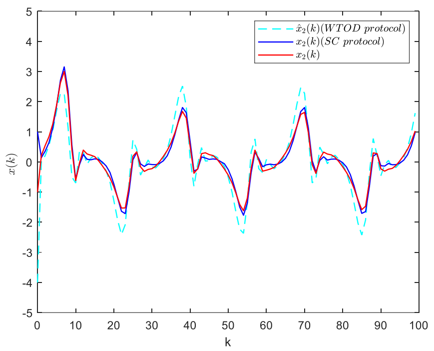

Fig. 13. The trajectories of $x_2(k)$ and its estimation $\hat{x}_2(k)$.

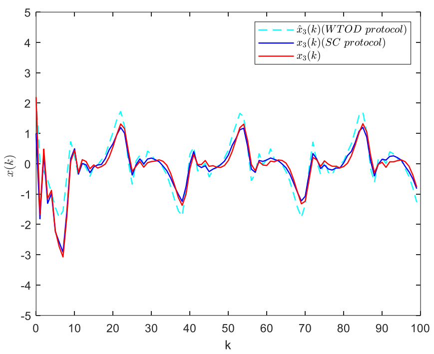

Fig.14. The trajectories of $x_3(k)$ and its estimation $\hat{x}_3(k)$.

5. CONCLUSIONS

In this paper, the non-fragile set-membership filtering problem has been investigated for a class of discrete time-varying networked systems under the influence of various scheduling protocols and hybrid cyber attacks. Due to limited networked bandwidth, only one sensor node is permitted to gain access to network medium according to the WTOD protocol/SC protocol at each transmission instant. In addition, the impact of two kinds of cyber attacks (namely, the replay attack and deception attack) on the filtering performance is also discussed. In such a framework, a non-fragile set-membership filter has been designed to obtain the state estimation for networked systems under the protocol scheduling and hybrid attacks. Sufficient conditions have been derived for the proposed filter to satisfy the prescribed P_k -dependent constraint in terms of mathematical induction. Furthermore, the optimal set-membership filtering gains have been obtained by optimizing the ellipsoid constraint of the filtering error subject to the aforementioned scheduling protocols and cyber attacks. Finally, the effectiveness of the proposed non-fragile set-membership filtering algorithm is verified by two simulation examples. In the future research work, we will develop advanced filtering algorithm based on event-triggering mechanism to further improve the filtering performance of networked systems under hybrid cyber attacks.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the financial supports by the National Science Foundation of China under Grant 62363024 and 62263019.

REFERENCES

Boyd S., El Ghaoui L., Feron E., et al. (1994). Linear matrix inequalities in system and control theory. *Philadelphia: SIAM Studies in Applied Mathematics*.

Chen B., Ho D W C., Hu G., et al. (2021). Delay-dependent distributed Kalman fusion estimation with dimensionality reduction in Cyber-Physical Systems. *IEEE Transactions on Cybernetics*, 52(12): 13557-13571.

Chen S., Ma L., Ma Y. (2020). Distributed set-membership filtering for nonlinear systems subject to Round-Robin protocol and stochastic communication protocol over sensor networks. *Neurocomputing*, 385: 13-21.

Chen Y., Zhu M., Lu R., et al. (2021). Distributed H_∞ filtering of nonlinear systems with random topology by an event-triggered protocol. *Science China Information Sciences*, 64: 1-15.

Cuong H M., Van Trieu P., Nho L C., et al. (2018). Adaptive neural network sliding mode control of shipboard container cranes considering actuator backlash. *Mechanical Systems and Signal Processing*, 112: 233-250.

Ding D., Liu H., Dong H., et al. (2022). Resilient filtering of nonlinear complex dynamical networks under randomly occurring faults and hybrid cyber-attacks. *IEEE Transactions on Network Science and Engineering*, 9(4): 2341-2352.

El Ghaoui L., Calafiore G. (2001). Robust filtering for discrete-time systems with bounded noise and parametric uncertainty. *IEEE Transactions on Automatic Control*, 46(7): 1084-1089.

Fort E H., Oya J R G., Chavero F M., et al. (2017). Intelligent containers based on a low-power sensor network and a non-invasive acquisition system for management and tracking of goods. *IEEE Transactions on Intelligent Transportation Systems*, 19(8): 2734-2738.

Ge X., Han Q L., Wang Z. (2017). A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks. *IEEE Transactions on Cybernetics*, 49(1): 171-183.

Ge X., Han Q L., Zhong M., et al. (2019). Distributed Krein space-based attack detection over sensor networks under deception attacks. *Automatica*, 109: 108557.

Han C., Chen D., Hu J., et al. (2023). Set membership filtering for discrete saturated time-varying networked systems with incomplete measurements under Round-Robin protocol. *Asian Journal of Control*, 25(6): 4721-4732.

Lee K H., Huang B. (2008). Robust H_2 optimal filtering for continuous-time stochastic systems with polytopic parameter uncertainty. *Automatica*, 44(10): 2686-2690.

Lehman B., Bentsman J., Lunel S V., et al. (1994). Vibrational control of nonlinear time lag systems with bounded delay: Averaging theory, stabilizability, and transient behavior. *IEEE Transactions on Automatic Control*, 39(5): 898-912.

Li M., Liang J. (2023). State estimation for 2-D uncertain systems with redundant channels and deception attacks: A set-membership method. *Applied Mathematics and Computation*, 457: 128190.

Li X., Dong H., Wang Z., et al. (2018). Set-membership filtering for state-saturated systems with mixed time-delays under Weighted Try-Once-Discard protocol. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 66(2): 312-316.

Liu K., Guo H., Zhang Q., et al. (2020a). Distributed secure filtering for discrete-time systems under Round-Robin protocol and deception attacks. *IEEE Transactions on Cybernetics*, 50(8): 3571-3580.

Liu L., Ma L., Wang Y., et al. (2020b). Distributed set-membership filtering for time-varying systems under constrained measurements and replay attacks. *Journal of the Franklin Institute*, 357(8): 4983-5003.

Petersen I R., Hollot C V. (1986). A Riccati equation approach to the stabilization of uncertain linear systems. *Automatica*, 22(4): 397-411.

Qu Y., Pang K. (2020). State estimation for a class of artificial neural networks subject to mixed attacks: A set-membership method. *Neurocomputing*, 411: 239-246.

Rahmanpour S., Esfanjani R M. (2019). Energy-aware planning of motion and communication strategies for networked mobile robots. *Information Sciences*, 497: 149-164.

Shen B., Wang Z., Liu X. (2011). Bounded H_∞ synchronization and state estimation for discrete time-varying stochastic complex networks over a finite horizon. *IEEE Transactions on Neural Networks*, 22(1): 145-157.

Shen H., Xing M., Huo S., et al. (2019). Finite-time H_∞ asynchronous state estimation for discrete-time fuzzy Markov jump neural networks with uncertain measurements. *Fuzzy Sets and Systems*, 356: 113-128.

Stojanovic V., Nedic N. (2016). Robust Kalman filtering for nonlinear multivariable stochastic systems in the presence of non-Gaussian noise. *International Journal of Robust and Nonlinear Control*, 26(3): 445-460.

Wang Q., Sun X., Wen C. (2021). Design method for a higher order extended Kalman filter based on maximum correlation entropy and a Taylor network system. *Sensors*, 21(17): 5864.

Wang W., Han C. (2021). Optimal H_2 filtering for sampled-data systems with measurement delays and packet dropouts. *IET Signal Processing*, 15(3): 182-194.

Wei G., Liu S., Wang L., et al. (2016). Event-based distributed set-membership filtering for a class of time-varying non-linear systems over sensor networks with saturation effects. *International Journal of General Systems*, 45(5): 532-547.

Zhang Y., Xia N., Han Q L., et al. (2020). Set-membership global estimation of networked systems. *IEEE Transactions on Cybernetics*, 52(3): 1454-1464.