Outlier-Resistant Recursive Security Filtering for Multirate Networked Systems Under Fading Measurements and Round-Robin Protocol

Jinliang Liu, *Member, IEEE*, Enyu Gong, Lijuan Zha, Xiangpeng Xie, *Senior Member, IEEE*, and Engang Tian, *Member, IEEE*

***Abstract*—This article investigates the recursive filtering problem with fading measurements and cyberattacks for multisensor multirate networked systems (MRNSs) the under the round-robin protocol (RRP). By exploiting the lifting technique, the sampling periods for both sensors and the state of the system are uniform. It is assumed that the phenomenon of fading measurements, which better describes practical engineering, arises stochastically, and the attenuation coefficients of which are described by a set of random variables with known statistical properties. In order to fully utilize the limited communication resources, RRP is introduced in the sensor-to-filter channel. Considering the measurement outliers, a saturation function is adopted in the filter structure to suppress the anomalous innovations so as to reduce the negative impact of the outliers. By means of the matrix difference equation, an upper bound is first obtained on the filtering error covariance, and the filter gain is designed to minimize the obtained upper bound by partial derivation. Moreover, the exponential boundedness of the filtering error dynamics is analyzed in the mean square sense. Finally, a numerical simulation example is given to demonstrate the validity of the proposed recursive security filtering scheme.**

***Index Terms*—Cyberattacks, fading measurements, multirate networked systems (MRNSs), outlier-resistant recursive security filtering, round-robin protocol (RRP).**

I. Introduction

DURING the past few decades, with the rapid development of the microelectronic technology, the networked control systems (NCSs) have received continuous research interest because of their practical applications ranging from different industrial systems to fundamental infrastructures, such as unmanned aerial vehicles [1], [2]; factory automation [1], [3]; power grids [4], [5]; and traffic systems [6]. The filtering problem or state estimation problem as a crucial topic in the area of NCSs has received persistent research attention. Up to now, many filtering algorithms have been developed, where the recursive filtering algorithm is apt to be implemented, hence it has gained particular research concerns [7], [8]. Kalman filtering (KF) method, the extended KF method [9], together with the unscented KF method [10], are all typical recursive filtering methods which have been studied and applied in widespread engineering practice. For instance, a state-saturated recursive filter was designed in [11] for a class of stochastic nonlinear complex networks in the presence of deception attacks, where an upper bound was guaranteed on the filtering error covariance and such an upper bound was then minimized. In [12], the distributed recursive filtering problem was investigated for discrete time-varying systems with state saturation and round-robin protocol (RRP) over sensor networks, and the filter parameters were designed such that the minimal filtering error covariance's upper bound was gained at each time instant.

To facilitate the development of the filtering algorithms, it is traditionally assumed that a uniform sampling period is utilized to the plant and sensors [13]. However, on account of diverse physical characteristics of the system components, it is quite unrealistic to unify the sampling periods for both plant and the multiple sensors in real practice [6]. As such, the setting multirate sampling strategy according to the importance of their signals is preferable in engineering applications [14], [15]. Due to the discordant sampling period, the filtering techniques designed for single-rate systems cannot be directly applied to multirate networked systems (MRNSs). Therefore, the filtering problems for MRNSs, which aim to estimate the system state by measurement outputs, have stirred considerable attention form researchers in the past decades [16], [17], [18]. With the help of the lifting technique, the MRNS in [17] was transformed into a corresponding single-rate system and distributed filter gains were derived under RRP. In [18], an MRNS was transformed into a single-rate one, and the vector augmentation method and an optimization algorithm was proposed to parameterize the estimator gains in order to investigate the

Manuscript received 2 September 2022; revised 30 December 2022 and 14 February 2023; accepted 18 February 2023. Date of publication 13 March 2023; date of current version 5 December 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62273174, Grant 61973152, Grant 62022044, and Grant 61903182, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20211290, and in part by the Qing Lan Project. Recommended by Associate Editor Jianping He. *(Corresponding author: Lijuan Zha.)*

Jinliang Liu, Enyu Gong, and Lijuan Zha are with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: liujinliang@vip.163.com; 13914866579@163.com; zhalijuan@vip.163.com).

Xiangpeng Xie is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: xiexiangpeng1953@163.com).

Engang Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

Digital Object Identifier 10.1109/TCNS.2023.3256299

set-membership state estimation problem under the FlexRay protocol.

Under the actual circumstance, due to the existing manufacturing variation and complicated environments, measurement output from individual sensor tends to suffer from different probabilistic information fading [12], [19], [20]. Taking fading effects on the sensor measurements and denial-of-service attacks into consideration simultaneously, Li et al. [21] tackled the distributed zonotopic set-membership filtering problem for discrete-time systems over sensor networks. Furthermore, via minimizing the F-radius of zonotope, an optimal filter parameter was derived. Nevertheless, compared with fruitful advancements on filtering problems with fading measurements, the corresponding research on recursive filtering problem for MRNSs with fading measurements has received much less attention, which partially motivates our current investigation.

Benefiting from the evolution of the wireless communication network, coupled with the continuous development of the control systems, the spatially distributed components can be connected by the wireless network, which facilitates the information exchange in the control systems. However, the wireless networks also have some defects, including the vulnerability to cyberattacks and constrained communication capacity issues induced by the limited networked bandwidth [22]. Among various security threats including deception attacks [23], [24], [25], [26], [27], [28]; denial-of-service attacks [29], [30], [31], [32], [33]; and replay attacks [34], the deception attacks are deemed as the most general yet hazardous ones in that the adversaries arbitrarily inject the false data, giving rise to filtering performance degeneration and system instability. Moreover, in engineering applications, the limited bandwidth challenge would bring about channel congestion and data collisions if multiple sensors are allowed to get access to transmit their measurement packets simultaneously. An active way of alleviating the communication burden is deploying communication protocols such as RRP [13], [17], [35], [36]; stochastic communication protocol [37]; try-once-discard protocol [38]; and FlexRay protocol [18] to orchestrate the transmission order of measurements. Among them, RRP is considered to be the most static and widely used scheduling protocol, under which each sensor node is assigned to the communication channel equally in a fixed circular order. Thus, the investigation of recursive filtering problem with fading measurements and cyberattacks for multisensor MRNSs under RRP would be of great significance.

In practical engineering applications, probable cyberattacks or any other sudden environmental changes may cause abnormal amplitude changes of measured outputs. This is referred to as the measurement outlier, which will degenerate or even damage the filter [1]. As such, it has aroused continuous attention from researchers in the areas of secure filtering/control, and some pioneering results have been reported on demonstrating the mechanism of measurement outliers and outlier resistance (see [39], [40], [41], and the references therein). In [1], an observer-based controller was designed for a class of NCSs under the encoding–decoding communication mechanism such that the system achieved input-to-state stability in the presence of measurement outliers. However, inadequate research

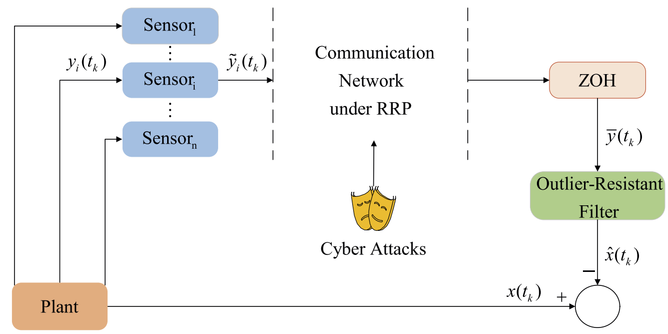

Fig. 1. Structure of the considered MRS.

attention has been paid to time-varying MRNSs with both measurement outliers and the above network-induced problems despite its practical significance; thus, it remains as a potential research branch. This is also the motivation of the current research.

Motivated by the above analysis, taking fading measurements, stochastic cyberattacks, as well as RRP into account, we are concerned with the filter parameter design and performance analysis of a class of discrete time-varying multisensor MRNSs in this article. The main contributions of this article are as follows. 1) A new discrete time-varying multisensor multirate system model is established, which considers the impacts of fading measurements, stochastic cyberattacks, and RRP. 2) An effective recursive filtering algorithm is designed that is applicable to online computation. 3) A sufficient condition is provided to guarantee the exponential mean-square boundedness of the filtering error dynamic system.

Notations: The notation used here is fairly standard. $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, and $\mathbb{R}^{m\times n}$ is the set of all real matrices of dimension $m\times n$. diag$\{\dots\}$ represents a blockdiagonal matrix, and col$\{\dots\}$ stands for a column vector composed of elements. In particular, diag$_n\{x_i\}$ stands for a block-diagonal matrix with matrices x_i $(i = 1,2,\dots,n)$ on the diagonal, col$_n\{x_i\}$ describes the column vector $\{x_1^T, x_2^T, \dots, x_n^T\}^T$. Prob$\{a\}$ stands for the occurrence probability of the event a. $\|\cdot\|$ is the Euclidean or spectral norm of vector of real matrices. I and 0 denote the identity matrix and zero matrix with proper dimensions, respectively. A^T, A^{-1}, tr$\{A\}$ represent the transpose, the inverse, and the trace of the matrix A, respectively. $\mathbb{E}\{\cdot\}$ means the expectation of the random variable. sym$\{X\} = X + X^T$ means the sum of matrix X and its transpose.

II. Problem Formulation and Preliminaries

A. System Model

As shown in Fig. 1, the plant is measured by n $(n \geq 2)$ sensors, and the measurement outputs may encounter fading phenomenon, which may occur in a probabilistic way. Sensors and the filter are connected through a communication channel that is likely to be attacked by adversaries. The RRP is introduced to coordinate the transmission sequence of the measurement outputs a the communication channel bandwidth is limited. An

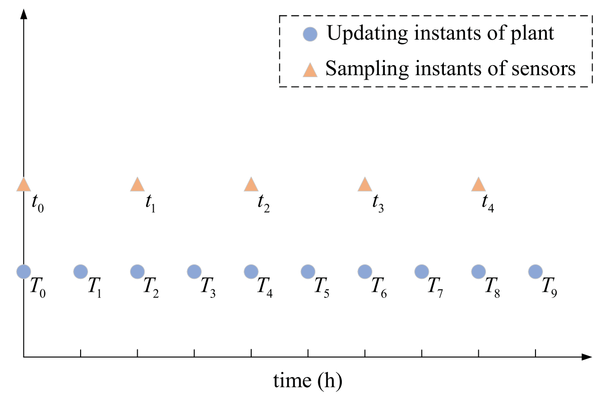

Fig. 2. Illustration of the multirate sampling scheme with $g = 2$.

outlier-resistant filter that is able to resist the cyberattacks and randomly fading measurements is constructed to estimate the system state.

Consider the following discrete time-varying multisensor MRNS described as follows:

$$\begin{cases} x(T_{k+1}) = A(T_k)x(T_k) + B(T_k)w(T_k) \\ y_i(t_k) = \lambda_i(t_k)C_i(t_k)x(t_k) + D_i(t_k)v_i(t_k) \end{cases} \quad (1)$$

where $x(T_k) \in \mathbb{R}^{n_x}$ is the system state, $y_i(t_k) \in \mathbb{R}^{n_y}$ is the measurement output by the ith sensor, respectively. $\lambda_i(t_k)$ represents the measurement attenuation coefficient of the ith sensor. $w(T_k) \in \mathbb{R}^{n_w}$ is the zero-mean process noise with covariance $Q(T_k) > 0$. $v_i(t_k)$ is the measurement noise for sensor i with zero mean and covariance $V_i(t_k) > 0$. $A(T_k), B(T_k), C_i(t_k)$ and $D_i(t_k)$ are time-varying matrices with appropriate dimensions. T_k represents the plant's updating instant while t_k means the sensors' sampling instant. The update period $h \triangleq T_{k+1} - T_k$ of the plant is different from the sampling period $H \triangleq t_{k+1} - t_k$ of the sensors, and they satisfy the relationship of $H = gh$, where $g \geq 2$ is a known positive integer. An illustration of the multirate sampling scheme with $g = 2$ is given in Fig. 2.

In addition, $\lambda_i(t_k)$ is uniformly distributed over the interval $(s_i, 1)\,(0 < s_i < 1)$ [12]. Here, the mean and variance of $\lambda_i(t_k)$ are given by $\bar{\lambda}_i(t_k) = (1 + s_i)/2$ and $r_i(t_k) = (1 - s_i)^2/12$, respectively. For later discussion convenience, we denote $\Lambda(t_k) = \text{diag}_n\{\lambda_i(t_k)\}, C(t_k) = \text{col}_n\{C_i(t_k)\}, D(t_k) = \text{diag}_n\{D_i(t_k)\}$ and $v(t_k) = \text{col}_n\{v_i(t_k)\}$.

Assumption 1: The random variables $w(T_k)$ and $v_i(t_k)$ are mutually independent. The initial state value $x(T_0)$ has the mean $m(T_0)$ and the covariance $P_{X(T_0)}$.

B. Stochastic Cyberattacks

In this article, sensors are connected to the filter through a communication channel. Due to the openness of the shared communication network, the measurement signals may be deliberately tampered by the randomly occurring malicious attacks that are launched by the adversary during the network transmission process [5], [35], [42]. We assume that this communication channel is prone to deception attacks, where the adversary intends to corrupt filter performance during the data transmission by sending certain deception signals into the true signal of the measurement output $y_i(t_k)$ in the communication network as shown in Fig. 1, and such an attacking behavior is described as follows:

$$\tilde{y}_i(t_k) = y_i(t_k) + \mu(t_k)\zeta_i(t_k). \quad (2)$$

$\tilde{y}_i(t_k)$ represents the actual signal passing through the network, which reflects the impact of randomly occurring deception attacks launched by the malicious adversary. $\mu(t_k)$ is the Bernoulli-distributed white sequences taking values on 0 or 1 with the following probabilities:

$$\text{Prob}\{\mu(t_k) = 1\} = \bar{\mu}, \quad \text{Prob}\{\mu(t_k) = 0\} = 1 - \bar{\mu} \quad (3)$$

where $\bar{\mu}$ is a known constant. $\zeta_i(t_k)$ is the false signal sent by the attacker to the i th sensor, which can be generated in the following form:

$$\zeta_i(t_k) = -y_i(t_k) + \eta_i(t_k) \quad (4)$$

where $\eta_i(t_k) \in \mathbb{R}^{n_y}$ satisfies $\|\eta_i(t_k)\| \leq \eta_i$ with covariance $E_i(t_k) > 0$. η_i is a known positive constant.

Remark 1: A set of Bernoulli-distributed white sequences $\mu(t_k)$ with known conditional probabilities to characterize the impacts of the attacks is introduced in (2). $\mu(t_k) = 0$ represents that the sensor measurement does not experience the deception attacks, and the actual transmitted signal is $y_i(t_k)$. Otherwise, $\mu(t_k) = 1$, this means the system is subject to deception attacks that will tamper the real data packets, in this case, the real transmitted signal is denoted as $\eta_i(t_k)$.

Remark 2: Security filtering, which deals with the filtering problem for networked system in the presence of malicious attacks, is acknowledged as an important research branch in the current control field [43]. Due to the antiattack countermeasures taken by the defenders, the resources limitations of the adversary, and the influence of network fluctuations [44], the cyberattacks are not always successful, and usually occur in an intermittently or randomly way. In the existing studies, various attack models have been proposed, such as Markov process models [45], constraint models [46], and Bernoulli models [47], [48], [49]. Among these proposed models, the Bernoulli stochastic process can exactly and expediently describe the probabilistic nature of the deception attacks, and then $\mu(t_k)$ is introduced.

C. Communication Protocol

Since the shared communication network between sensors and the filter is of limited bandwidth, RRP is employed to avoid data collisions and to schedule the transmission order of the sensors in the sensor-to-filter channel [13], [32], [35], [36], [50]. To characterize RRP in a precise way, we denote $\delta(t_k) = 1 + \text{mod}(k - 1, n)$ as the selected sensor that is granted the privilege to transmit a signal at time instant t_k. That is, under the RRP mechanism, only one sensor is allowed to transmit its measurement output at each sampling instant. Here, denote $\delta(t_0) = n$ when $k = 0$. Under the communication protocol, we define the available signal at the filter as $\breve{y}_i(t_k)$, which is formulated as

$$\breve{y}_i(t_k) = \gamma\left(\delta(t_k), i\right)\tilde{y}_i(t_k) + (1 - \gamma(\delta(t_k), i))\,\breve{y}_i(t_{k-1}) \quad (5)$$

where $\gamma(\cdot,\cdot)$ is the Kronecker function defined by $\gamma(a,b)=1$ if $a=b$ and $\gamma(a,b)=0$ if $a\neq b$. Moreover, it is assumed that $\breve{y}_i(t_k)=0$ for any $k<0$.

For expression convenience, we define

$$\bar{y}(t_k)=\text{col}_n\left\{\breve{y}_i(t_k)\right\},\ \eta(t_k)=\text{col}_n\left\{\eta_i(t_k)\right\}$$
$$\Gamma(t_k)=\text{diag}_n\left\{\gamma(\delta(t_k),i)I\right\}.$$

Then, we can obtain the following augmented measurement outputs based on RRP:

$$\begin{aligned}\bar{y}(t_k)=&\ [1-\mu(t_k)]\,\Gamma(t_k)\Lambda(t_k)C(t_k)x(t_k)\\&+[1-\mu(t_k)]\,\Gamma(t_k)D(t_k)v(t_k)+\mu(t_k)\Gamma(t_k)\eta(t_k)\\&+[I-\Gamma(t_k)]\,\bar{y}(t_{k-1}).\end{aligned}\tag{6}$$

D. Lifting Technique

In what follows, the lifting technique [51] is utilized to convert the MRNS into a single-rate one in order to facilitate the filter design.

Lemma 1: Define

$$\breve{x}(t_k)=\text{col}\left\{x(t_{k-1}+h),x(t_{k-1}+2h),\ldots,x(t_k)\right\}$$
$$\breve{w}(t_k)=\text{col}\left\{w(t_k),w(t_k+h),\ldots,w\left(t_k+(g-1)h\right)\right\}$$
$$\breve{A}(t_k)=\text{col}_g\left\{\widetilde{A}_i(t_k)\right\}$$
$$\breve{B}(t_k)=\text{col}\left\{\widetilde{B}_1^{(g)}(t_k),\widetilde{B}_2^{(g-1)}(t_k),\ldots,\widetilde{B}_g^{(1)}(t_k)\right\}$$
$$\breve{C}(t_k)=\begin{bmatrix}\underbrace{0_{nn_y\times n_x}\ldots 0_{nn_y\times n_x}}_{g-1} & C(t_k)\end{bmatrix}$$
$$\widetilde{A}_i(t_k)=\begin{bmatrix}\underbrace{0_{n_x\times n_x}\ldots 0_{n_x\times n_x}}_{g-1} & \vec{A}_i(t_k)\end{bmatrix},\ i=1,\ldots,g$$
$$\vec{A}_{g-m+1}(t_k)=\prod_{i=m}^{g}A(t_{k+1}-ih),\ m=1,\ldots,g$$
$$\widetilde{B}_m^{(s)}(t_k)=\begin{cases}\begin{bmatrix}B(t_k) & \underbrace{0\ldots0}_{g-1}\end{bmatrix},m=1,\ s=g\\ \begin{bmatrix}\vec{B}_1^{(s)}\ldots\vec{B}_{m-1}^{(s)} & B\left(t_k+(m-1)h\right) & \underbrace{0\ldots0}_{g-m}\end{bmatrix}\\ \qquad m=2,\ldots,g,\ s=g-m+1\end{cases}$$

$$\vec{B}_j^{(s)}=\prod_{i=s}^{g-j}A(t_{k+1}-ih)B\left(t_k+(j-1)h\right),j=1,\ldots,m-1$$
$$\breve{B}(t_k+jh)=\begin{bmatrix}\underbrace{0\ldots0}_{j} & B(t_k+jh) & \underbrace{0\ldots0}_{g-1-j}\end{bmatrix},j=1,\ldots,g-1.$$

Then the single-rate form of (1) is given by

$$\begin{cases}\breve{x}(t_{k+1})=\breve{A}(t_k)\breve{x}(t_k)+\breve{B}(t_k)\breve{w}(t_k)\\ \bar{y}(t_k)=[1-\mu(t_k)]\,\Gamma(t_k)\Lambda(t_k)\breve{C}(t_k)\breve{x}(t_k)+[1-\mu(t_k)]\\ \qquad\times\Gamma(t_k)D(t_k)v(t_k)+\mu(t_k)\Gamma(t_k)\eta(t_k)\\ \qquad+[I-\Gamma(t_k)]\,\bar{y}(t_{k-1}).\end{cases}\tag{7}$$

Proof: According to the system state equation in (1), one has

$$x(t_k+h)=\vec{A}_1(t_k)x(t_k)+\widetilde{B}_1^{(g)}(t_k)\breve{w}(t_k)\tag{8}$$

and then

$$\begin{aligned}x(t_k+2h)&=A(t_k+h)x(t_k+h)+B(t_k+h)w(t_k+h)\\&=\vec{A}_2(t_k)x(t_k)+\widetilde{B}_2^{(g-1)}(t_k)\breve{w}(t_k).\end{aligned}\tag{9}$$

Similarly, it can be concluded that

$$\begin{aligned}x(t_{k+1}-h)&=x\left(t_k+(g-1)h\right)\\&=\vec{A}_{g-1}(t_k)x(t_k)+\widetilde{B}_{g-1}^{(2)}(t_k)\breve{w}(t_k).\end{aligned}\tag{10}$$

Therefore

$$x(t_{k+1})=\vec{A}_g(t_k)x(t_k)+\widetilde{B}_g^{(1)}(t_k)\breve{w}(t_k).\tag{11}$$

Then, based on the definition of $\breve{x}(t_k)$, we obtain the compact form (7), which completes the proof of the lemma.

For convenience of derivation, define

$$\bar{x}(t_k)=\text{col}\left\{\breve{x}(t_k),\bar{y}(t_{k-1})\right\}$$
$$\mathscr{A}_f(t_k)=\begin{bmatrix}\mathcal{A}(t_k)\\ \mathscr{C}_f(t_k)\end{bmatrix},\quad \mathscr{B}_f(t_k)=\begin{bmatrix}\mathcal{B}(t_k)\\ \mathscr{D}_f(t_k)\end{bmatrix}$$
$$\mathcal{A}(t_k)=\begin{bmatrix}\breve{A}(t_k) & 0\end{bmatrix},\quad \mathcal{B}(t_k)=\begin{bmatrix}\breve{B}(t_k) & 0 & 0\end{bmatrix}$$
$$\mathscr{C}_f(t_k)=\begin{bmatrix}\left\{[1-\mu(t_k)]\,\Gamma(t_k)\Lambda(t_k)\breve{C}(t_k)\right\}^T\\ [I-\Gamma(t_k)]^T\end{bmatrix}^T$$
$$\mathscr{D}_f(t_k)=\begin{bmatrix}0\\ \left\{[1-\mu(t_k)]\,\Gamma(t_k)D(t_k)\right\}^T\\ [\mu(t_k)\Gamma(t_k)]^T\end{bmatrix}^T$$
$$\omega(t_k)=\begin{bmatrix}\breve{w}(t_k)\\ v(t_k)\\ \eta(t_k)\end{bmatrix}$$

then, we have

$$\begin{cases}\bar{x}(t_{k+1})=\mathscr{A}_f(t_k)\bar{x}(t_k)+\mathscr{B}_f(t_k)\omega(t_k)\\ \bar{y}(t_k)=\mathscr{C}_f(t_k)\bar{x}(t_k)+\mathscr{D}_f(t_k)\omega(t_k).\end{cases}\tag{12}$$

■

Remark 3: The lifting technique is one of the popular means that are employed to deal with multirate systems [6]. The dominant idea of the lifting technique is to unify the update period of different devices in a system. Since the update period h of the plant is different from the sampling period H of the sensors in (1), the states $x(t_{k-1}+h),x(t_{k-1}+2h),\ldots,x(t_k)$ in the interval $(t_{k-1}, t_k]$ are first augmented into a vector $\breve{x}(t_k)$. Then, a new state equation with the state update period H is obtained with the help of the original state equation. Accordingly, (1) is transformed into (12). In short, the lifting technique deals with the asynchronous sampling/updating issue by increasing the state update period [16], which is an effective method to transform a multirate system into an equivalent single-rate system.

E. Outlier-Resistant Filter Design

As discussed in Section I, if measurement outliers are not properly handled, it is likely to deteriorate the filter performance or even make the filtering error dynamics unstable. To mitigate the negative influences from the measurement outliers, a saturation function $\sigma(\cdot)$ is embedded in the filter structure whose saturation level can be determined in line with the prior knowledge on the range of the innovation.

Denote

$$\mathcal{Y}(t_k) = \bar{y}(t_k) - \mathscr{C}_f(t_k)\hat{x}(t_k). \tag{13}$$

Then, a so-called outlier-resistant filter is constructed as follows:

$$\hat{x}(t_{k+1}) = \mathscr{A}_f(t_k)\hat{x}(t_k) + K_f(t_k)\sigma(\mathcal{Y}(t_k)) \tag{14}$$

where $\hat{x}(t_k)$ is the estimate of $\bar{x}(t_k)$ and $K_f(t_k)$ is the filter gain to be designed. The initial value of the filter is $\hat{x}(t_0) = \mathbb{E}\{\bar{x}(t_0)\}$. In particular, the introduced saturation function $\sigma(\cdot) : \mathbb{R}^{nn_y} \to \mathbb{R}^{nn_y}$ is defined as follows:

$$\sigma(u) = \begin{bmatrix}\sigma_1(u_1) & \sigma_2(u_2) & \dots & \sigma_{nn_y}(u_{nn_y})\end{bmatrix}^T \tag{15}$$

with

$$\begin{aligned}\sigma_i(u_i) = {} & \operatorname{sign}(u_i)\varphi\left(|u_i|, u_{i,\max}\right) u_{i,\max} \\ & + \left[1 - \varphi\left(|u_i|, u_{i,\max}\right)\right] u_i \end{aligned} \tag{16}$$

where nn_y is the product of n and n_y, $\operatorname{sign}(\cdot)$ is the signum function, and $u_{i,\max}$ is the ith element of the vector $u_{\max}$, which represents the saturation level. $\varphi(\cdot,\cdot)$ is the function defined by $\varphi(a, b) = 1$ if $a > b$ and $\varphi(a, b) = 0$ if $a \le b$.

Remark 4: Aiming at restraining the side effects of measurement outliers, $\sigma_i(u_i)$ in the introduced saturation function $\sigma(\cdot)$ is given by

$$\sigma_i(u_i) = \begin{cases} u_i, & \text{if } |u_i| \le u_{i,\max} \\ \operatorname{sign}(u_i)u_{i,\max}, & \text{otherwise.}\end{cases} \tag{17}$$

For the sake of simplicity and facilitating later analysis, by the conception of $\varphi(\cdot,\cdot)$, $\sigma_i(u_i)$ is rewritten as (16), an equivalent yet tractable form.

Remark 5: It is noted that the measurement outliers that result from intermittent hardware failure, stochastic cyberattacks, or unexpected environmental changes in the process of signal transmission deviate from the normal measurements significantly. If not handled properly, it would result in the Kalman filter state estimation deviation [8], damage the optimal parameter estimate [52], and deteriorate the performance of the system. As such, in this article, we propose an outlier-resistant filter described as (14) to keep a desirable filtering performance in the presence of measurement outliers.

For discussion convenience, we define

$$\begin{aligned}\mathcal{Y}(t_k) &= \operatorname{col}_{nn_y}\{\mathcal{Y}_i(t_k)\} \\ \Psi(t_k) &= \operatorname{diag}_{nn_y}\{\varphi(|\mathcal{Y}_i(t_k)|, u_{i,\max})I\} \\ U(t_k) &= \operatorname{col}_{nn_y}\{\operatorname{sign}(\mathcal{Y}_i(t_k))u_{i,\max}\}.\end{aligned}$$

Then, the saturation function $\sigma(\mathcal{Y}(t_k))$ can be written as

$$\sigma(\mathcal{Y}(t_k)) = \Psi(t_k)U(t_k) + [I - \Psi(t_k)]\,\mathcal{Y}(t_k). \tag{18}$$

Let $\tilde{x}(t_k) = \bar{x}(t_k) - \hat{x}(t_k)$ be the filtering error and $P(t_k) = \mathbb{E}\{\tilde{x}(t_k)\tilde{x}^T(t_k)\}$ as the filtering error covariance of filter (14). In this article, the objective is to develop a filter such that an upper bound $\Sigma(t_k)$ is ensured for $P(t_k)$ and appropriate $K_f(t_k)$ is designed to obtain the minimized $\Sigma(t_k)$ by solving the Riccati-like difference equations. We give the following lemma, definition, and assumption that will be useful in obtaining the main results.

Lemma 2: [53] It is supposed that a matrix function $\varrho_k(\cdot) = \varrho_k^T(\cdot) : \mathbb{R}^s \to \mathbb{R}^s$ and the matrix $X = X^T \ge 0$ and $Y = Y^T \ge 0$ for $k \ge 0$. If

$$\begin{aligned}\varrho_k(X) &= \varrho_k^T(X) \\ \varrho_k(X) &\le \varrho_k^T(Y) \qquad \forall\, X \le Y\end{aligned}$$

then given the initial condition $M_0 = N_0 > 0$, there exists the solutions M_k and N_k to the following difference equations:

$$M_{k+1} \le \varrho_k(M_k), \quad N_{k+1} = \varrho_k(N_k)$$

satisfying

$$M_{k+1} \le N_{k+1}.$$

Definition 1: [8] Let scalars $\phi > 0, \zeta > 0$, and $0 < \nu < 1$, if for all $k \ge 0$

$$\mathbb{E}\left\{\|\psi(t_k)\|^2\right\} \le \phi\mathbb{E}\left\{\|\psi(t_0)\|^2\right\}\nu^k + \zeta$$

holds, then the stochastic process $\psi(t_k)$ is exponentially bounded in the mean square sense.

Assumption 2: Given positive real numbers $0 < \bar{a} < 1, \bar{b}, \underline{b}, \bar{c}, \underline{c}, \bar{d}, \underline{d}, \bar{w}, \underline{w}, \bar{e}$ and $\underline{e}$. The following conditions $\|\mathscr{A}_f(t_k)\| \le \bar{a}, \underline{b}^2 I \le \mathscr{B}_f(t_k)\mathscr{B}_f^T(t_k) \le \bar{b}^2 I, \underline{c}^2 I \le \mathscr{C}_f(t_k)\mathscr{C}_f^T(t_k) \le \bar{c}^2 I, \underline{d}^2 I \le \mathscr{D}_f(t_k)\mathscr{D}_f^T(t_k) \le \bar{d}^2 I, \underline{w} I \le W(t_k) \le \bar{w}^2 I, \underline{e} I \le \Sigma(t_k) \le \bar{e} I$ hold for all $k \ge 0$.

III. Main Results

In this section, the upper bound $\Sigma(t_k)$ of the filtering error covariance $P(t_k)$ is first given, and an effective algorithm to design the expected filter parameter to get a minimized upper bound at each time-step k is presented subsequently. Furthermore, the exponential boundedness of the filtering error is also analyzed in the sense of the mean square.

Theorem 1: Given positive scalars κ_i $(i = 1, 2, \dots, 9)$ and the filter gain $K_f(t_k)$, consider the following recursion for $\Sigma(t_{k+1})$:

$$\Sigma(t_{k+1}) = \tau_1\mathcal{M}(t_k)\Sigma(t_k)\mathcal{M}^T(t_k)$$

$$
\begin{aligned}
&+\tau_2\mathcal{N}(t_k)W(t_k)\mathcal{N}^T(t_k)\\
&+\tau_3 K_f(t_k)\text{tr}\left\{\mathscr{C}_f(t_k)\Sigma(t_k)\mathscr{C}_f^T(t_k)\right\}IK_f^T(t_k)\\
&+\tau_4 K_f(t_k)\text{tr}\left\{\mathscr{D}_f(t_k)W(t_k)\mathscr{D}_f^T(t_k)\right\}IK^T(t_k)\\
&+\tau_5 nn_y\bar{\lambda}K_f(t_k)K_f^T(t_k)
\end{aligned}\tag{19}
$$

where

$$
\begin{aligned}
\tau_1 &= 1+\kappa_1+\kappa_2+\kappa_3\\
\tau_2 &= 1+\kappa_4+\kappa_5+\kappa_6\\
\tau_3 &= 1+\kappa_1^{-1}+\kappa_4^{-1}+\kappa_7+\kappa_8\\
\tau_4 &= 1+\kappa_2^{-1}+\kappa_5^{-1}+\kappa_7^{-1}+\kappa_9\\
\tau_5 &= 1+\kappa_3^{-1}+\kappa_6^{-1}+\kappa_8^{-1}+\kappa_9^{-1}\\
\mathcal{M}(t_k) &= \mathscr{A}_f(t_k)-K_f(t_k)\mathscr{C}_f(t_k)\\
\mathcal{N}(t_k) &= \mathscr{B}_f(t_k)-K_f(t_k)\mathscr{D}_f(t_k)\\
W(t_k) &= \mathbb{E}\left\{\omega(t_k)\omega^T(t_k)\right\}\\
&= \text{diag}\left\{\tilde{Q}(t_k),\tilde{V}(t_k),\tilde{E}(t_k)\right\}\\
\tilde{Q}(t_k) &= \text{diag}\left\{Q(t_k),Q(t_k+h),\ldots,Q(t_{k+1}-h)\right\}\\
\tilde{V}(t_k) &= \text{diag}_n\left\{V_i(t_k)\right\}\\
\tilde{E}(t_k) &= \text{diag}_n\left\{E_i(t_k)\right\},\bar{\lambda}=\sum_{i=1}^{nn_y}u_{i,\max}^2
\end{aligned}
$$

with the real-valued matrices $\Sigma(t_k)=\Sigma^T(t_k)\geq 0$ $(k\geq 0)$, and the initial condition $\Sigma(t_0)=P(t_0)$. Then, an upper bound $\Sigma(t_{k+1})$ is obtained for the filtering error covariance $P(t_{k+1})$.

Proof: In light of (12)–(14) and (18), the filtering error $\tilde{x}(t_{k+1})$ is constructed as follows:

$$
\begin{aligned}
\tilde{x}(t_{k+1}) &= \mathcal{M}(t_k)\tilde{x}(t_k)+\mathcal{N}(t_k)\omega(t_k)+K_f(t_k)\mathcal{R}(t_k)\\
&\quad +K_f(t_k)\mathcal{S}(t_k)-K_f(t_k)\mathcal{T}(t_k)
\end{aligned}\tag{20}
$$

where

$$
\begin{aligned}
\mathcal{R}(t_k) &= \Psi(t_k)\mathscr{C}_f(t_k)\tilde{x}(t_k)\\
\mathcal{S}(t_k) &= \Psi(t_k)\mathscr{D}_f(t_k)\omega(t_k)\\
\mathcal{T}(t_k) &= \Psi(t_k)U(t_k).
\end{aligned}
$$

Then, the filtering error covariance $P(t_{k+1})$ can be obtained as follows:

$$
\begin{aligned}
P(t_{k+1}) &= \mathbb{E}\left\{\tilde{x}(t_{k+1})\tilde{x}^T(t_{k+1})\right\}\\
&= \mathcal{M}(t_k)P(t_k)\mathcal{M}^T(t_k)+\mathcal{N}(t_k)W(t_k)\mathcal{N}^T(t_k)\\
&\quad +K_f(t_k)\mathbb{E}\left\{\mathcal{R}(t_k)\mathcal{R}^T(t_k)\right\}K_f^T(t_k)\\
&\quad +K_f(t_k)\mathbb{E}\left\{\mathcal{S}(t_k)\mathcal{S}^T(t_k)\right\}K_f^T(t_k)\\
&\quad +K_f(t_k)\mathbb{E}\left\{\mathcal{T}(t_k)\mathcal{T}^T(t_k)\right\}K_f^T(t_k)\\
&\quad +\text{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\omega^T(t_k)\mathcal{N}^T(t_k)\}\right\}\\
&\quad +\text{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\mathcal{R}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad +\text{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad -\text{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad +\text{sym}\left\{\mathbb{E}\{\mathcal{N}(t_k)\omega(t_k)\mathcal{R}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad +\text{sym}\left\{\mathbb{E}\{\mathcal{N}(t_k)\omega(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad -\text{sym}\left\{\mathbb{E}\{\mathcal{N}(t_k)\omega(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad +\text{sym}\left\{\mathbb{E}\{K_f(t_k)\mathcal{R}(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad -\text{sym}\left\{\mathbb{E}\{K_f(t_k)\mathcal{R}(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\}\\
&\quad -\text{sym}\left\{\mathbb{E}\{K_f(t_k)\mathcal{S}(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\}.
\end{aligned}\tag{21}
$$

With the help of the matrix operation and using the properties of the trace of matrix, we can easily derive that

$$
\begin{aligned}
&K_f(t_k)\mathbb{E}\left\{\mathcal{R}(t_k)\mathcal{R}^T(t_k)\right\}K_f^T(t_k)\\
&\leq K_f(t_k)\mathbb{E}\left\{\text{tr}\left\{\mathcal{R}(t_k)\mathcal{R}^T(t_k)\right\}I\right\}K_f^T(t_k)\\
&\leq K_f(t_k)\text{tr}\left\{\mathbb{E}\left\{\mathscr{C}_f(t_k)\tilde{x}(t_k)\tilde{x}^T(t_k)\mathscr{C}_f^T(t_k)\right\}\right\}IK_f^T(t_k)\\
&= K_f(t_k)\text{tr}\left\{\mathscr{C}_f(t_k)P(t_k)\mathscr{C}_f^T(t_k)\right\}IK_f^T(t_k).
\end{aligned}\tag{22}
$$

Similarly, we can get

$$
\begin{aligned}
&K_f(t_k)\mathbb{E}\left\{\mathcal{S}(t_k)\mathcal{S}^T(t_k)\right\}K_f^T(t_k)\\
&\leq K_f(t_k)\mathbb{E}\left\{\text{tr}\left\{\mathcal{S}(t_k)\mathcal{S}^T(t_k)\right\}I\right\}K_f^T(t_k)\\
&\leq K_f(t_k)\text{tr}\left\{\mathbb{E}\left\{\mathscr{D}_f(t_k)\omega(t_k)\omega^T(t_k)\mathscr{D}_f^T(t_k)\right\}\right\}IK_f^T(t_k)\\
&= K_f(t_k)\text{tr}\left\{\mathscr{D}_f(t_k)W(t_k)\mathscr{D}_f^T(t_k)\right\}IK_f^T(t_k)
\end{aligned}\tag{23}
$$

$$
\begin{aligned}
&K_f(t_k)\mathbb{E}\left\{\mathcal{T}(t_k)\mathcal{T}^T(t_k)\right\}K_f^T(t_k)\\
&\leq K_f(t_k)\mathbb{E}\left\{U(t_k)U^T(t_k)\right\}K_f^T(t_k)\\
&\leq K_f(t_k)\text{tr}\left\{\mathbb{E}\left\{U(t_k)U^T(t_k)\right\}\right\}IK_f^T(t_k)\\
&= nn_y\bar{\lambda}K_f(t_k)K_f^T(t_k).
\end{aligned}\tag{24}
$$

Note that $\mathbb{E}\{\tilde{x}(t_k)\omega^T(t_k)\}=0$, it is easy to get that $\text{sym}\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\omega^T(t_k)\mathcal{N}^T(t_k)\}\}=0$. By using the well-known elementary inequality

$$
\left(\kappa^{1/2}X-\kappa^{(-1/2)}Y\right)\left(\kappa^{1/2}X-\kappa^{(-1/2)}Y\right)^T\geq 0 \tag{25}
$$

where X and Y are the matrices with appropriate dimensions, κ is an arbitrary positive constant, we obtain

$$
\begin{aligned}
&\text{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\mathcal{R}^T(t_k)K_f^T(t_k)\}\right\}\\
&\leq \kappa_1\mathcal{M}(t_k)P(t_k)\mathcal{M}^T(t_k)\\
&\quad +\kappa_1^{-1}K_f(t_k)\mathbb{E}\left\{\mathcal{S}(t_k)\mathcal{S}^T(t_k)\right\}K_f^T(t_k)\\
&\leq \kappa_1\mathcal{M}(t_k)P(t_k)\mathcal{M}^T(t_k)\\
&\quad +\kappa_1^{-1}K_f(t_k)\text{tr}\left\{\mathscr{C}_f(t_k)P(t_k)\mathscr{C}_f^T(t_k)\right\}IK_f^T(t_k).
\end{aligned}
$$

Similarly, it can also be derived that

$$
\text{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\}
$$

$$
\begin{aligned}
&\leq \kappa_2 \mathcal{M}(t_k) P(t_k) \mathcal{M}^T(t_k) \\
&\quad + \kappa_2^{-1} K_f(t_k) \mathrm{tr}\left\{\mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k)\right\} I K_f^T(t_k) \\
&- \mathrm{sym}\left\{\mathbb{E}\{\mathcal{M}(t_k)\tilde{x}(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_3 \mathcal{M}(t_k) P(t_k) \mathcal{M}^T(t_k) + \kappa_3^{-1} n n_y \bar{\lambda} K_f(t_k) K_f^T(t_k) \\
&\mathrm{sym}\left\{\mathbb{E}\{\mathcal{N}(t_k)\omega(t_k)\mathcal{R}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_4 \mathcal{N}(t_k) W(t_k) \mathcal{N}^T(t_k) \\
&\quad + \kappa_4^{-1} K_f(t_k) \mathrm{tr}\left\{\mathscr{C}_f(t_k) P(t_k) \mathscr{C}_f^T(t_k)\right\} I K_f^T(t_k) \\
&\mathrm{sym}\left\{\mathbb{E}\{\mathcal{N}(t_k)\omega(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_5 \mathcal{N}(t_k) W(t_k) \mathcal{N}^T(t_k) \\
&\quad + \kappa_5^{-1} K_f(t_k) \mathrm{tr}\left\{\mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k)\right\} I K_f^T(t_k), \\
&- \mathrm{sym}\left\{\mathbb{E}\{\mathcal{N}(t_k)\omega(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_6 \mathcal{N}(t_k) W(t_k) \mathcal{N}^T(t_k) + \kappa_6^{-1} n n_y \bar{\lambda} K_f(t_k) K_f^T(t_k) \\
&\mathrm{sym}\left\{\mathbb{E}\{K_f(t_k)\mathcal{R}(t_k)\mathcal{S}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_7 K_f(t_k) \mathrm{tr}\left\{\mathscr{C}_f(t_k) P(t_k) \mathscr{C}_f^T(t_k)\right\} I K_f^T(t_k) \\
&\quad + \kappa_7^{-1} K_f(t_k) \mathrm{tr}\left\{\mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k)\right\} I K_f^T(t_k) \\
&- \mathrm{sym}\left\{\mathbb{E}\{K_f(t_k)\mathcal{R}(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_8 K_f(t_k) \mathrm{tr}\left\{\mathscr{C}_f(t_k) P(t_k) \mathscr{C}_f^T(t_k)\right\} I K_f^T(t_k) \\
&\quad + \kappa_8^{-1} n n_y \bar{\lambda} K_f(t_k) K_f^T(t_k) \\
&- \mathrm{sym}\left\{\mathbb{E}\{K_f(t_k)\mathcal{S}(t_k)\mathcal{T}^T(t_k)K_f^T(t_k)\}\right\} \\
&\leq \kappa_9 K_f(t_k) \mathrm{tr}\left\{\mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k)\right\} I K_f^T(t_k) \\
&\quad + \kappa_9^{-1} n n_y \bar{\lambda} K_f(t_k) K_f^T(t_k).
\end{aligned}
$$

Summarizing the above discussions, we have

$$
\begin{aligned}
P(t_{k+1}) \leq\ & \tau_1 \mathcal{M}(t_k) P(t_k) \mathcal{M}^T(t_k) + \tau_2 \mathcal{N}(t_k) W(t_k) \mathcal{N}^T(t_k) \\
& + \tau_3 K_f(t_k) \mathrm{tr}\left\{\mathscr{C}_f(t_k) P(t_k) \mathscr{C}_f^T(t_k)\right\} I K_f^T(t_k) \\
& + \tau_4 K_f(t_k) \mathrm{tr}\left\{\mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k)\right\} I K^T(t_k) \\
& + \tau_5 n n_y \bar{\lambda} K_f(t_k) K_f^T(t_k).
\end{aligned} \tag{26}
$$

It can be noticed that the constraints of Lemma 2 are all fulfilled based on (19) and (26). Therefore, from the above analysis, we have

$$
P(t_{k+1}) \leq \Sigma(t_{k+1}). \tag{27}
$$

In Theorem 1, the upper bound $\Sigma(t_{k+1})$ of the filtering error covariance $P(t_{k+1})$ is presented. Next, we will give the following theorem, which demonstrates the approach to parameterize the filter gain by utilizing the obtained upper bound.

To proceed, we denote notations as follows:

$$
\begin{cases}
\mathcal{U}(t_k) = \tau_1 \mathscr{A}_f(t_k)\Sigma(t_k)\mathscr{C}_f^T(t_k) + \tau_2 \mathscr{B}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k) \\
\mathcal{V}(t_k) = \tau_1 \mathscr{C}_f(t_k)\Sigma(t_k)\mathscr{C}_f^T(t_k) + \tau_2 \mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k) \\
\qquad\quad + \tau_3 \mathrm{tr}\left\{\mathscr{C}_f(t_k)\Sigma(t_k)\mathscr{C}_f^T(t_k)\right\} I \\
\qquad\quad + \tau_4 \mathrm{tr}\left\{\mathscr{D}_f(t_k) W(t_k) \mathscr{D}_f^T(t_k)\right\} I + \tau_5 n n_y \bar{\lambda}
\end{cases} \tag{28}
$$

where τ_i $(i = 1, 2)$ has been defined in Theorem 1. ■

Theorem 2: The upper bound $\Sigma(t_k)$ in Theorem 1 can be minimized through designing the filter gain matrix $K_f(t_k)$, which satisfies the following form:

$$
K_f(t_k) = \mathcal{U}(t_k)\mathcal{V}^{-1}(t_k). \tag{29}
$$

Moreover, the minimal upper bound for the filtering error covariance can be obtained as

$$
\begin{aligned}
\Sigma(t_{k+1}) =\ & \tau_1 \mathscr{A}_f(t_k)\Sigma(t_k)\mathscr{A}_f^T(t_k) + \tau_2 \mathscr{B}_f(t_k) W(t_k) \\
& \times \mathscr{B}_f^T(t_k) - \mathcal{U}(t_k)\mathcal{V}^{-1}(t_k)\mathcal{U}^T(t_k).
\end{aligned} \tag{30}
$$

Proof: Based on (19), by taking the partial derivative of $\mathrm{tr}\{\Sigma(t_{k+1})\}$ with respect to the gain matrix $K_f(t_k)$, it can be computed that

$$
\begin{aligned}
&\frac{\partial \mathrm{tr}\left\{\Sigma(t_{k+1})\right\}}{\partial K_f(t_k)} \\
&= 2\{\tau_1[-\mathscr{A}_f(t_k)P(t_k)\mathscr{C}_f^T(t_k) + K_f(t_k)\mathscr{C}_f(t_k)P(t_k) \\
&\quad \times \mathscr{C}_f^T(t_k)] + \tau_2[-\mathscr{B}_f(t_k)W(t_k)\mathscr{D}_f^T(t_k) + K_f(t_k)\mathscr{D}_f(t_k) \\
&\quad \times W(t_k)\mathscr{D}_f^T(t_k)] + \tau_3 K_f(t_k)\mathrm{tr}\{\mathscr{C}_f(t_k)P(t_k)\mathscr{C}_f^T(t_k)\} I \\
&\quad + \tau_4 K_f(t_k)\mathrm{tr}\{\mathscr{D}_f(t_k)W(t_k)\mathscr{D}_f^T(t_k)\} I + \tau_5 n n_y \bar{\lambda} K_f(t_k)\}.
\end{aligned} \tag{31}
$$

Letting $\partial \mathrm{tr}\{\Sigma(t_{k+1})\}/\partial K_f(t_k) = 0$, based on (28), we can easily obtain $K_f(t_k)\mathcal{V}(t_k) = \mathcal{U}(t_k)$. It is obvious that $\mathcal{V}(t_k)$ is a positive-definite matrix. Therefore, we can compute the filter parameters as follows:

$$
K_f(t_k) = \mathcal{U}(t_k)\mathcal{V}^{-1}(t_k) \tag{32}
$$

and the minimum of $\Sigma(t_{k+1})$ is shown in (30), which completes the entire proof of Theorem 2. ■

According to the above results, the upper bound of the filtering error covariance has been first obtained in Theorem 1, and then the optimal filter parameter has been calculated in Theorem 2. The proposed outlier-resistant recursive security filtering algorithm is presented in Algorithm 1. Compared with the existing literature, this scheme is different in the following ways. 1) The multirate strategy is introduced in the system model for different system components, according to the importance of their signals, and fading measurements as well as cyberattacks are taken into consideration in the construction of the system. 2) The RRP is employed in the sensor-to-filter channel, thereby reducing the data congestion and collisions. 3) An outlier-resistant filter is developed to restrain measurement outliers from devastating the filtering accuracy.

Algorithm 1: Outlier-Resistant Recursive Security Filtering Algorithm.

Step 1. Give positive scalar τ_i $(i = 1, 2, \ldots, 5)$, the maximum step M and set the initial conditions $k = 0, \hat{x}(t_0) = \mathbb{E}\{\bar{x}(t_0)\}, \Sigma(t_0) = P(t_0)$.
Step 2. Compute filter gain $K_f(t_k)$ for the time step k according to (29).
Step 3. Calculate $\hat{x}(t_{k+1})$ for the filter based on its structure (14).
Step 4. In the light of (19), derive the filtering error covariance upper bound $\Sigma(t_k)$. Set $k = k + 1$.
Step 5. If $k < M$, then go to Step 2, else go to Step 6.
Step 6. Stop.

In the following part of this section, we will investigate the boundedness of the filtering error dynamics (20) with its filter parameter (29).

Theorem 3: Consider the discrete time-varying MRNS (1) and the filter (14), whose gain is (29), and the dynamic of filtering error (20) is exponentially bounded in mean square sense under Assumption 2.

Proof: Based on (12) and (14), the filtering error (20) is rewritten as

$$\tilde{x}(t_{k+1}) = \mathscr{A}_f(t_k)\tilde{x}(t_k) + \mathscr{B}_f(t_k)\omega(t_k) - K_f(t_k)\sigma(\mathcal{Y}(t_k)).$$

Combining Assumption 2 and (29), it is derived that

$$\mathcal{U}(t_k) \leq \tau_1 \mathscr{A}_f(t_k)\Sigma(t_k)\mathscr{C}_f^T(t_k)$$
$$\mathcal{V}^{-1}(t_k) \leq \left[\tau_1 \mathscr{C}_f(t_k)\Sigma(t_k)\mathscr{C}_f^T(t_k)\right]^{-1}.$$

Therefore

$$\begin{aligned}
&\|\mathbb{E}\{K_f(t_k)K_f^T(t_k)\}\| \\
&\leq \|\mathbb{E}\{\mathscr{A}_f(t_k)\mathscr{C}_f^{-1}(t_k)(\mathscr{A}_f(t_k)\mathscr{C}_f^{-1}(t_k))^T\}\| \\
&\leq \frac{\bar{a}^2}{\underline{c}^2} := k.
\end{aligned}$$

According to the characteristic of the saturation function $\sigma(\mathcal{Y}(t_k))$ and the definition of the matrix trace and norm, one has

$$\begin{aligned}
&\mathbb{E}\left\{\sigma(\mathcal{Y}(t_k))\sigma^T(\mathcal{Y}(t_k))\right\} \leq \mathbb{E}\left\{\text{tr}\{\sigma(\mathcal{Y}(t_k))\sigma^T(\mathcal{Y}(t_k))\}I\right\} \\
&\leq \mathbb{E}\left\{\text{tr}\left\{\text{diag}_{nn_y}\{u_{i,\max}^2\}\right\} I\right\} \\
&= \bar{\lambda} I_{nn_y} \\
&\mathbb{E}\left\{(\mathscr{B}_f(t_k)\omega(t_k))^T(\mathscr{B}_f(t_k)\omega(t_k))\right\} \\
&= \mathbb{E}\left\{\text{tr}\left\{\mathscr{B}_f(t_k)\omega(t_k)\omega^T(t_k)\mathscr{B}_f^T(t_k)\right\}\right\} \\
&= \text{tr}\left\{\mathscr{B}_f(t_k)W(t_k)\mathscr{B}_f^T(t_k)\right\} \\
&\leq (gn_x + nn_y)\bar{w}\bar{b}^2 := l
\end{aligned}$$

and

$$\begin{aligned}
&\mathbb{E}\left\{(K_f(t_k)\sigma^T(\mathcal{Y}(t_k)))(K_f(t_k)\sigma(\mathcal{Y}(t_k)))\right\} \\
&\leq \bar{\lambda}(gn_x + nn_y)\lambda_{\max}\left(\mathbb{E}\{K_f(t_k)K^T(t_k)\}\right) \\
&= \bar{\lambda}(gn_x + nn_y)\|\mathbb{E}\{K_f(t_k)K^T(t_k)\}\| \\
&= \bar{\lambda}(gn_x + nn_y)k := m
\end{aligned}$$

where $\lambda_{\max}(\mathbb{E}\{K_f(t_k)K^T(t_k)\})$ represents the maximal eigenvalues of $K_f(t_k)K^T(t_k)$. ":=" means "defined as," which is used to define a new symbol.

Next, for any scalar $\bar{\varepsilon} > 0$ and matrix $\Theta(t_k) > 0$, consider the following iterative matrix equation:

$$\begin{aligned}
\Theta(t_{k+1}) = {} & \mathscr{A}_f(t_k)\Theta(t_k)\mathscr{A}_f^T(t_k) \\
& + \mathscr{B}_f(t_k)W(t_k)\mathscr{B}_f^T(t_k) + \bar{\varepsilon}I
\end{aligned} \tag{33}$$

with the initial value being

$$\Theta(t_0) = \mathscr{B}_f(t_k)W(t_0)\mathscr{B}_f^T(t_k) + \bar{\varepsilon}I. \tag{34}$$

Therefore, we have

$$\begin{aligned}
\|\Theta(t_{k+1})\| \leq {} & \|\mathscr{A}_f(t_k)\|^2\|\Theta(t_k)\| \\
& + \|\mathscr{B}_f(t_k)W(t_k)\mathscr{B}_f^T(t_k)\| + \|\bar{\varepsilon}I\| \\
\leq {} & \bar{a}^2\|\Theta(t_k)\| + \bar{b}^2\bar{w} + \bar{\varepsilon}.
\end{aligned}$$

By iterative calculation, one has that

$$\begin{aligned}
\|\Theta(t_k)\| &\leq \bar{a}^{2k}\|\Theta(t_0)\| + (\bar{b}^2 + \bar{\varepsilon})\sum_{t=0}^{k-1}\bar{a}^{2t} \\
&\leq \|\Theta(t_0)\| + (\bar{b}^2\bar{w} + \bar{\varepsilon})\sum_{t=0}^{\infty}\bar{a}^{2t} \\
&= \|\Theta(t_0)\| + \frac{\bar{b}^2\bar{w} + \bar{\varepsilon}}{1 - \bar{a}^2}.
\end{aligned}$$

In light of $\Theta(t_k) \geq \bar{\varepsilon}I$, then, for all $k \geq 0$, there exists a positive scalar $\bar{\theta}$ such that

$$\bar{\varepsilon}I \leq \Theta(t_k) \leq \bar{\theta}I \tag{35}$$

holds where

$$\bar{\theta} = \|\Theta(t_0)\| + \frac{\bar{b}^2\bar{w} + \bar{\varepsilon}}{1 - \bar{a}^2}. \tag{36}$$

Define

$$\Omega(t_k) = \tilde{x}^T(t_k)\Theta^{-1}(t_k)\tilde{x}(t_k) \tag{37}$$

then, for an arbitrary positive scalar υ, we have

$$\begin{aligned}
&\mathbb{E}\left\{\Omega(t_{k+1})\right\} - (1 + \upsilon)\Omega(t_k) \\
&\leq (1 + \upsilon)\mathbb{E}\{\tilde{x}^T(t_k)(\mathscr{A}_f^T(t_k)\Theta^{-1}(t_{k+1})\mathscr{A}_f(t_k) \\
&\quad - \Theta^{-1}(t_{k+1}))\tilde{x}(t_k)\} + (1 + \upsilon^{-1})\mathbb{E}\{(K_f(t_k)\sigma(\mathcal{Y}(t_k)))^T \\
&\quad \times \Theta^{-1}(t_{k+1})(K_f(t_k)\sigma(\mathcal{Y}(t_k)))\} + \mathbb{E}\{(\mathscr{B}_f(t_k)\omega(t_k))^T \\
&\quad \times \Theta^{-1}(t_{k+1})(\mathscr{B}_f(t_k)\omega(t_k))\}.
\end{aligned} \tag{38}$$

For convenience of expression, we define

$$\mathcal{Z}(t_k) = \mathscr{B}_f(t_k)W(t_k)\mathscr{B}_f^T(t_k) + \bar{\varepsilon}I.$$

By resorting to the fundamental matrix inversion lemma and (33), it follows that:

$$\mathscr{A}_f^T(t_k)\Theta^{-1}(t_{k+1})\mathscr{A}_f(t_k) - \Theta^{-1}(t_k)$$

$$
\begin{aligned}
&= \mathscr{A}_f^T(t_k)((\mathscr{A}_f(t_k)\Theta(t_k)\mathscr{A}_f^T(t_k))^{-1} \\
&\quad + \mathcal{Z}^{-1}(t_k))\mathscr{A}_f(t_k) - \Theta^{-1}(t_k) \\
&= (\Theta(t_k) + \mathscr{A}_f^{-1}(t_k)\mathcal{Z}(t_k)(\mathscr{A}_f^T(t_k))^{-1})^{-1} - \Theta^{-1}(t_k) \\
&= (\Theta(t_k) + \mathscr{A}_f^{-1}(t_k)\mathcal{Z}(t_k)(\mathscr{A}_f^T(t_k))^{-1})^{-1} \\
&\quad \times (I - (\Theta(t_k) + \mathscr{A}_f^{-1}(t_k)\mathcal{Z}(t_k)(\mathscr{A}_f^T(t_k))\Theta^{-1}(t_k)) \\
&= (\mathscr{A}_f^T(t_k)\mathcal{Z}^{-1}(t_k)\mathscr{A}_f(t_k)\Theta(t_k) + I)^{-1}\Theta^{-1}(t_k)) \\
&\leq \left(\frac{\bar{a}^2\bar{\theta}}{\underline{b}^2\underline{w}} + 1\right)^{-1} \Theta^{-1}(t_k). \qquad (39)
\end{aligned}
$$

Combining (37), (38), and (39), it is derived that

$$
\begin{aligned}
&\mathbb{E}\{\Omega(t_{k+1})\} - (1+\upsilon)\Omega(t_k) \\
&\leq -(1+\upsilon)\left(\frac{\bar{a}^2\bar{\theta}}{\underline{b}^2\underline{w}} + 1\right)^{-1} \mathbb{E}\{\Omega(t_k)\} + (1+\upsilon^{-1})\frac{m}{\bar{\varepsilon}} + \frac{l}{\bar{\varepsilon}}. \qquad (40)
\end{aligned}
$$

Accordingly, we can always find an appropriate positive scalar υ, which guarantees $\varpi \in (0,1)$ and $0 < \frac{\xi\bar{\theta}}{1-\varpi} < 1$, then, (40) can be rearranged as

$$
\mathbb{E}\{\Omega(t_{k+1})\} \leq \varpi\mathbb{E}\{\Omega(t_k)\} + \xi \qquad (41)
$$

where

$$
\varpi = (1+\upsilon)\left(1 - \left(\frac{\bar{a}^2\bar{\theta}}{\underline{b}^2\underline{w}} + 1\right)^{-1}\right)
$$

$$
\xi = (1+\upsilon^{-1})\frac{m}{\bar{\varepsilon}} + \frac{l}{\bar{\varepsilon}}.
$$

Substituting (37) for (41), we get

$$
\begin{aligned}
\mathbb{E}\{\|\tilde{x}(t_{k+1})\|^2\} &\leq \frac{\|\Theta(t_{k+1})\|}{\|\Theta(t_k)\|}\mathbb{E}\{\|\tilde{x}(t_k)\|^2\}\varpi \\
&\quad + \|\Theta(t_{k+1})\|\xi. \qquad (42)
\end{aligned}
$$

Substituting (35) into (42), by recursive operation, one has

$$
\begin{aligned}
\mathbb{E}\{\|\tilde{x}(t_{k+1})\|^2\} &\leq \frac{\bar{\theta}}{\bar{\varepsilon}}\mathbb{E}\{\|\tilde{x}(t_0)\|^2\}\varpi^{k+1} + \xi\bar{\theta}\sum_{t=0}^{k}\varpi^t \\
&\leq \frac{\bar{\theta}}{\bar{\varepsilon}}\mathbb{E}\{\|\tilde{x}(t_0)\|^2\}\varpi^{k+1} + \xi\bar{\theta}\sum_{t=0}^{\infty}\varpi^t \\
&= \frac{\bar{\theta}}{\bar{\varepsilon}}\mathbb{E}\{\|\tilde{x}(t_0)\|^2\}\varpi^{k+1} + \frac{\xi\bar{\theta}}{1-\varpi}. \qquad (43)
\end{aligned}
$$

According to Definition 1, we confirm that the dynamic of the filtering error $\tilde{x}(t_k)$ is exponentially bounded in the mean square sense. ■

Remark 6: The upper bound of filtering error covariance obtained by the method utilized in Theorem 1 of this article is less conservative, in comparison with the approach used in [54]. Besides, it is worth noting that due to energy constraints, the spectral norm of $\mathscr{A}_f(t_k)$, the variances of $\mathscr{B}_f(t_k), \mathscr{C}_f(t_k), \mathscr{D}_f(t_k)$, and the noise covariance matrix $W(t_k)$ are all bounded in practical application as shown in Assumption 2.

IV. Numerical Illustrative Example

In this section, the effectiveness and applicability of the proposed outlier-resistant recursive security filtering design method is validated via a numerical simulation example.

Consider the discrete time-varying MRNS (1) which is measured by three sensors, with parameters shown as follows:

$$
A(T_k) = \begin{bmatrix} 0.97 + 0.2\cos(T_k) & 0.52 - 0.1\sin(T_k) \\ -0.08 & 0.57 + 0.2\cos(T_k) \end{bmatrix}
$$

$$
B(T_k) = [0.08 \ \ 0.06]^T
$$

$$
C_1(t_k) = \begin{bmatrix} 7\sin(t_k) & 8\cos(t_k) \end{bmatrix}, \ D_1(t_k) = 0.95\sin(t_k)
$$

$$
C_2(t_k) = \begin{bmatrix} 8\sin(t_k) & 7\cos(t_k) \end{bmatrix}, \ D_2(t_k) = \sin(t_k)
$$

$$
C_3(t_k) = \begin{bmatrix} 9\sin(t_k) & 5\cos(t_k) \end{bmatrix}, \ D_3(t_k) = 0.25\sin(t_k).
$$

The process noise $w(T_k)$ and measurement noise $v_i(t_k)$ $(i = 1,2,3)$ are zero-mean Gaussian white noises with covariance $Q(T_k) = 0.05, V_1(t_k) = 0.03, V_2(t_k) = 0.05, V_3(t_k) = 0.04$. The relationship of H and h satisfies $H = 2h$, and we assume that $H = 2, h = 1$ in this simulation part. The measurement attenuation coefficient $\lambda_i(t_k)$, which is uniformly distributed over segments $(0.4 + 0.1i, 1)$ for $i = 1,2,3,4$, respectively.

In this example, the probability $\bar{\mu}$ of the deception attacks is selected as 0.3, and the saturation levels are $u_{1,\max} = 10$, $u_{2,\max} = 20$ and $u_{3,\max} = 15$. Set the initial values of the state as $x(t_0) = [2 \ -2]^T$ and the covariance as $P(t_0) = 0$. Let $\text{MSE}(t_k)$ denote the mean square error of the estimate, which is defined by

$$
\text{MSE}(t_k) = \frac{1}{M}\sum_{j=1}^{M}\sum_{i=1}^{2}\left(\bar{x}_i^{(j)}(t_k) - \hat{x}_i^{(j)}(t_k)\right)^2.
$$

In order to avoid one-time occasionality, 100 Monte Carlo tests are conducted, in other words, $M = 100$. Then, according to Algorithm 1, filter gain and the minimal upper bound of filtering error covariance are successively obtained.

Considering cyberattacks or any other network-induced problems, the occurrence of measurement outliers may lead to innovation changes and then degenerate or even damage the filter. Therefore, in order to testify the ability of the proposed filtering scheme against fading measurements, deception attacks, and measurement outliers, the following ordinary filter (44) is designed and compared with the proposed filter (14) experimentally [8]:

$$
\hat{x}(t_{k+1}) = \mathscr{A}_f(t_k)\hat{x}(t_k) + K(t_k)\mathcal{Y}(t_k) \qquad (44)
$$

where $K(t_k)$ is the filter gain. We assume that measurement outliers are characterized by white Gaussian noises with a covariance of 20 000. The measurement outliers occur intermittently, and the occurrence period of this outlier is $4h$. Also, it is supposed that there are no outliers at the initial time instant 0.

The simulation results are presented in Figs. 3–7. Specifically, Fig. 3 shows the estimate of the proposed outlier-resistant recursive security filter and the ordinary filter on the system state

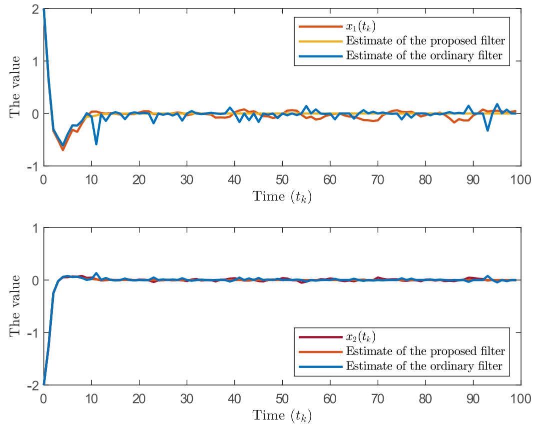

Fig. 3. $x(t_k)$ and its estimate.

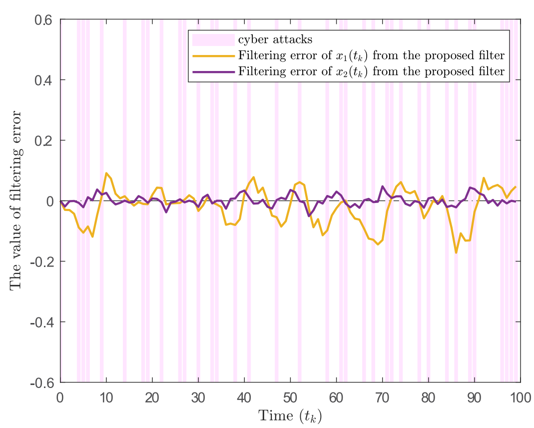

Fig. 4. Filtering error of the proposed filter.

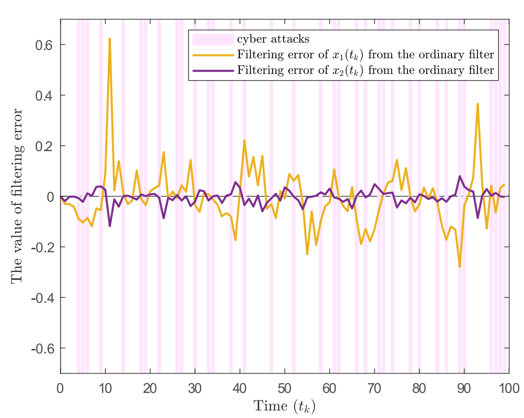

Fig. 5. Filtering error of the ordinary filter.

trajectories. It can be seen from this figure that the estimation effect of the proposed filter is better than that of the ordinary filter.

The error between the state $x(t_k)$ and its estimate of the proposed outlier-resistant filter and the ordinary filter under the influence of deception attacks, is displayed in Figs. 4 and 5, respectively. As can be seen from these two figures, what they

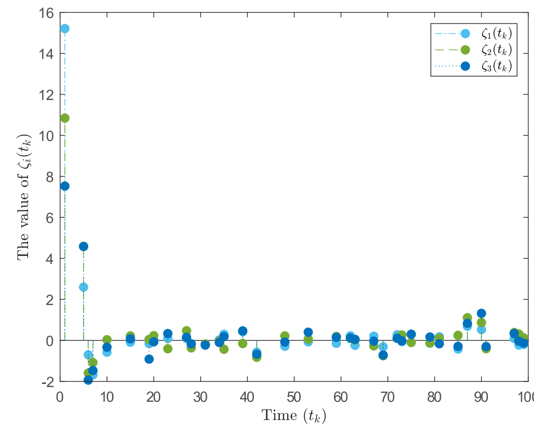

Fig. 6. Value of $\zeta_i(t_k)$.

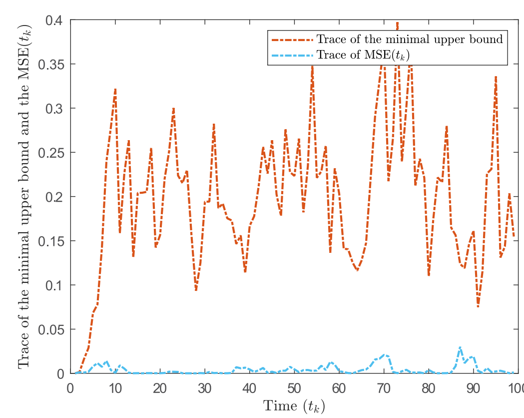

Fig. 7. Trace of the minimal upper bound and the MSE with the proposed filtering scheme.

have in common is that the estimation error is relatively small at the time when no attack occurs, while under the influence of malicious attacks, the estimate value will suddenly deviate from the normal value $x(t_k)$, resulting in a large error value. The difference is that the estimation error of the proposed outlier-resistant recursive security filter is about -0.1 to 0.1, which is smaller than that of the ordinary filter. The estimation error of the ordinary filter is approximately between -0.3 and 0.62. To facilitate the understanding of the effectiveness of the proposed filter and the detail of deception attacks, we give the value of the false signal sent by the attacker to the sensors when attacks occur, which is shown in Fig. 6.

In addition, Fig. 7 depicts the trace of the minimal upper bound on the covariance of the filtering error and the MSE of the proposed security outlier-resistant filtering scheme. In this figure, it can be seen that the trace of mean square errors is always below the trace of the upper bound, which conforms to our expectation.

According to the simulation results obtained, we can get the conclusion that, in the presence of measurement outliers, the proposed filter performs well and can effectively suppress the influence of measurement outliers. Compared with the filter proposed in this article, the estimate of the ordinary filter deviates from the system state and the estimation error is relatively large. Therefore, the robustness of the proposed filter to the fading measurements, cyberattacks, and measurement outliers is truly effective.

V. Conclusion

This article is concerned with outlier-resistant recursive filtering problems for RRP-based MRNSs with fading measurements and cyberattacks. Facilitated by the lifting technique, the subsequent processing can be easily tackled while the sampling period of the sensors differs from the plant update period of the system. Measurement outputs from sensors are likely to decay in a random way due to the complex and volatile environments. We assume that the signals in the sensor-to-filter channel may be modified by randomly occurring cyberattacks and orchestrated by RRP. A novel outlier-resistant filter design method is presented in order to restrain the abnormal innovations and ensure the reliability of the filter. Moreover, an upper bound for the filtering error covariance, which can be minimized by designing proper filter gain at each time step, has been derived via applying the matrix operation and using the properties of the trace of the matrix. In addition, the exponential boundedness of the filtering error dynamics has been analyzed in the mean square sense. Finally, a numerical simulation example has been exploited to demonstrate the feasibility and effectiveness of the proposed algorithm. Related topics for future research include the distributed outlier-resistant recursive filtering problems for MRNSs over sensor networks, and the outlier-resistant filtering fusion problems for MRNSs with network-induced phenomena.

References

[1] J. Li, Z. Wang, H. Dong, and X. Yi, "Outlier-resistant observer-based control for a class of networked systems under encoding-decoding mechanism," *IEEE Syst. J.*, vol. 16, no. 1, pp. 922–932, Mar. 2022.

[2] Y. Cui, Y. Liu, W. Zhang, and F. E. Alsaadi, "Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 51, no. 1, pp. 561–573, Jan. 2021.

[3] M. Ma, T. Wang, J. Qiu, and H. R. Karimi, "Adaptive fuzzy decentralized tracking control for large-scale interconnected nonlinear networked control systems," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 10, pp. 3186–3191, Oct. 2021.

[4] L. Hu, Z. Wang, and X. Liu, "Dynamic state estimation of power systems with quantization effects: A recursive filter approach," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1604–1614, Aug. 2016.

[5] L. Ma, Z. Wang, Q.-L. Han, and H.-K. Lam, "Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks," *IEEE Sensors J.*, vol. 17, no. 7, pp. 2279–2288, Apr. 2017.

[6] Y. Shen, Z. Wang, H. Dong, and H. Liu, "Multi-sensor multi-rate fusion estimation for networked systems: Advances and perspectives," *Inf. Fusion*, vol. 82, pp. 19–27, 2022.

[7] W. Song, Z. Wang, J. Wang, F. E. Alsaadi, and J. Shan, "Distributed auxiliary particle filtering with diffusion strategy for target tracking: A dynamic event-triggered approach," *IEEE Trans. Signal Process.*, vol. 69, pp. 328–340, Jan. 2021.

[8] Y. Shen, Z. Wang, B. Shen, and H. Dong, "Outlier-resistant recursive filtering for multisensor multirate networked systems under weighted try-once-discard protocol," *IEEE Trans. Cybern.*, vol. 51, no. 10, pp. 4897–4908, Oct. 2021.

[9] P. Frogerais, J.-J. Bellanger, and L. Senhadji, "Various ways to compute the continuous-discrete extended Kalman filter," *IEEE Trans. Autom. Control*, vol. 57, no. 4, pp. 1000–1004, Apr. 2012.

[10] S. Liu, Z. Wang, Y. Chen, and G. Wei, "Protocol-based unscented Kalman filtering in the presence of stochastic uncertainties," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1303–1309, Mar. 2020.

[11] B. Shen, Z. Wang, D. Wang, and Q. Li, "State-saturated recursive filter design for stochastic time-varying nonlinear complex networks under deception attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 10, pp. 3788–3800, Oct. 2020.

[12] 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.

[13] X. Li, F. Han, N. Hou, H. Dong, and H. Liu, "Set-membership filtering for piecewise linear systems with censored measurements under round-robin protocol," *Int. J. Syst. Sci.*, vol. 51, no. 9, pp. 1578–1588, 2020.

[14] J. Salt, J. Alcaina, Ángel Cuenca, and A. Baños, "Multirate control strategies for avoiding sample losses: Application to UGV path tracking," *ISA Trans.*, vol. 101, pp. 130–146, 2020.

[15] N. Davari and A. Gholami, "Variational Bayesian adaptive Kalman filter for asynchronous multirate multi-sensor integrated navigation system," *Ocean Eng.*, vol. 174, pp. 108–116, 2019.

[16] H. Geng, Y. Liang, Y. Liu, and F. E. Alsaadi, "Bias estimation for asynchronous multi-rate multi-sensor fusion with unknown inputs," *Inf. Fusion*, vol. 39, pp. 139–153, 2018.

[17] S. Liu, Z. Wang, G. Wei, and M. Li, "Distributed set-membership filtering for multirate systems under the round-robin scheduling over sensor networks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1910–1920, May 2020.

[18] S. Liu, Z. Wang, L. Wang, and G. Wei, "Recursive set-membership state estimation over a FlexRay network," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 52, no. 6, pp. 3591–3601, Jun. 2022.

[19] C. Wen, Z. Wang, J. Hu, Q. Liu, and F. E. Alsaadi, "Recursive filtering for state-saturated systems with randomly occurring nonlinearities and missing measurements," *Int. J. Robust Nonlinear Control*, vol. 28, no. 5, pp. 1715–1727, 2018.

[20] Y. Yin, W. Yu, X. Bu, and Q. Yu, "Security data-driven iterative learning control for unknown nonlinear systems with hybrid attacks and fading measurements," *ISA Trans.*, vol. 129, pp. 1–12, 2022.

[21] X. Li, G. Wei, and L. Wang, "Distributed set-membership filtering for discrete-time systems subject to denial-of-service attacks and fading measurements: A zonotopic approach," *Inf. Sci.*, vol. 547, pp. 49–67, 2021.

[22] F. Yang, J. Li, H. Dong, and Y. Shen, "Proportional–integral-type estimator design for delayed recurrent neural networks under encoding–decoding mechanism," *Int. J. Syst. Sci.*, vol. 53, no. 13, pp. 2729–2741, 2022.

[23] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.

[24] J. Liu, T. Yin, J. Cao, D. Yue, and H. R. Karimi, "Security control for T–S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 51, no. 10, pp. 6544–6554, Oct. 2021.

[25] Z. Wu, E. Tian, and H. Chen, "Covert attack detection for LFC systems of electric vehicles: A dual time-varying coding method," *IEEE/ASME Trans. Mechatronics*, early access, Sep. 9, 2022, doi: 10.1109/TMECH.2022.3201875.

[26] Z. Wang, D. Wang, B. Shen, and F. E. Alsaadi, "Centralized security-guaranteed filtering in multirate-sensor fusion under deception attacks," *J. Franklin Inst.*, vol. 355, no. 1, pp. 406–420, 2018.

[27] D. Xu, S. Zhu, E. Tian, and J. Liu, "An adaptive torus-event-based H_∞ controller design for networked T-S fuzzy systems under deception attacks," *Int. J. Robust Nonlinear Control*, vol. 32, no. 6, pp. 3425–3441, 2022.

[28] F. Qu, E. Tian, and X. Zhao, "Chance-constrained H_∞ state estimation for recursive neural networks under deception attacks and energy constraints: The finite-horizon case," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Jan. 7, 2022, doi: 10.1109/TNNLS.2021.3137426.

[29] N. Zhao, P. Shi, W. Xing, and J. Chambers, "Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 158–167, Mar. 2021.

[30] C. Deng and C. Wen, "Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 3, pp. 1308–1318, Sep. 2020.

[31] J. Liu, Y. Dong, L. Zha, E. Tian, and X. Xie, "Event-based security tracking control for networked control systems against stochastic cyber-attacks," *Inf. Sci.*, vol. 612, pp. 306–321, 2022.
[32] J. Zhang, J. Sun, and H. Lin, "Optimal DoS attack schedules on remote state estimation under multi-sensor round-robin protocol," *Automatica*, vol. 127, 2021, Art. no. 109517.
[33] J. Cao, D. Ding, J. Liu, E. Tian, and X. Xie, "Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks," *Inf. Sci.*, vol. 548, no. 10, pp. 69–84, 2021.
[34] J. Liu, T. Yin, D. Yue, H. R. Karimi, and J. Cao, "Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 162–173, Jan. 2021.
[35] K. Liu, H. Guo, Q. Zhang, and Y. Xia, "Distributed secure filtering for discrete-time systems under round-robin protocol and deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3571–3580, Aug. 2020.
[36] W. Song, Z. Wang, J. Wang, and J. Shan, "Particle filtering for a class of cyber-physical systems under round-robin protocol subject to randomly occurring deception attacks," *Inf. Sci.*, vol. 544, pp. 298–307, 2021.
[37] D. Ding, Z. Wang, and Q.-L. Han, "Neural-network-based output-feedback control with stochastic communication protocols," *Automatica*, vol. 106, pp. 221–229, 2019.
[38] L. Zou, Z. Wang, Q.-L. Han, and D. Zhou, "Ultimate boundedness control for networked systems with try-once-discard protocol and uniform quantization effects," *IEEE Trans. Autom. Control*, vol. 62, no. 12, pp. 6582–6588, Dec. 2017.
[39] J. Li, Z. Wang, H. Dong, and G. Ghinea, "Outlier-resistant remote state estimation for recurrent neural networks with mixed time-delays," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 5, pp. 2266–2273, May 2021.
[40] H. Geng, Z. Wang, A. Mousavi, F. E. Alsaadi, and Y. Cheng, "Outlier-resistant filtering with dead-zone-like censoring under try-once-discard protocol," *IEEE Trans. Signal Process.*, vol. 70, pp. 714–728, Jan. 2022.
[41] J. Sun, B. Shen, and Y. Liu, "A resilient outlier-resistant recursive filtering approach to time-delayed spatial–temporal systems with energy harvesting sensors," *ISA Trans.*, vol. 127, pp. 41–49, 2022.
[42] D. Zhao, Z. Wang, G. Wei, and Q.-L. Han, "A dynamic event-triggered approach to observer-based PID security control subject to deception attacks," *Automatica*, vol. 120, 2020, Art. no. 109128.
[43] X.-M. Zhang et al., "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 1, pp. 1–17, Jan. 2020.
[44] F. Wang, Z. Wang, J. Liang, and C. Silvestre, "A recursive algorithm for secure filtering for two-dimensional state-saturated systems under network-based deception attacks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 678–688, Mar./Apr. 2022.
[45] D. Shi, R. J. Elliott, and T. Chen, "On finite-state stochastic modeling and secure estimation of cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 65–80, Jan. 2017.
[46] X. Li, G. Wei, D. Ding, and S. Liu, "Recursive filtering for time-varying discrete sequential systems subject to deception attacks: Weighted try-once-discard protocol," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 52, no. 6, pp. 3704–3713, Jun. 2022.
[47] 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.
[48] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, and J. Cao, "Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13800–13808, Dec. 2022.
[49] H. Gao, H. Dong, Z. Wang, and F. Han, "Recursive minimum-variance filter design for state-saturated complex networks with uncertain coupling strengths subject to deception attacks," *IEEE Trans. Cybern.*, vol. 52, no. 10, pp. 11121–11132, Oct. 2022.
[50] F. Wang, Z. Wang, J. Liang, and X. Liu, "Resilient filtering for linear time-varying repetitive processes under uniform quantizations and round-robin protocols," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 65, no. 9, pp. 2992–3004, Sep. 2018.
[51] D. G. Meyer, "A new class of shift-varying operators, their shift-invariant equivalents, and multirate digital systems," *IEEE Trans. Autom. Control*, vol. 35, no. 4, pp. 429–433, Apr. 1990.
[52] D. De Palma and G. Indiveri, "Output outlier robust state estimation," *Int. J. Adapt. Control Signal Process.*, vol. 31, no. 4, pp. 581–607, 2016.
[53] B. Shen, Z. Wang, D. Wang, J. Luo, H. Pu, and Y. Peng, "Finite-horizon filtering for a class of nonlinear time-delayed systems with an energy harvesting sensor," *Automatica*, vol. 100, pp. 144–152, 2019.
[54] B. Shen, Z. Wang, D. Wang, and H. Liu, "Distributed state-saturated recursive filtering over sensor networks under round-robin protocol," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3605–3615, Aug. 2020.

Jinliang Liu (Member, IEEE) received the Ph.D. degree in control theory and control engineering from the School of Information Science and Technology, Donghua University, Shanghai, China, in 2011.

He was a Postdoctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from 2013 to 2016. He was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, University of Hong Kong, Hong Kong, from 2016 to 2017. He was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea, from 2017 to 2018. He is currently a Professor with the Nanjing University of Finance and Economics, Nanjing, China. His research interests include networked control systems, complex dynamical networks, and time-delay systems.

Enyu Gong received the B.S. degree in Internet of Things engineering from Jiangsu University, Zhenjiang, China, in 2021. She is currently working toward the M.S. degree in computer science and technology with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China.

Her research interests include fuzzy control, networked control systems, and secure state estimation.

Lijuan Zha received the Ph.D. degree in control science and engineering from Donghua University, Shanghai, China, in 2018.

She is currently an Associate Professor with the Nanjing University of Finance and Economics, Nanjing, China. She was also a Postdoctoral Research Associate with the School of Mathematics, Southeast University, Nanjing. Her current research interests include networked control systems, neural networks, and complex dynamical systems.

Xiangpeng Xie (Senior Member, IEEE) received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively.

From 2010 to 2014, he was a Senior Engineer with the Metallurgical Corporation of China Ltd., Beijing, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.

Prof. Xie serves as an Associate Editor for the *International Journal of Fuzzy Systems* and *International Journal of Control, Automation, and Systems*.

Engang Tian (Member, IEEE) received the B.S. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Postdoctoral Research Fellow with the Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, China, and joined the University of Shanghai for Science and Technology, Shanghai, where he is currently a Professor with the School of Optical-Electrical and Computer Engineering. He has authored or coauthored more than 100 papers in refereed international journals. His research interests include networked control systems, cyberattacks, as well as nonlinear stochastic control and filtering.