Particle Filtering for A Class of Cyber-Physical Systems under Round-Robin Protocol Subject to Randomly Occurring Deception Attacks

Weihao Song[a], Zidong Wang[b,c], Jianan Wang[a,*], Jiayuan Shan[a]

[a]*School of Aerospace Engineering, Beijing Institute of Technology, Beijing 100081, China.*
[b]*College of Electrical Engineering and Automation, Shandong University of Science and Technology, Qingdao 266590, China.*
[c]*Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom.*

Abstract

In this paper, the particle filtering problem is studied for a class of general nonlinear cyber-physical systems with non-Gaussian noises under Round-Robin protocol (RRP) subject to the randomly occurring deception attacks. In order to prevent the data from collisions and alleviate the communication overhead for the shared network with limited resources, the RRP is introduced in the sensor-to-filter channel to schedule the multiple sensors with a predefined transmission order. Under the RRP, only one sensor can be granted the access to the shared channel for measurement transmission at each time instant. A Bernoulli-distributed stochastic variable is utilized to describe the characteristic of random occurrence of deception attacks initiated by the adversaries. A RRP-based particle filtering algorithm is developed by establishing a modified likelihood function, where the statistical property of the randomly occurring deception attacks is exploited and the RRP-induced effect on the filter design is reflected. Finally, an illustrative example regarding the target tracking problem is provided to verify the feasibility and effectiveness of the developed particle filtering scheme.

Keywords: Particle filtering, cyber-physical systems, Round-Robin protocol, randomly occurring deception attacks, nonlinear systems, non-Gaussian noises.

1. Introduction

In the past few decades, the filtering problem for nonlinear systems has received considerable research interest due to its successful applications to a diverse range of practical domains including, but are not limited to, mathematical finance [4], target tracking and localization [7], induction motor drives [14] and satellite orbit estimation [18]. The general framework for nonlinear filtering has been established with the help of Bayesian estimation theory, which involves the recursive calculation of the Chapman-Kolmogorov equation and the Bayesian formula [30]. Unfortunately, it is quite difficult (if not impossible) to obtain an analytical solution in most cases (except for

[*] Corresponding author

Email addresses: 3120160034@bit.edu.cn (Weihao Song), Zidong.Wang@brunel.ac.uk (Zidong Wang), wangjianan@bit.edu.cn (Jianan Wang), sjy1919@bit.edu.cn (Jiayuan Shan)

the linear system with Gaussian noises) since the multidimensional integrals are required to be calculated. Therefore, much effort has been devoted to the development of approximate nonlinear filtering algorithms.

As one of the widely used approximate filtering approaches, the extended Kalman filtering (EKF) algorithm and its variations have attracted a great deal of research attention from both academia and industry [13, 17, 19]. However, a prerequisite for the effective utilization of the EKF algorithm is the availability/calculation of the Jacobian matrix for linearization, which is often impractical and therefore limits the application potentials especially when the system possesses high-degree of nonlinearity or discontinuity. For the purpose of seeking alternatives to the EKF algorithm, a large number of nonlinear filtering algorithms have been put forward with examples including the unscented Kalman filtering [16], the cubature Kalman filtering [1], and the sparse-grid based nonlinear filtering [15] techniques, all of which are capable of capturing the higher-order moments and achieving higher accuracy than the traditional EKF method. It should be pointed out that all the above-mentioned algorithms are inseparable from an underlying assumption that the considered systems undergo noisy disturbances that are of Gaussian types, and such an assumption is often unrealistic in most real-world cases. As such, the particle filtering technique has come into being for its distinctive advantages in dealing with the non-Gaussian systems [2, 21]. Up to now, many works related to the particle filtering have been published for various systems under various performance indices such as event-triggered mechanisms [20, 27], outlier-resistant schemes [26, 33], and some network-induced phenomena including delayed measurements [38], non-Gaussian fading measurements [22] and packet dropouts [35].

In practical applications of the cyber-physical systems (CPSs), it is often necessary for many components to operate (or communicate with others) via a shared communication network [6], and this renders more opportunities for the malicious attackers to hijack and falsify the measurement outputs (or control commands). Consequently, increasing research attention has recently been paid to the secure filtering/control problems against various security threats, and some typical examples include the deception attacks [9, 11], denial-of-service attacks [3, 12] and replay attacks [36]. Among them, the deception attacks are deemed to be one of the most hazardous attack types since the adversary can arbitrarily inject the false data to degenerate the filtering/control performance and even destabilize the whole system. As such, the filtering/control problem with deception attacks has been receiving some initial research attention and some elegant results have been reported. For example, the secure distributed finite-time filtering problem has been studied in [32] for the positive systems over sensor networks subject to the deception attacks.

In the context of the filtering problem, it is often the case that multiple sensors transmit their respective measurement outputs to the filter simultaneously [23]. Such simultaneous transmissions of massive data will inevitably give rise to the phenomenon of data collision in the communication network with limited communication capacity. In order to alleviate the data collision and guarantee the desired filtering performance, it is of vital importance to use certain rules/protocols to schedule the multiple sensors and utilize the limited network bandwidth in a reasonable way. Accordingly, a large amount of research results have recently been reported on the analysis and synthesis problems for networked systems under communication protocols such as Round-Robin protocol (RRP) [25], stochastic communication protocol [37] and weighted Try-Once-Discard protocol [29]. The common feature of these communication protocols is that only one sensor (or one component) can be granted the access to the transmission channel at each time, thereby ensuring the reliability and efficiency of the data transmission.

As a type of deterministic communication protocol, the well-known RRP has captured the everincreasing attention from researchers and has been frequently used in industry. The scheduling mechanism of a RRP is to grant each sensor the access to transmit its measurement output in a fixed circular order. By now, much research has been carried out on the RRP-based filtering problem [28, 24]. Nevertheless, to the best of the authors' knowledge, the particle filtering problem for general nonlinear/non-Gaussian CPSs under the RRP is far from being well addressed despite its practical significance, not to mention the case when the randomly occurring deception attacks also come into existence. In fact, the fundamental difficulties encountered in the particle filter design for CPSs under RRP lie in the following two aspects: 1) how to depict the communication protocol and deception attacks in the sequential Bayesian filtering framework in a rigorously mathematical way; and 2) how to calculate the likelihood function based on the scheduled and corrupted (if attacked successfully) measurements, and update the importance weights? The main motivation of this paper is therefore to provide satisfactory answers to these two questions.

Motivated by the above discussions, in this paper, the RRP-based particle filtering problem is investigated for a class of nonlinear/non-Gaussian CPSs subject to the randomly occurring deception attacks. The main contributions of this paper are highlighted as follows: 1) the particle filtering issue is addressed for the nonlinear/non-Gaussian CPSs in the simultaneous presence of the RRP and the randomly occurring deception attacks; 2) a modified likelihood function is explicitly derived by incorporating the probability information of the successfully launched deception attacks under the RRP; and 3) a protocol-based particle filtering algorithm is proposed, which is shown to be more efficient than its standard counterpart from both communication and computation perspectives, and has certain robustness against the deception attacks.

The rest of this paper is organized as follows. In Section 2, a mathematical description of the considered problem is formulated. The RRP-based particle filtering framework with randomly occurring deception attacks is established in Section 3. The simulation results are provided in Section 4 to demonstrate the effectiveness of the developed particle filtering algorithm. Finally, some concluding remarks are summarized in Section 5.

Notation. Throughout this paper, the notations used are fairly standard. Let $\mathbb{R}^n$ represent the n-dimensional Euclidean vector space. The superscript T denotes the operation of transpose and $\mathrm{mod}(u, v)$ denotes the modulo operation that returns the remainder after dividing u by v. $\mathrm{diag}\{d_1, d_2, \ldots, d_n\}$ represents a diagonal matrix with $d_1, d_2, \ldots, d_n$ being its diagonal elements. $p_x(\cdot)$ stands for the probability density function of a stochastic variable x and $P\{X\}$ denotes the occurrence probability of a discrete event X. $\mathcal{N}(x; \mu, \Sigma)$ represents the Gaussian probability density function of a stochastic variable x with mean μ and covariance Σ.

2. Problem Formulation and Preliminaries

Consider the following discrete-time nonlinear dynamic system:

$$x_{k+1} = f(x_k) + \omega_k \tag{1}$$

where $x_{k+1} \in \mathbb{R}^{n_x}$ is the state of the system at time instant $k+1$, $f(\cdot) : \mathbb{R}^{n_x} \mapsto \mathbb{R}^{n_x}$ denotes the state transition function, and $\omega_k \in \mathbb{R}^{n_x}$ represents the process noise satisfying $p_{\omega_k}(\cdot)$.

The measurement equation of the ith sensor is modelled by

$$y_k^i = h^i(x_k) + \nu_k^i, \qquad i = 1, 2, \cdots, N \tag{2}$$

where $y_k^i \in \mathbb{R}^{n_y}$ is the measurement output of the ith sensor at time instant k, $h^i(\cdot) : \mathbb{R}^{n_x} \mapsto \mathbb{R}^{n_y}$ denotes the measurement function of the ith sensor, and $\nu_k^i \in \mathbb{R}^{n_y}$ is the measurement noise on the ith sensor satisfying $p_{\nu_k^i}(\cdot)$.

In order to mitigate the data collision and reduce the consumption of network communication resources, the RRP is introduced in the sensor-to-filter channel to schedule the measurement transmission. Under the RRP, only the measurement output of one sensor can be transmitted to the filter at each time instant. Here, γ_k is used to denote the particular sensor that is granted the access at time instant k, which can be calculated as

$$\gamma_k = \mathrm{mod}(k + \gamma_{\mathrm{ini}} - 2, N) + 1 \tag{3}$$

where γ_{ini} is the assigned sensor having the initial access.

In fact, due to the opening-up characteristic of the shared communication network, the transmission process of the measurements is vulnerable to the cyber attacks. In other words, the measurement $y_k^{\gamma_k}$ may be deliberately falsified by the randomly occurring deception attacks during transmission over the network, and such an attacking behavior can be modeled by

$$\tilde{y}_k^{\gamma_k} = y_k^{\gamma_k} + \eta_k \varrho_k^{\gamma_k} \tag{4}$$

where $\tilde{y}_k^{\gamma_k}$ denotes the measurement that may be corrupted and $\varrho_k^{\gamma_k}$ represents the deception attack initiated by the adversaries characterized by

$$\varrho_k^{\gamma_k} = -y_k^{\gamma_k} + \xi_k \tag{5}$$

with ξ_k being the random deception signal satisfying $p_{\xi_k}(\cdot)$. It is worthwhile to note that the deception attacks initiated by adversaries might not be always effective owing to the intricate network environment and the defense measures. As such, from the viewpoint of defenders, the deception attacks are likely to occur in a random fashion. The stochastic variable η_k, which is employed to characterize the phenomenon of the randomly occurring deception attacks, is a Bernoulli-distributed white sequence taking values on 0 or 1 with the following probability distribution:

$$\begin{cases} P\{\eta_k = 1\} = \bar{\eta} \\ P\{\eta_k = 0\} = 1 - \bar{\eta} \end{cases} \tag{6}$$

where $\bar{\eta} \in [0, 1)$ is a known constant referred to as the success rate of the launched deception attacks. Then, the available measurement signals at the filter end with the zero input strategy are denoted as

$$\bar{y}_k = \begin{bmatrix} (\bar{y}_k^1)^T & (\bar{y}_k^2)^T & \cdots & (\bar{y}_k^N)^T \end{bmatrix}^T \tag{7}$$

where

$$\bar{y}_k^i = \begin{cases} \tilde{y}_k^{\gamma_k}, & \text{if } i = \gamma_k; \\ 0_{n_y \times 1}, & \text{otherwise.} \end{cases}$$

Before proceeding further, the following three assumptions are made to clarify the considered system.

Assumption 1. *The initial state x_0 satisfies the prior probability distribution $p_{x_0}(\cdot)$.*

Assumption 2. *The measurement noise sequences $\{\nu_k^i\}_{i=1}^N$ and the process noise sequence ω_k are mutually independent and also independent of the initial state x_0.*

Assumption 3. *The nonlinear functions $f(\cdot)$ and $h^i(\cdot)$, as well as the probability density functions $p_{\omega_k}(\cdot)$, $p_{\nu_k^i}(\cdot)$ and $p_{\xi_k}(\cdot)$, are all known.*

The purpose of this paper is to develop a particle filtering algorithm for the general nonlinear/non-Gaussian CPSs under the RRP subject to the randomly occurring deception attacks such that the estimate of state x_k can be obtained in the sense of minimum mean-square error based on the scheduled and corrupted measurement information.

3. RRP-Based Particle Filtering Algorithm with Randomly Occurring Deception Attacks

In this section, the basic framework of the standard particle filtering algorithm [2] is briefly revisited, and then the RRP-based particle filtering scheme with randomly occurring deception attacks is developed. A schematic diagram of the considered CPS is depicted in Fig. 1.

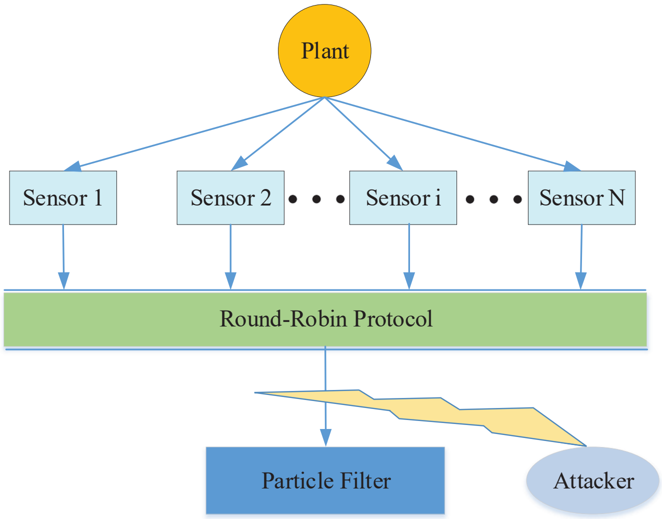

Figure 1: Block diagram of the CPS subject to randomly occurring deception attacks under RRP.

Generally speaking, the fundamental idea of the particle filtering algorithm is to use the importance sampling method [2] to approximate the posterior probability density function with a set of weighted particles as

$$p(x_{0:k}|\bar{y}_{1:k}) = \sum_{m=1}^{M} W_k^m \delta(x_{0:k} - x_{0:k}^m) \tag{8}$$

where $\delta(\cdot)$ is the Dirac delta function and the particles $\{x_{0:k}^m\}_{m=1}^M$ are drawn from an importance density $q(x_{0:k}|\bar{y}_{1:k})$, $x_{0:k}$ denotes the trajectory of x from time instant 0 to k, and $\bar{y}_{1:k}$ denotes the set of all received measurements up to time instant k, i.e. $\bar{y}_{1:k} = \{\bar{y}_1, \bar{y}_2, \cdots, \bar{y}_k\}$. In addition, the importance weights $\{W_k^m\}_{m=1}^M$ can be determined as

$$W_k^m \propto \frac{p(x_{0:k}^m|\bar{y}_{1:k})}{q(x_{0:k}^m|\bar{y}_{1:k})}. \tag{9}$$

Assuming that the state evolution follows the first-order Markov process, it can be obtained from the Bayesian theorem that

$$\begin{aligned} p(x_{0:k}|\bar{y}_{1:k}) &= \frac{p(\bar{y}_k|x_{0:k}, \bar{y}_{1:k-1})p(x_{0:k}|\bar{y}_{1:k-1})}{p(\bar{y}_k|\bar{y}_{1:k-1})} \\ &\propto p(\bar{y}_k|x_{0:k}, \bar{y}_{1:k-1})p(x_{0:k}|\bar{y}_{1:k-1}) \\ &= p(\bar{y}_k|x_{0:k}, \bar{y}_{1:k-1})p(x_k, x_{0:k-1}|\bar{y}_{1:k-1}) \\ &= p(\bar{y}_k|x_k, \bar{y}_{1:k-1})p(x_k|x_{k-1})p(x_{0:k-1}|\bar{y}_{1:k-1}). \end{aligned} \tag{10}$$

On the other hand, under the assumption that the previous state information $x_{0:k-1}$ and the current measurement $\bar{y}_k$ are uncorrelated, the importance density function $q(x_{0:k}|\bar{y}_{1:k})$ can be further expressed as

$$q(x_{0:k}|\bar{y}_{1:k}) = q(x_k|x_{0:k-1}, \bar{y}_{1:k})q(x_{0:k-1}|\bar{y}_{1:k-1}). \tag{11}$$

From (9)-(11), the importance weights are recursively calculated by

$$W_k^m \propto W_{k-1}^m \frac{p(\bar{y}_k|x_k^m, \bar{y}_{1:k-1})p(x_k^m|x_{k-1}^m)}{q(x_k^m|x_{0:k-1}^m, \bar{y}_{1:k})} \tag{12}$$

where the particles $\{x_k^m\}_{m=1}^M$ are drawn from the proposal density function $q(x_k|x_{0:k-1}, \bar{y}_{1:k})$.

Note that the likelihood function $p(\bar{y}_k|x_k^m, \bar{y}_{1:k-1})$ cannot be simply written as $p(\bar{y}_k|x_k^m)$ due to the existence of the RRP. To be more specific, if the past transmitted measurements $\bar{y}_{1:k-1}$ are given, then the sensor having the access at time instant $k-1$ (denoted as γ_{k-1}) is determined. Therefore, we have

$$\begin{aligned} p(\bar{y}_k|x_k^m, \bar{y}_{1:k-1}) &= p(\bar{y}_k|x_k^m, \gamma_{k-1}) \\ &= p(\bar{y}_k^1, \bar{y}_k^2, \cdots, \bar{y}_k^N|x_k^m, \gamma_k) \\ &= p(0, \cdots, 0, \bar{y}_k^{\gamma_k}, 0, \cdots, 0|x_k^m) \\ &= p(\tilde{y}_k^{\gamma_k}|x_k^m) \end{aligned} \tag{13}$$

where the second equality results from the property of the RRP that the transmission order is deterministic.

According to the law of total probability, we can write

$$\begin{aligned} & p(\tilde{y}_k^{\gamma_k}|x_k^m) \\ =& p(\tilde{y}_k^{\gamma_k}, \eta_k = 0|x_k^m) + p(\tilde{y}_k^{\gamma_k}, \eta_k = 1|x_k^m) \\ =& p(\tilde{y}_k^{\gamma_k}|\eta_k = 0, x_k^m)P\{\eta_k = 0|x_k^m\} + p(\tilde{y}_k^{\gamma_k}|\eta_k = 1, x_k^m)P\{\eta_k = 1|x_k^m\} \\ =& (1-\bar{\eta})p(\tilde{y}_k^{\gamma_k}|\eta_k = 0, x_k^m) + \bar{\eta}p(\tilde{y}_k^{\gamma_k}|\eta_k = 1, x_k^m) \\ =& (1-\bar{\eta})p_{\nu_k^{\gamma_k}}(\tilde{y}_k^{\gamma_k} - h^{\gamma_k}(x_k^m)) + \bar{\eta}p_{\xi_k}(\tilde{y}_k^{\gamma_k}). \end{aligned} \tag{14}$$

Remark 1. *It is worth mentioning that, given the measurements at the time instant $k-1$, the stochasticity of the measurement outputs $\bar{y}_k$ received by the filter is only reflected in the updated component $\tilde{y}_k^{\gamma_k}$ according to the RRP. When the zero input strategy is employed as shown in (7), all the measurements but the updated one are definitely equal to zero. In the case of the zero-order holder strategy, the current available measurements (except the output of the sensor granted the access) are totally determined by previously transmitted measurements. Thus, under the RRP, only the measurement output $\tilde{y}_k^{\gamma_k}$ is utilized to calculate the likelihood value and accordingly update the importance weight with both kinds of data-holding strategies. On the other hand, the scheduled measurement is prone to be overheard and modified by the cunning adversaries during the wireless transmission, and a Bernoulli-distributed stochastic variable η_k is introduced to depict the random nature of the effective deception attacks. Specifically, if $\eta_k = 1$, the scheduled measurement is successfully attacked by the malicious attackers and, if $\eta_k = 0$, the scheduled measurement is safely transmitted to the filter end. In addition, if the success rate of the launched deception attacks is set as $\bar{\eta} = 0$, then the addressed problem reduces to the case where only the RRP is taken into account.*

As can be seen from (12), the term $p(x_k|x_{k-1})$ in the numerator is the transition probability density function, which is determined by the dynamics of state model (1). The term $q(x_k|x_{0:k-1}, \bar{y}_{1:k})$ in the denominator is the proposal density function to draw the random particles, which can deteriorate the performance of the particle filtering to some extent when inappropriately selected. Following the line of the literature [26, 34], the transition probability density is chosen as the proposal density function due primarily to its simplicity and convenience. Based on (13)-(14), the update rule (12) of importance weights is written as

$$\begin{aligned} W_k^m \propto & W_{k-1}^m p(\bar{y}_k|x_k^m, \bar{y}_{1:k-1}) \\ = & W_{k-1}^m \big[(1-\bar{\eta}) p_{\nu_k^{\gamma_k}}(\tilde{y}_k^{\gamma_k} - h^{\gamma_k}(x_k^m)) + \bar{\eta} p_{\xi_k}(\tilde{y}_k^{\gamma_k})\big]. \end{aligned} \tag{15}$$

The RRP-based particle filtering algorithm with randomly occurring deception attacks can now be summarized in Algorithm 1.

Remark 2. *From Algorithm 1, we can see that the update of importance weights only depends on the point-wise evaluation of a portion of likelihood function at each particle, which is easy to implement but does not utilize the most recent observation to sample new particles. For the case where the likelihood function is very narrow or lies in the tail of the prior distribution, the phenomenon of particle degeneracy may occur and thus deteriorates the filtering performance [31]. A common solution to this problem is to choose the posterior probability density function acquired from other nonlinear filters (e.g., extended Kalman filter and unscented Kalman filter) as the proposal density function $q(x_k^m|x_{0:k-1}^m, \bar{y}_{1:k})$. Unfortunately, in this paper, the available measurements $\bar{y}_{1:k}$ at the filter end are scheduled by the RRP and further compromised by the deception attacks, which renders the standard nonlinear filters inapplicable. Therefore, we will consider the possibility of extending our results by using the proposal density function obtained from the RRP-based unscented Kalman filter, which is one of our future research directions. For more details about the protocol-based unscented Kalman filtering algorithm, we refer the interested readers to [24].*

Remark 3. *Up to now, the particle filtering problem has been addressed for a class of nonlinear/non-Gaussian CPSs subject to the randomly occurring deception attacks under the RRP. Compared with existing results, the RRP has been taken into consideration in the particle filtering framework to schedule the sensors and hence avoid the data collision in practical applications, which is necessary*

Algorithm 1 RRP-based particle filtering algorithm with randomly occurring deception attacks

```
Step 1. Particle initialization
        Draw $M$ particles from the initial prior probability distribution $x_0^m \sim p_{x_0}(\cdot)$ and all importance weights are set to be identical, i.e. $\frac{1}{M}$. Moreover, set the maximum simulation time $K$.
Step 2. Importance sampling
        For each $m = 1, \ldots, M$, draw particle $x_k^m$ from the transition probability density distribution $p(x_k|x_{k-1}^m)$, i.e., $x_k^m = f(x_{k-1}^m) + \omega_{k-1}^m$, where $\omega_{k-1}^m$ is sampled from $p_{\omega_{k-1}}(\cdot)$.
Step 3. Measurement update
        Collect the measurements at the filter end under the randomly occurring deception attacks and the scheduling mechanism of the RRP.
Step 4. Weight calculation
        Calculate the importance weights $\{\hat{W}_k^m\}_{m=1}^M$ according to
            $\hat{W}_k^m = W_{k-1}^m \big[(1-\bar{\eta}) p_{\nu_k^{\gamma_k}}(\tilde{y}_k^{\gamma_k} - h^{\gamma_k}(x_k^m)) + \bar{\eta} p_{\xi_k}(\tilde{y}_k^{\gamma_k})\big]$,
        and normalize the weights as $W_k^m = \frac{\hat{W}_k^m}{\sum_{m=1}^M \hat{W}_k^m}$.
Step 5. State estimate update
        Calculate the state estimate $\hat{x}_k$ and estimation error covariance $P_k$ as
            $\hat{x}_k = \sum_{m=1}^{M} W_k^m x_k^m$,
            $P_k = \sum_{m=1}^{M} W_k^m (x_k^m - \hat{x}_k)(x_k^m - \hat{x}_k)^T$.
Step 6. Resampling
        Resample a new set of particles with equal weights from $\sum_{m=1}^M W_k^m \delta(x_k - x_k^m)$.
Step 7. If $k < K$, then go to Step 2; otherwise go to Step 8.
Step 8. Stop.
```

in the network with limited bandwidth. Meanwhile, the probability information of the randomly occurring deception attacks has been inserted into the modified likelihood function to improve the robustness against the malicious attacks launched by the adversaries. On the other hand, when a large number of sensors are deployed to observe the target plant, the update of likelihood value at the filter end needs to calculate the product of N local likelihood functions, which may be computationally expensive in the standard particle filtering algorithm. However, in our proposed algorithm, the likelihood function is only computed based on reduced sensor information at each time instant, which can relax the burden from the perspective of computation resources.

4. Simulation Example

In this section, a target tracking problem is provided to evaluate the tracking performance of the proposed particle filtering algorithm. The state vector of the moving target is defined as $x_k = [\zeta_k^t, \dot{\zeta}_k^t, \psi_k^t, \dot{\psi}_k^t]^T$, where (ζ_k^t, ψ_k^t) and $(\dot{\zeta}_k^t, \dot{\psi}_k^t)$ denote the position and velocity at time instant k in the two-dimensional Cartesian coordinates ζ and ψ, respectively. The target motion is modelled by [5]

$$x_{k+1} = \begin{bmatrix} 1 & T & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & T \\ 0 & 0 & 0 & 1 \end{bmatrix} x_k + \omega_k \tag{16}$$

where T represents the sampling interval and ω_k the zero-mean Gaussian white noise sequence with covariance

$$Q_k = \sigma_\omega^2 \begin{bmatrix} \frac{T^3}{3} & \frac{T^2}{2} & 0 & 0 \\ \frac{T^2}{2} & T & 0 & 0 \\ 0 & 0 & \frac{T^3}{3} & \frac{T^2}{2} \\ 0 & 0 & \frac{T^2}{2} & T \end{bmatrix} \tag{17}$$

where σ_ω^2 denotes the acceleration variance.

The measurement function of the ith sensor is expressed by

$$h^i(x_k) = \begin{bmatrix} \sqrt{(\zeta_k^t - \zeta^{s,i})^2 + (\psi_k^t - \psi^{s,i})^2} \\ \text{atan2}(\psi_k^t - \psi^{s,i}, \zeta_k^t - \zeta^{s,i}) \end{bmatrix} \tag{18}$$

where $(\zeta^{s,i}, \psi^{s,i})$ denotes the position of the ith sensor. The measurement noise on the ith sensor is modelled by a mixture of two Gaussian distributions, i.e.,

$$p(\nu_k^i) = (1 - \kappa^i)\mathcal{N}(\nu_k^i; \mu_1^i, \Sigma_1^i) + \kappa^i \mathcal{N}(\nu_k^i; \mu_2^i, \Sigma_2^i) \tag{19}$$

where κ^i stands for the glint probability.

For the purpose of comparison, the tracking performance will be evaluated under the following four scenarios: 1) tracking with the proposed RRP-based particle filtering algorithm under randomly occurring deception attacks (denoted as RRP-PF-DA); 2) tracking with the RRP-based standard particle filtering algorithm neglecting the effect of randomly occurring deception attacks (denoted as RRP-SPF-DA); 3) tracking with the RRP-based standard particle filtering algorithm utilizing normal measurements (denoted as RRP-SPF-NM); and 4) tracking with the particle filtering algorithm using all the sensors' measurements and considering the effect of randomly occurring deception attacks (denoted as PF-DA).

In all simulations, the trajectory of the target is generated with $x_0 = [20, 0.3, 20, 0.3]^T$, $T = 1$ and $\sigma_\omega = 0.055$, and 4 sensors, as shown in Fig. 2, are deployed to observe the target. Other parameters required in the simulation are set as follows: $M = 500$, $\mu_1^i = [0, 0]^T$, $\Sigma_1^i = \text{diag}\{4, (\pi/180)^2\}$, $\mu_2^i = [0, 0]^T$, $\Sigma_2^i = \text{diag}\{25, (\pi/90)^2\}$, $\kappa^i = 0.2$, $\bar{\eta} = 0.2$. In addition, the deception attack signal satisfies a uniform distribution on a two-dimensional set $[-10, 80] \times [-\pi/2, \pi/2]$. To evaluate the performance of the filtering algorithms, the root mean-square error (RMSE) on both position and velocity estimates are introduced as the performance metric, which are calculated over $L = 50$ Monte Carlo runs as

$$\text{RMSE}_{\text{p},k} = \sqrt{\frac{1}{L}\sum_{l=1}^{L}\Big[(\zeta_k^{t,l} - \hat{\zeta}_k^{t,l})^2 + (\psi_k^{t,l} - \hat{\psi}_k^{t,l})^2\Big]},$$

$$\text{RMSE}_{\text{v},k} = \sqrt{\frac{1}{L}\sum_{l=1}^{L}\Big[(\dot{\zeta}_k^{t,l} - \hat{\dot{\zeta}}_k^{t,l})^2 + (\dot{\psi}_k^{t,l} - \hat{\dot{\psi}}_k^{t,l})^2\Big]}$$

where the realization and estimate of $(\zeta_k^t, \psi_k^t, \dot{\zeta}_k^t, \dot{\psi}_k^t)$ in the lth Monte Carlo run are represented by $(\zeta_k^{t,l}, \psi_k^{t,l}, \dot{\zeta}_k^{t,l}, \dot{\psi}_k^{t,l})$ and $(\hat{\zeta}_k^{t,l}, \hat{\psi}_k^{t,l}, \hat{\dot{\zeta}}_k^{t,l}, \hat{\dot{\psi}}_k^{t,l})$, respectively.

One realization of the true target trajectory and the trajectories estimated by the abovementioned algorithms are shown in Fig. 2. We see that the RRP-PF-DA, RRP-SPF-NM and PF-DA can closely track the true trajectory, while RRP-SPF-DA fails to track the target in most of the time. The simulation results obtained from the 50 Monte Carlo runs are displayed in Figs. 3-4 and Table 1, from which we observe that the proposed RRP-PF-DA can attenuate the impact of the randomly occurring deception attacks to some extent and achieve a satisfactory tracking performance. When compared with the PF-DA, the proposed RRP-PF-DA has distinct advantages in terms of average running time and communication rate, although at the cost of sacrificing certain tracking accuracy. Hence, we can naturally draw a conclusion that the proposed algorithm is more efficient in the CPS with limited computation and communication resources.

Table 1: Performance comparisons with respect to average RMSE, running time and communication times

	RMSE_p	RMSE_v	Running Time	Communication Times
RRP-PF-DA	0.9012	0.1197	0.0205	120
RRP-SPF-DA	9.7923	0.3760	0.0199	120
RRP-SPF-NM	0.8044	0.1169	0.0200	120
PF-DA	0.5746	0.1018	0.0764	480

Another group of simulation is conducted to investigate the effect of the randomly occurring deception attacks on the tracking performance. The behaviors of the RMSEs on both position and velocity estimates obtained with different occurrence probabilities are plotted in Figs. 5-6. As expected, the tracking performance degrades with increasing occurrence probabilities of the deception attacks.

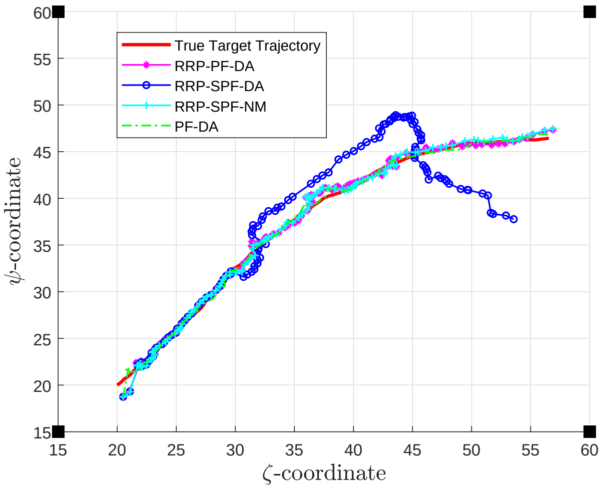

Figure 2: One realization of the target trajectory and its estimates obtained from RRP-PF-DA, RRP-SPF-DA, RRP-SPF-NM and PF-DA. The black squares denote the sensors' positions.

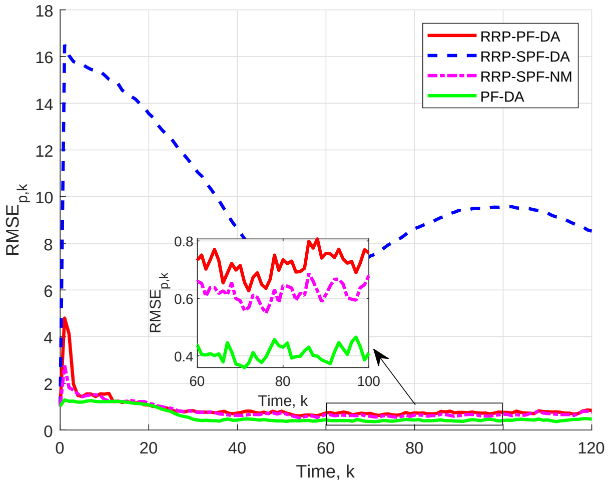

Figure 3: RMSEs on position estimates of RRP-PF-DA, RRP-SPF-DA, RRP-SPF-NM and PF-DA.

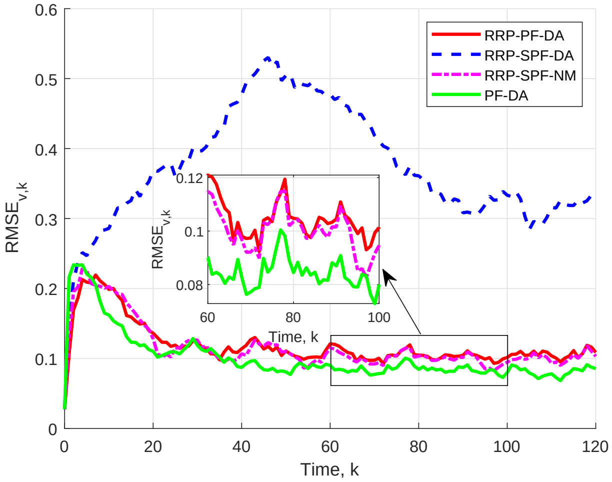

Figure 4: RMSEs on velocity estimates of RRP-PF-DA, RRP-SPF-DA, RRP-SPF-NM and PF-DA.

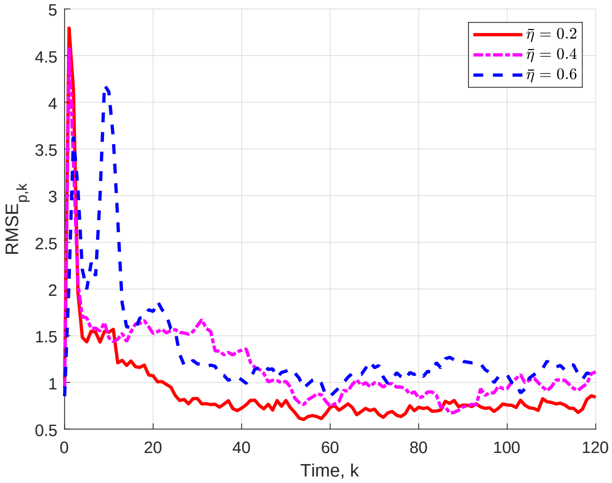

Figure 5: RMSEs on position estimates with $\bar{\eta} = 0.2, 0.4, 0.6$.

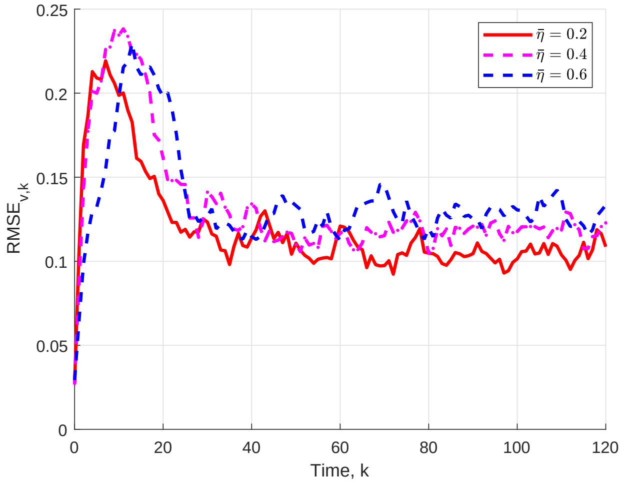

Figure 6: RMSEs on velocity estimates with $\bar{\eta} = 0.2, 0.4, 0.6$.

5. Conclusions

In this paper, we have investigated the sequential Bayesian filtering problem for the nonlinear/non-Gaussian CPSs subject to the randomly occurring deception attacks in the framework of particle filtering under the RRP. The measurement transmission has been scheduled by the RRP and a Bernoulli-distributed stochastic variable with known probability distribution has been employed to characterize the randomly occurring deception attacks. A modified likelihood function under the RRP has been constructed to attenuate the effect of the randomly occurring deception attacks on the estimation performance. Finally, an illustrative example has been presented to demonstrate the feasibility and effectiveness of the proposed RRP-PF-DA algorithm. The simulation results have shown that the proposed RRP-PF-DA algorithm can provide an effective alternative to the PF-DA algorithm in a bandwidth-limited network. The directions of future research would focus on considering more sophisticated attacks [8] as well as other communication protocols including stochastic communication protocol and weighted Try-Once-Discard protocol, and designing the secure communication scheme based on the principle of cryptology [10].

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grants 61873148 and 61933007, the China Scholarship Council under Grant 201806030206, and the Alexander von Humboldt Foundation of Germany.

References

[1] I. Arasaratnam, S. Haykin, Cubature Kalman filters, IEEE Trans. Autom. Control 54 (6) (2009) 1254–1269.

[2] M. S. Arulampalam, S. Maskell, N. Gordon, T. Clapp, A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking, IEEE Trans. Signal Process. 50 (2) (2002) 174–188.

[3] G. K. Befekadu, V. Gupta, P. J. Antsaklis, Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies, IEEE Trans. Autom. Control 60 (12) (2015) 3299–3304.

[4] P. Date, K. Ponomareva, Linear and non-linear filtering in mathematical finance: A review, IMA J. Manag. Math. 22 (3) (2011) 195–211.

[5] S. S. Dias, M. G. S. Bruno, Cooperative target tracking using decentralized particle filtering and RSS sensors, IEEE Trans. Signal Process. 61 (14) (2013) 3632–3646.

[6] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, X.-M. Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275 (2018) 1674–1683.

[7] A. Farina, B. Ristic, D. Benvenuti, Tracking a ballistic target: Comparison of several nonlinear filters, IEEE Trans. Aerosp. Electron. Syst. 38 (3) (2002) 854–867.

[8] X. Ge, Q.-L. Han, X.-M. Zhang, D. Ding, F. Yang, Resilient and secure remote monitoring for a class of cyber-physical systems against attacks, Inf. Sci. in press (doi: 10.1016/j.ins.2019.10.057)

[9] W. He, X. Gao, W. Zhong, F. Qian, Secure impulsive synchronization control of multi-agent systems under deception attacks, Inf. Sci. 459 (2018) 354–368.

[10] W. He, T. Luo, Y. Tang, W. Du, Y.-C. Tian, F. Qian, Secure communication based on quantized synchronization of chaotic neural networks under an event-triggered strategy, IEEE Trans. Neural Netw. Learn Syst. in press (doi: 10.1109/TNNLS.2019.2943548)

[11] W. He, F. Qian, Q.-L. Han, G. Chen, Almost sure stability of nonlinear systems under random and impulsive sequential attacks, IEEE Trans. Autom. Control in press (doi: 10.1109/TAC.2020.2972220)

[12] N. Hou, Z. Wang, D. W. C. Ho and H. Dong, Robust partial-nodes-based state estimation for complex networks under deception attacks, IEEE Transactions on Cybernetics, Vol. 50, No. 6, Jun. 2020, pp. 2793-2802.

[13] J. Hu, Z. Wang, H. Gao, L. K. Stergioulas, Extended Kalman filtering with stochastic nonlinearities and multiple missing measurements, Automatica 48 (9) (2012) 2007–2015.

[14] S. Jafarzadeh, C. Lascu, M. S. Fadali, Square root unscented Kalman filters for state estimation of induction motor drives, IEEE Trans. Ind. Appl. 49 (1) (2013) 92–99.

[15] B. Jia, M. Xin, Y. Cheng, Sparse-grid quadrature nonlinear filtering, Automatica 48 (2) (2012) 327–341.

[16] S. Julier, J. Uhlmann, H. F. Durrant-Whyte, A new method for the nonlinear transformation of means and covariances in filters and estimators, IEEE Trans. Autom. Control 45 (3) (2000) 477–482.

[17] S. Kluge, K. Reif, M. Brokate, Stochastic stability of the extended Kalman filter with intermittent observations, IEEE Trans. Autom. Control 55 (2) (2010) 514–518.

[18] D.-J. Lee, K. T. Alfriend, Sigma point filtering for sequential orbit estimation and prediction, J. Spacecr. Rockets 44 (2) (2007) 388–398.

[19] W. Li, Y. Jia, J. Du, State estimation for stochastic complex networks with switching topology, IEEE Trans. Autom. Control 62 (12) (2017) 6377–6384.

[20] W. Li, Z. Wang, Q. Liu, L. Guo, An information aware event-triggered scheme for particle filter based remote state estimation, Automatica 103 (2019) 151–158.

[21] W. Li, Z. Wang, Y. Yuan, L. Guo, Particle filtering with applications in networked systems: A survey, Complex Intell. Syst. 2 (4) (2016) 293–315.

[22] W. Li, Z. Wang, Y. Yuan, L. Guo, Two-stage particle filtering for non-Gaussian state estimation with fading measurements, Automatica 115 (2020) art. no. 108882, 12 pages.

[23] Q. Liu, Z. Wang, Q.-L. Han and C. Jiang, Quadratic estimation for discrete time-varying non-Gaussian systems with multiplicative noises and quantization effects, *Automatica*, vol. 113, Art. no. 108714, Mar. 2020.

[24] S. Liu, Z. Wang, Y. Chen, G. Wei, Protocol-based unscented Kalman filtering in the presence of stochastic uncertainties, IEEE Trans. Autom. Control 65 (3) (2020) 1303–1309.

[25] S. Liu, Z. Wang, G. Wei and M. Li, Distributed set-membership filtering for multi-rate systems under the Round-Robin scheduling over sensor networks, *IEEE Transactions on Cybernetics*, Vol. 50, No. 5, May 2020, pp. 1910-1920.

[26] C. S. Maíz, E. M. Molanes-López, J. Míguez, P. M. Djurić, A particle filtering scheme for processing time series corrupted by outliers, IEEE Trans. Signal Process. 60 (9) (2012) 4611–4627.

[27] N. Sadeghzadeh-Nokhodberiz, M. Davoodi, N. Meskin, Stochastic event-triggered particle filtering for state estimation, *Second International Conference on Event-Based Control, Communication, and Signal Processing (EBCCSP)*, Krakow, Poland, 2016, pp. 1–4.

[28] B. Shen, Z. Wang, D. Wang and H. Liu, Distributed state-saturated recursive filtering over sensor networks under Round-Robin protocol, *IEEE Transactions on Cybernetics*, in press, DOI: 10.1109/TCYB.2019.2932460.

[29] Y. Shen, Z. Wang, B. Shen, F. E. Alsaadi, F. E. Alsaadi, Fusion estimation for multi-rate linear repetitive processes under weighted Try-Once-Discard protocol, Inf. Fusion 55 (2020) 281–291.

[30] H. Tanizaki, *Nonlinear Filters: Estimation and Applications*, 2nd ed. Berlin: Springer, 1996.

[31] R. Van der Merwe, A. Doucet, N. De Freitas, E. Wan, The unscented particle filter, Adv. Neural Inf. Process. Syst. 13 (2001) 584–590.

[32] S. Xiao, Q.-L. Han, X. Ge, Y. Zhang, Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks, IEEE Trans. Cybern. 50 (3) (2020) 1220–1229.

[33] D. Xu, C. Shen, F. Shen, A robust particle filtering algorithm with non-Gaussian measurement noise using Student-t distribution, IEEE Signal Process. Lett. 21 (1) (2014) 30–34.

[34] L. Xu, K. Ma, W. Li, Y. Liu, F. E. Alsaadi, Particle filtering for networked nonlinear systems subject to random one-step sensor delay and missing measurements, Neurocomputing 275 (2018) 2162–2169.

[35] C. Yang, H. Fang, B. Shi, Particle filter with Markovian packet dropout and time delay, J. Frankl. Inst. 356 (1) (2019) 675–696.

[36] D. Ye, T.-Y. Zhang, G. Guo, Stochastic coding detection scheme in cyber-physical systems against replay attack, Inf. Sci. 481 (2019) 432–444.

[37] Y. Yuan, Z. Wang, P. Zhang, H. Liu, Near-optimal resilient control strategy design for state-saturated networked systems under stochastic communication protocol, IEEE Trans. Cybern. 49 (8) (2019) 3155–3167.

[38] Y. Zhang, Y. Huang, N. Li, L. Zhao, Particle filter with one-step randomly delayed measurements and unknown latency probability, Int. J. Syst. Sci. 47 (1) (2016) 209–221.