Statistical Linear Regression Approach to Kalman Filtering and Smoothing under Cyber-Attacks

Kundan Kumar, Muhammad Iqbal, and Simo Särkkä
Department of Electrical Engineering and Automation, Aalto University, Finland
{kundan.kumar, muhammad.iqbal, simo.sarkka}@aalto.fi

***Abstract*—Remote state estimation in cyber-physical systems is often vulnerable to cyber-attacks due to wireless connections between sensors and computing units. In such scenarios, adversaries compromise the system by injecting false data or blocking measurement transmissions via denial-of-service attacks, distorting sensor readings. This paper develops a Kalman filter and Rauch–Tung–Striebel (RTS) smoother for linear stochastic state-space models subject to cyber-attacked measurements. We approximate the faulty measurement model via generalized statistical linear regression (GSLR). The GSLR-based approximated measurement model is then used to develop a Kalman filter and RTS smoother for the problem. The effectiveness of the proposed algorithms under cyber-attacks is demonstrated through a simulated aircraft tracking experiment.**

***Index Terms*—Remote state estimation, cyber-physical systems, cyber-attacks, generalized statistical linear regression.**

I. Introduction

Cyber-physical systems (CPSs) are integral to applications such as intelligent transportation, terrestrial exploration, power grids, aerospace, and hazardous environments [1]–[5]. These systems rely on wireless communication for remote monitoring and control, making them vulnerable to cyber-attacks. Adversaries can manipulate sensor measurements by injecting false data or blocking transmissions, thereby compromising system performance. In the absence of such adversarial disruptions, state estimation methods such as the Kalman filter (KF) and Rauch–Tung–Striebel (RTS) smoother provide optimal solutions for linear Gaussian systems [6], [7]. However, their performance degrades significantly under cyber-attacks, necessitating robust estimation techniques capable of handling compromised measurements.

Several types of cyber attack models have been studied in the literature, including replay attacks [8], denial-of-service (DoS) attacks [9], and false data injection (FDI) attacks [10], [11]. In a replay attack, the intruder observes and records measurement readings for a certain time period and later retransmits the recorded measurements to carry out the attacks [8]. The DoS attacks [9] block measurement transmission from the sensor to the computing unit. In FDI attacks, the intruders have access to the measurements and modify them in a random manner [10], [12]. In this manuscript, we focus on the state estimation under the DoS and FDI attacks.

A few works have addressed the estimation problem under DoS and FDI attacks. The authors in [9] proposed an optimal attack strategy for an energy-constrained attacker in a linear state space model (SSM). In [13], a game-theoretic approach is used to develop a state estimation algorithm for linear SSM under DoS attacks. For the linear system dealing with the additive FDI attacks, the state estimation algorithms have been developed for sensor networks [12] and power grids [14]. A risk-sensitive filtering algorithm for an inaccurate linear system model under additive FDI attacks was proposed in [15]. To handle additive FDI attacks in nonlinear state-space models, estimation algorithms based on the extended Kalman filter (EKF), unscented Kalman filter (UKF), and cubature Kalman filter (CKF) have been developed in [16]–[18]. Recently, [10], [11] proposed a generalized Bayesian filtering framework to address simultaneous additive and multiplicative FDI attacks. A state estimation algorithm under DoS and additive FDI attacks was developed in [19]. However, there is a lack of estimation methods that account for DoS and simultaneous additive and multiplicative FDI attacks. This paper aims to address this gap.

In this paper, we develop a Kalman type of filter and RTS smoother for state space models under DoS and FDI attacks. First, we approximate the faulty measurement model [10] using the generalized statistical linear regression (GSLR) approach. Subsequently, the GSLR-based approximated measurement is used to develop the estimation algorithm under the Bayesian framework. The main contributions of this article are as follows: (1) We present a unified formulation of the faulty measurement model that accounts for DoS and simultaneous additive and multiplicative FDI attacks. (2) Using the GSLR method, we approximate the faulty measurement model. (3) Based on the approximated measurement model, we develop the Kalman filter and RTS smoother. (4) Finally, we demonstrate the performance of the proposed algorithm through numerical experiments.

II. Problem Formulation

Consider a stochastic dynamical system with the following state space model [7], [20]

$$x_k = A_{k-1}x_{k-1} + \eta_{k-1}, \tag{1}$$

$$z_k = H_k x_k + \nu_k, \tag{2}$$

where $x_k \in \mathbb{R}^{n_x}$, and $z_k \in \mathbb{R}^{n_z}$ are the state of the dynamic system and sensor measurement, respectively. Here, the matrix $A_{k-1} \in \mathbb{R}^{n_x \times n_x}$ is the state transition matrix of the dynamic model, $H_k \in \mathbb{R}^{n_z \times n_x}$ is the measurement model matrix. The terms $\eta_{k-1} \sim \mathcal{N}(0,\, Q_{k-1})$ and $\nu_k \sim \mathcal{N}(0,\, R_k)$ represent the Gaussian process noise and measurement noise, respectively.

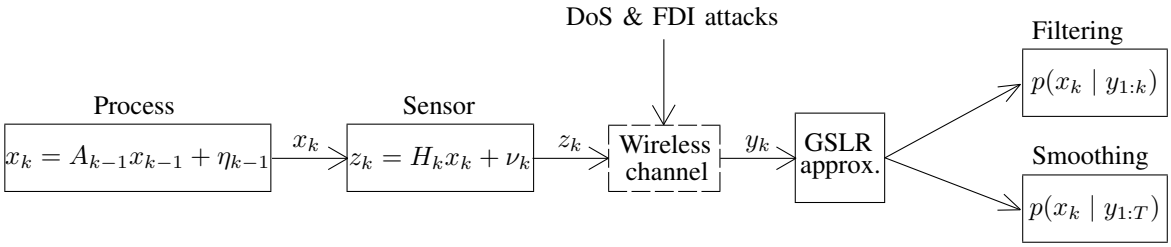


Fig. 1 Schematic diagram of the proposed estimation algorithm under DoS and FDI attacks. The filtering (forward pass) and smoothing algorithms are developed based on the GSLR-based approximated faulty measurement model.

TABLE I Various attack types under different stochastic parameters

Parameters		Attack types
$\xi_{b,k}=1,\ \xi_{c,k},\xi_{a,k},\xi_{m,k}\in\{0,1\}$		No attack
$\xi_{b,k}=0,\xi_{c,k}=1$	$\xi_{a,k}=1,\xi_{m,k}=0$	Additive FDIA [11], [19]
	$\xi_{a,k}=0,\xi_{m,k}=1$	Multiplicative FDIA [11]
	$\xi_{a,k}=1,\ \xi_{m,k}=1$	Simultaneous FDIA [10]
$\xi_{b,k}=0,\xi_{c,k}=0,\ \ \xi_{a,k},\xi_{m,k}\in\{0,1\}$		DoS attack [19]

The initial state $x_0 \sim \mathcal{N}(\hat{x}_{0|0},\, P_{0|0})$, and the noises η_{k-1} and ν_k are mutually independent.

A. Measurement model under DoS and FDI attacks

Sensor measurements transmitted over a wireless communication channel to a remote computing unit are vulnerable to adversarial manipulation [8]–[11] (see Fig. 1). Attackers can alter the measurements through DoS and FDI attacks [10], [11], [19]. We model the faulty measurement under DoS and FDI attacks as follows:

$$\begin{aligned} y_k = \xi_{b,k} z_k + (1-\xi_{b,k})\xi_{c,k}\Big\{&\xi_{m,k} m_k (z_k + \xi_{a,k} a_k) \\ &+ (1-\xi_{m,k})(z_k + \xi_{a,k} a_k)\Big\}, \end{aligned} \tag{3}$$

where $y_k \in \mathbb{R}^{n_z}$ is the measurement after the attack, $a_k \sim \mathcal{N}(\mu_a, \Sigma_a)$ and $m_k \sim \mathcal{N}(\mu_m, \sigma_m^2)$ are additive and multiplicative false data parameter to alter the sensor measurement. The terms $\xi_{a,k}$, $\xi_{b,k}$, $\xi_{c,k}$ and $\xi_{m,k}$ in the model are Bernoulli random variables (BRVs) with probabilities α_a, α_b, α_c, and α_m, respectively. The model given in (3) can further be simplified to

$$\begin{aligned} y_k = \xi_{b,k} z_k + (1-\xi_{b,k})\xi_{c,k}\,&(1 + \xi_{m,k}\,(m_k - 1)) \\ &\times (z_k + \xi_{a,k} a_k). \end{aligned} \tag{4}$$

Table I presents attack scenarios under various stochastic parameter values. For special cases of the attacks model in (4), see the references in the rightmost column of Table I. The faulty measurement model given in (4) combines the models proposed in [10] and [19] into a single model.

III. Approximating the Faulty Measurement using GSLR Method

In this section, we aim to approximate the faulty measurement model (4) using GSLR [7], [21], [22] with respect to the probability density function (pdf) $\mathcal{N}(x_k \mid \hat{x}_{k|k-1},\, P_{k|k-1})$ as follows:

$$y_k \approx H_k^+ x_k + b_k^+ + \tilde{\nu}_k, \tag{5}$$

where $H_k^+ \in \mathbb{R}^{n_z \times n_x}$ and $b_k^+ \in \mathbb{R}^{n_z}$ are the coefficients of the approximation, and $\tilde{\nu}_k \sim \mathcal{N}(0, \tilde{\Omega}_k)$ represents the error, consisting of approximation error and measurement noise. The associated parameters of the approximated measurement model (5) can be expressed as

$$\begin{aligned} H_k^+ &= P_{k|k-1}^{yx} P_{k|k-1}^{-1}, \\ b_k^+ &= \hat{y}_{k|k-1} - H_k^+ \hat{x}_{k|k-1}, \\ \tilde{\Omega}_k &= P_{k|k-1}^{yy} - H_k^+ P_{k|k-1} H_k^{+\top}. \end{aligned} \tag{6}$$

In (6), the associated moments can be computed as follows:

$$\hat{y}_{k|k-1} = E_{\text{pr}}\left[E\left[y_k \mid x_k\right]\right], \tag{7}$$

$$P_{k|k-1}^{yy} = E_{\text{pr}}\left[\mathbb{V}\left[y_k \mid x_k\right]\right] + \mathbb{V}_{\text{pr}}\left[E\left[y_k \mid x_k\right]\right], \tag{8}$$

$$P_{k|k-1}^{yx} = \mathbb{C}_{\text{pr}}\left[E\left[y_k \mid x_k\right], x_k\right], \tag{9}$$

where $E_{\text{pr}}[\cdot]$, $\mathbb{V}_{\text{pr}}[\cdot]$, $\mathbb{C}_{\text{pr}}[\cdot]$ denote expectation, variance, and covariance, respectively, with respect to the prior pdf $\mathcal{N}(x_k \mid \hat{x}_{k|k-1},\, P_{k|k-1})$. Before computing the moments mentioned above, we introduce the following useful lemma.

Lemma 1. *Consider the probability distribution of attack parameters, $a_k \sim \mathcal{N}(\mu_a, \Sigma_a)$, $m_k \sim \mathcal{N}(\mu_m, \sigma_m^2)$ and BRVs $\xi_{a,k}$, $\xi_{b,k}$, $\xi_{c,k}$, $\xi_{m,k}$. Then, we have the following:*

$$\begin{aligned} &E\left[(1-\xi_{b,k})^2 \xi_{c,k}^2 \big(1 + \xi_{m,k}(m_k - 1)\big)^2\right] \\ &\quad = (1-\alpha_b)\alpha_c\left[(1-\alpha_m) + \alpha_m(\sigma_m^2 + \mu_m^2)\right], \end{aligned} \tag{10}$$

$$\begin{aligned} &E\Big[\big\{(1-\xi_{b,k})\xi_{c,k}(1 + \xi_{m,k}(m_k - 1)) - (1-\alpha_b)\alpha_c \\ &\times (1 + \alpha_m(\mu_M - 1))\big\}^2\Big] = (1-\alpha_b)\alpha_c\Big[\big((1-\alpha_m) \\ &+ \alpha_m(\mu_m^2 + \sigma_m^2)\big) - (1-\alpha_b)\alpha_c\big(1 + \alpha_m(\mu_m - 1)\big)^2\Big], \end{aligned} \tag{11}$$

and

$$\begin{aligned} &E\big[\big(\xi_{a,k}(a_k - \mu_a) + (\xi_{a,k} - \alpha_a)\mu_a\big)\big(\xi_{a,k}(a_k - \mu_a) \\ &+ (\xi_{a,k} - \alpha_a)\mu_a\big)^\top\big] = \alpha_a \Sigma_a + \alpha_a(1-\alpha_a)\mu_a \mu_a^\top. \end{aligned} \tag{12}$$

Proof. First, recall that if ξ is a Bernoulli random variable with probability α, we have

$$\begin{aligned} &p(\xi = 1) = E[\xi] = E[\xi^r] = \alpha, \\ &p(\xi = 0) = E[1 - \xi] = E[(1 - \xi)^r] = 1 - \alpha, \\ &E[(\xi - \alpha)^2] = (1 - \alpha)\alpha, \end{aligned} \tag{13}$$

where $r \geq 2$ is an arbitrary constant. The expected value of the square of $(1 - \xi_{b,k})\xi_{c,k}(1 + \xi_{m,k}(m_k - 1))$ is

$$\begin{aligned} &E\big[(1 - \xi_{b,k})^2\xi_{c,k}^2\big(1 + \xi_{m,k}(m_k - 1)\big)^2\big] = E\big[(1 - \xi_{b,k})^2\big] \\ &\times E\big[\xi_{c,k}^2\big]E\big[1 + \xi_{m,k}^2(m_k^2 - 2m_k + 1) + 2\xi_{m,k}(m_k - 1)\big]. \end{aligned}$$

Using (13) and probability distribution of m_k, the above equation becomes (10). Now, we calculate

$$\begin{aligned} &E\Big[\big\{(1 - \xi_{b,k})\xi_{c,k}\big(1 + \xi_{m,k}(m_k - 1)\big) - (1 - \alpha_b)\alpha_c\big(1 + \alpha_m \\ &\times (\mu_M - 1)\big)\big\}^2\Big] = E\Big[(1 - \xi_{b,k})^2\xi_{c,k}^2\big(1 + \xi_{m,k}(m_k - 1)\big)^2\Big] \\ &- 2E\Big[(1 - \xi_{b,k})\xi_{c,k}\big(1 + \xi_{m,k}(m_k - 1)\big)\Big](1 - \alpha_b)\alpha_c\big(1 + \alpha_m \\ &\times (\mu_M - 1)\big) + (1 - \alpha_b)^2\alpha_c^2\big(1 + \alpha_m(\mu_M - 1)\big)^2. \end{aligned}$$

Utilizing (13) along with the distribution of m_k, the above equation simplifies to (11). We compute the expected value of the given below equation as

$$\begin{aligned} &E\big[\big(\xi_{a,k}(a_k - \mu_a) + (\xi_{a,k} - \alpha_a)\mu_a\big)\big(\xi_{a,k}(a_k - \mu_a) \\ &+ (\xi_{a,k} - \alpha_a)\mu_a\big)^\top\big] = E\big[\xi_{a,k}^2(a_k - \mu_a)(a_k - \mu_a)^\top\big] \\ &+ E\big[\xi_{a,k}(\xi_{a,k} - \alpha_a)(a_k - \mu_a)\mu_a^\top\big] + E\big[\xi_{a,k}(\xi_{a,k} - \alpha_a) \\ &\times \mu_a(a_k - \mu_a)^\top\big] + E\big[(\xi_{a,k} - \alpha_a)^2\mu_a\mu_a^\top\big]. \end{aligned}$$

Following the properties of $\xi_{a,k}$ and a_k, we receive (12). □

A. Conditional moment computation

Next, we compute the moments given in (7)-(9), which we use in (6). The conditional expectation of y_k given x_k using (2) and (4) is as follows:

$$\begin{aligned} E[y_k \mid x_k] &= \alpha_b H_k x_k + (1 - \alpha_b)\alpha_c \\ &\times (1 + \alpha_m(\mu_m - 1))\,(H_k x_k + \alpha_a\mu_a). \end{aligned} \tag{14}$$

The expectation of (14) with respect to the pdf $\mathcal{N}(\hat{x}_{k|k-1},\, P_{k|k-1})$ is given by

$$\begin{aligned} \hat{y}_{k|k-1} &= E_{\text{pr}}[E[y_k \mid x_k]] = \alpha_b H_k\hat{x}_{k|k-1} + (1 - \alpha_b)\alpha_c \\ &\times (1 + \alpha_m(\mu_m - 1))\,(H_k\hat{x}_{k|k-1} + \alpha_a\mu_a). \end{aligned} \tag{15}$$

Now, we aim to compute $\mathbb{V}_{\text{pr}}$. To this end, we calculate the difference between $E[y_k \mid x_k]$ and $\hat{y}_{k|k-1}$, which is given by

$$\begin{aligned} E[y_k \mid x_k] - \hat{y}_{k|k-1} &= \alpha_b H_k(x_k - \hat{x}_{k|k-1}) + (1 - \alpha_b) \\ &\times \alpha_c\,(1 + \alpha_m(\mu_m - 1))\,H_k(x_k - \hat{x}_{k|k-1}). \end{aligned} \tag{16}$$

Using (16), we calculate $\mathbb{V}_{\text{pr}}\,[E\,[y_k \mid x_k]]$ as follows:

$$\begin{aligned} &\mathbb{V}_{\text{pr}}\,[E\,[y_k \mid x_k]] = E_{\text{pr}}\big[(E[y_k \mid x_k] - \hat{y}_{k|k-1})(E[y_k \mid x_k] \\ &- \hat{y}_{k|k-1})^\top\big] = \Big(\alpha_b^2 + 2\alpha_b(1 - \alpha_b)\alpha_c\big(1 + \alpha_m(\mu_m - 1)\big) \\ &+ (1 - \alpha_b)^2\alpha_c^2\big(1 + \alpha_m(\mu_m - 1)\big)^2\Big)H_k P_{k|k-1}H_k^\top. \end{aligned} \tag{17}$$

Next, we aim to compute the variance of $(y_k \mid x_k)$, denoted as $\mathbb{V}[y_k \mid x_k]$. Before doing so, we first determine the following:

$$\begin{aligned} &y_k - E\,[y_k \mid x_k] = (\xi_{b,k} - \alpha_b)H_k x_k + \xi_{b,k}\nu_k + (1 - \xi_{b,k})\xi_{c,k} \\ &\big(1 + \xi_{m,k}(m_k - 1)\big)\Big(\xi_{a,k}(a_k - \mu_a) + (\xi_{a,k} - \alpha_a)\mu_a + \nu_k\Big) + \\ &\Big((1 - \xi_{b,k})\xi_{c,k}\big(1 + \xi_{m,k}(m_k - 1)\big) - (1 - \alpha_b)\alpha_c\big(1 + \alpha_m \\ &\times (\mu_m - 1)\big)\Big)(H_k x_k + \alpha_a\mu_a). \end{aligned}$$

Using (13) and Lemma 1, we compute $\mathbb{V}[y_k \mid x_k]$ as follows:

$$\begin{aligned} &\mathbb{V}[y_k \mid x_k] = E\left[(y_k - E\,[y_k \mid x_k])\,(y_k - E\,[y_k \mid x_k])^\top \mid x_k\right] \\ &= E\big[(\xi_{b,k} - \alpha_b)^2\big]E\big[H_k x_k x_k^\top H_k^\top\big] + E[\xi_{b,k}^2]E[\nu_k\nu_k^\top] + \\ &E\left[(1 - \xi_{b,k})^2\xi_{c,k}^2\big(1 + \xi_{m,k}(m_k - 1)\big)^2\right]E\Big[\big(\xi_{a,k}\,(a_k - \mu_a) \\ &+ (\xi_{a,k} - \alpha_a)\,\mu_a\big)\big(\xi_{a,k}\,(a_k - \mu_a) + (\xi_{a,k} - \alpha_a)\,\mu_a\big)^\top + \nu_k\nu_k^\top\Big] \\ &+ E\left[\Big((1 - \xi_{b,k})\xi_{c,k}\,(1 + \xi_{m,k}(m_k - 1)) - (1 - \alpha_b)\alpha_c(1 + \alpha_m \right. \\ &\left.\times(\mu_m - 1))\Big)^2\right]E\left[(H_k x_k + \alpha_a\mu_a)(H_k x_k + \alpha_a\mu_a)^\top \mid x_k\right] \\ &= (1 - \alpha_b)\alpha_b H_k E[x_k x_k^\top]H_k^\top + \alpha_b R_k + (1 - \alpha_b)\alpha_c\big(\alpha_m(\sigma_m^2 + \\ &\mu_m^2) + (1 - \alpha_m)\big)\big(\alpha_a\Sigma_a + \alpha_a(1 - \alpha_a)\mu_a\mu_a^\top + R_k\big) + (1 - \alpha_b) \\ &\alpha_c\Big(\big\{(1 - \alpha_m) + \alpha_m(\mu_m^2 + \sigma_m^2)\big\} - (1 - \alpha_b)\alpha_c(1 + \alpha_m(\mu_m - \\ &1))^2\Big)\big(H_k x_k x_k^\top H_k^\top + \alpha_a H_k x_k\mu_a^\top + \alpha_a\mu_a x_k^\top H_k^\top + \alpha_a^2\mu_a\mu_a^\top\big). \end{aligned}$$

The expectation of $\mathbb{V}\,[y_k \mid x_k]$ with respect to prior pdf $\mathcal{N}(\hat{x}_{k|k-1},\, P_{k|k-1})$ is given below:

$$\begin{aligned} &E_{\text{pr}}\,[\mathbb{V}\,[y_k \mid x_k]] = (1 - \alpha_b)\alpha_b H_k(P_{k|k-1} + \hat{x}_{k|k-1}\hat{x}_{k|k-1}^\top) \\ &\times H_k^\top + \alpha_b R_k + (1 - \alpha_b)\alpha_c\big(\alpha_m(\sigma_m^2 + \mu_m^2) + (1 - \alpha_m)\big) \\ &\big(\alpha_a\Sigma_a + \alpha_a(1 - \alpha_a)\mu_a\mu_a^\top + R_k\big) + (1 - \alpha_b)\alpha_c\Big(\big\{(1 - \alpha_m) \\ &+ \alpha_m(\mu_m^2 + \sigma_m^2)\big\} - (1 - \alpha_b)\alpha_c(1 + \alpha_m(\mu_m - 1))^2\Big) \\ &\Big(H_k\big(P_{k|k-1} + \hat{x}_{k|k-1}\hat{x}_{k|k-1}^\top\big)H_k^\top + \alpha_a H_k\hat{x}_{k|k-1}\mu_a^\top \\ &+ \alpha_a\mu_a\hat{x}_{k|k-1}^\top H_k^\top + \alpha_a^2\mu_a\mu_a^\top\Big). \end{aligned} \tag{18}$$

The expression for $P_{k|k-1}^{yy}$ is derived by adding (17) and (18) as given in (8). Using (9) and (16), we compute $P_{k|k-1}^{yx}$ as

$$\begin{aligned} P_{k|k-1}^{yx} &= E_{\text{pr}}\left[\big(E[y_k \mid x_k] - \hat{y}_{k|k-1}\big)\left(x_k - \hat{x}_{k|k-1}\right)^\top\right] \\ &= \Big(\alpha_b + (1 - \alpha_b)\alpha_c\big(1 + \alpha_m(\mu_m - 1)\big)\Big)H_k P_{k|k-1}. \end{aligned} \tag{19}$$

After computing these moments, we can evaluate the parameters of the GSLR approximated measurement model given in (6). Let us denote the set of parameters related to process dynamics, the measurement model, DoS and FDI attacks as $\Theta_k = [A_k, H_k, Q_k, R_k, \alpha_a, \alpha_b, \alpha_c, \alpha_m, \mu_a, \Sigma_a, \mu_m, \sigma_m^2]$. The pseudo-code for computing the GSLR parameters is presented in Algorithm 1.

Algorithm 1 Computation of GSLR parameters

function $[H_k^+, b_k^+, \tilde{\Omega}_k] = \text{GSLR}(\hat{x}_{k|k-1}, P_{k|k-1}, \Theta_k)$.
  Obtain $\hat{y}_{k|k-1}$, $P^{yy}_{k|k-1}$, and $P^{yx}_{k|k-1}$ following (15), (8), and (19), respectively.
  Compute H_k^+, b_k^+, and $\tilde{\Omega}_k$ using (6).
end function

IV. Kalman Filter and RTS Smoother under Cyber-Attacks

In this section, we derive the Kalman filter and RTS smoother based on the linear SSM (1)-(2) and the GSLR-based approximated faulty measurement model (5). The smoothing algorithm consists of two sequential steps: (i) the forward pass and (ii) the backward pass. In forward pass, the Kalman filtering algorithm is used to compute the prior and posterior moments. Using [7, Lemma A.3], the marginal distribution of x_k is $p(x_k \mid y_{1:k-1}) = \mathcal{N}(x_k \mid \hat{x}_{k|k-1}, P_{k|k-1})$, where

$$\hat{x}_{k|k-1} = A_{k-1}\hat{x}_{k-1|k-1}, \tag{20}$$
$$P_{k|k-1} = A_{k-1}P_{k-1|k-1}A_{k-1}^\top + Q_{k-1}. \tag{21}$$

Next, we compute the joint distribution of the state, x_k and the GSLR-based approximated measurement, y_k given $y_{1:k-1}$ as follows:

$$\begin{aligned} &p(x_k, y_k \mid y_{1:k-1}) = p(y_k \mid x_k)\, p(x_k \mid y_{1:k-1}) \\ &\approx \mathcal{N}(y_k \mid H_k^+ x_k + b_k^+, \tilde{\Omega}_k)\, \mathcal{N}(x_k \mid \hat{x}_{k|k-1}, P_{k|k-1}) \\ &\approx \mathcal{N}\left(\begin{bmatrix} x_k \\ y_k \end{bmatrix} \middle| \hat{\mathcal{X}}_k, \mathcal{P}_k \right), \end{aligned}$$

where

$$\hat{\mathcal{X}}_k = \begin{bmatrix} \hat{x}_{k|k-1} \\ H_k^+ \hat{x}_{k|k-1} + b_k^+ \end{bmatrix},$$
$$\mathcal{P}_k = \begin{bmatrix} P_{k|k-1} & P_{k|k-1}H_k^{+\top} \\ H_k^+ P_{k|k-1} & H_k^+ P_{k|k-1} H_k^{+\top} + \tilde{\Omega}_k \end{bmatrix}.$$

The conditional probability distribution of x_k given $y_{1:k}$ is

$$p(x_k \mid y_{1:k}) \approx \mathcal{N}(x_k \mid \hat{x}_{k|k}, P_{k|k}),$$

where

$$\begin{aligned} \hat{x}_{k|k} = \hat{x}_{k|k-1} &+ P_{k|k-1}H_k^{+\top}(H_k^+ P_{k|k-1} H_k^{+\top} + \tilde{\Omega}_k)^{-1} \\ &\times (y_k - H_k^+ \hat{x}_{k|k-1} - b_k^+), \end{aligned} \tag{22}$$
$$\begin{aligned} P_{k|k} = P_{k|k-1} &- P_{k|k-1}H_k^{+\top}(H_k^+ P_{k|k-1} H_k^{+\top} + \tilde{\Omega}_k)^{-1} \\ &\times H_k^+ P_{k|k-1}. \end{aligned} \tag{23}$$

After computing $p(x_k \mid y_{1:k}) \approx \mathcal{N}(x_k \mid \hat{x}_{k|k}, P_{k|k})$ for $k \in \{1, \ldots, T\}$, we perform the backward pass step to recursively compute $p(x_k \mid y_{1:T}) = \mathcal{N}(x_k \mid \hat{x}^s_{k|T}, P^s_{k|T})$ starting from $k = T$. Note that the smoothing algorithm is independent of the measurement model, allowing us to directly apply the standard smoothing algorithm for the linear affine SSM [7, pp. 255–260]. The detailed implementation of the Kalman filtering and smoothing solution for the attacked model is presented in Algorithm 2.

Algorithm 2 Kalman filter and RTS smoother for the attacked model

function $[\hat{x}_{k|k}, P_{k|k}, \hat{x}^s_{k|T}, P^s_{k|T}] = \text{KFS}(\hat{x}_{0|0}, P_{0|0}, \Theta_k)$.
  for $k = 1, \ldots, T$ **do**
    Compute $\hat{x}_{k|k-1}$ and $P_{k|k-1}$ using Eqs. (20)-(21).
    $[H_k^+, b_k^+, \tilde{\Omega}_k] = \text{GSLR}(\hat{x}_{k|k-1}, P_{k|k-1}, \Theta_k)$.
    Compute $\hat{x}_{k|k}$ and $P_{k|k}$ following Eqs. (22)-(23).
  end for
  $\hat{x}^s_{T|T} = \hat{x}_{T|T}$ and $P^s_{T|T} = P_{T|T}$.
  for $k = T-1, \ldots, 1$ **do**
    $K_s = P_{k|k}A_k^\top P^{-1}_{k+1|k}$.
    $\hat{x}^s_{k|T} = \hat{x}_{k|k} + K_s(\hat{x}^s_{k+1|T} - \hat{x}_{k+1|k})$.
    $P^s_{k|T} = P_{k|k} + K_s(P^s_{k+1|T} - P_{k+1|k})K_s^\top$.
  end for
end function

V. Simulation Results

We consider an air-traffic control scenario [23], in which an aircraft performs a maneuver in a two-dimensional space with a known turn rate. The discrete-time dynamics of the maneuvering aircraft can be expressed as

$$x_k = \begin{bmatrix} 1 & 0 & \frac{\sin\omega t}{\omega} & -\frac{1-\cos\omega t}{\omega} \\ 0 & 1 & \frac{1-\cos\omega t}{\omega} & \frac{\sin\omega t}{\omega} \\ 0 & 0 & \cos\omega t & -\sin\omega t \\ 0 & 0 & \sin\omega t & \cos\omega t \end{bmatrix} x_{k-1} + \eta_{k-1},$$

where the state of the aircraft, $x = \begin{bmatrix} x_1 & x_2 & \dot{x}_1 & \dot{x}_2 \end{bmatrix}^\top$, (x_1, x_2) and $(\dot{x}_1, \dot{x}_2)$ represent the position and velocity of the aircraft in the x and y directions, respectively, $t = 0.05$ s is the sampling time, and $\omega = 3^\circ$/s is turn rate. The process noise $\eta_{k-1} \sim \mathcal{N}(0, Q)$ with $Q = \text{diag}(0.3^2, 0.3^2, 0.05^2, 0.05^2)$. The measurement available to the estimator is the position of the aircraft, that is

$$z_k = \begin{bmatrix} I_{2\times 2} & 0_{2\times 2} \end{bmatrix} x_k + \nu_k,$$

where $\nu_k \sim \mathcal{N}(0, R)$ with $R = \text{diag}(12, 12)$. We perform the simulation for 20 s. The following parameters associated with the cyber-attacks are used in the simulation: $\alpha_a = 0.3$, $\alpha_b = 0.7$, $\alpha_c = 0.9$, $\alpha_m = 0.1$, $m_k \sim \mathcal{N}(0.95, 0.10^2)$ and $a_k \sim \mathcal{N}(\mu_a, \Sigma_a)$, where $\mu_a = \begin{bmatrix} 0.7 & 0.9 \end{bmatrix}^\top$ and $\Sigma_a = \text{diag}(1, 0.5)$. We initialize the estimator with $x_0 = \begin{bmatrix} 200\,\text{m} & 200\,\text{m} & 15\,\text{m/s} & 15\,\text{m/s} \end{bmatrix}^\top$, $\hat{x}_{0|0} = \begin{bmatrix} 250\,\text{m} & 150\,\text{m} & 12\,\text{m/s} & 17\,\text{m/s} \end{bmatrix}^\top$, and $P_{0|0} = \text{diag}(10^2\,\text{m}^2, 10^2\,\text{m}^2, 4^2\,\text{m}^2/\text{s}^2, 4^2\,\text{m}^2/\text{s}^2)$.

We implemented the standard KF, the standard RTSS, the proposed filtering algorithm (that is, the forward pass of Algorithm 2), and the RTS smoother, referring to them as the proposed KF and proposed RTSS. Fig. 2 shows the simulated true aircraft trajectory, the measurements under cyber-attacks, and the estimated trajectory obtained using the proposed KF and RTSS in a single Monte Carlo (MC) run. Notably, Fig. 2 demonstrates that the proposed KF and RTSS effectively track the aircraft even in the presence of cyber-attacks.

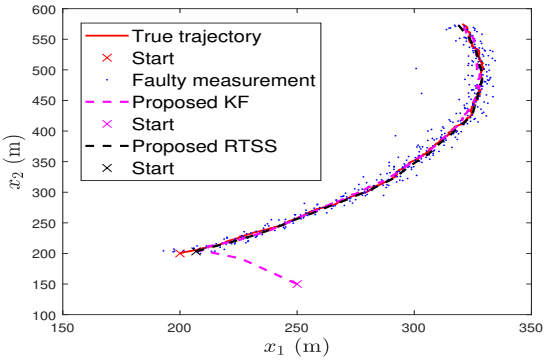
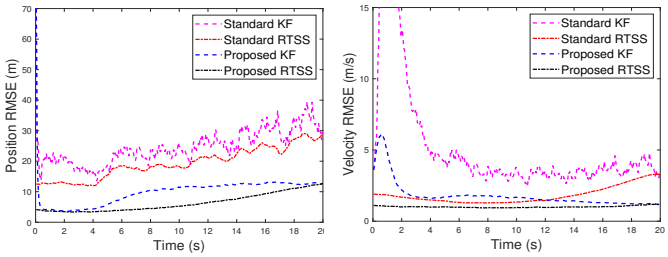


Fig. 2 The true trajectory, faulty measurement, the proposed KF and RTSS for the aircraft tracking problem in the presence of cyber-attacks in a single representative run.



(a) Position RMSE (b) Velocity RMSE

Fig. 3 The position and velocity RMSE of different estimators for the aircraft tracking problem under DoS and FDI attacks, obtained from 100 MC runs.

We evaluate the estimators' performance in terms of the position and velocity root mean square error (RMSE). Fig. 3 presents the position and velocity RMSE of the different estimators obtained from 100 MC runs. The results indicate that the proposed KF and RTSS achieve lower RMSE compared to the standard estimators under cyber-attacks.

VI. Conclusion

In this article, we have developed a Kalman filter and RTS smoother for the linear SSM under DoS and FDI attacks. We reformulated the faulty measurement model that accounts for DoS and simultaneous additive and multiplicative FDI attacks. We approximated the faulty measurement model using the conditional expectation from the GSLR method. The GSLR-based approximated measurement model was used to derive the filtering and smoothing algorithms. The performance of the methods was illustrated in a simulated aircraft tracking experiment. In the future, we plan to extend this method to nonlinear state-space models.

References

[1] J. Hu, Z. Wang, D. Chen, and F. E. Alsaadi, "Estimation, filtering and fusion for networked systems with network-induced phenomena: New progress and prospects," *Information Fusion*, vol. 31, pp. 65–75, 2016.

[2] X. M. Zhang, Q. L. Han, and X. Yu, "Survey on recent advances in networked control systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1740–1752, 2015.

[3] C. Wu, Z. Hu, J. Liu, and L. Wu, "Secure estimation for cyber-physical systems via sliding mode," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3420–3431, 2018.

[4] H. M. Khalid and J. C. H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.

[5] L. Zhang, H. Gao, and O. Kaynak, "Network-induced constraints in networked control systems—A survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 403–416, 2012.

[6] H. E. Rauch, F. Tung, and C. T. Striebel, "Maximum likelihood estimates of linear dynamic systems," *AIAA journal*, vol. 3, no. 8, pp. 1445–1450, 1965.

[7] S. Särkkä and L. Svensson, *Bayesian filtering and smoothing*, 2nd ed. Cambridge University Press, 2023.

[8] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2009, pp. 911–918.

[9] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

[10] S. Chen, Q. Zhang, D. Lin, and S. Wang, "A class of nonlinear Kalman filters under a generalized measurement model with false data injection attacks," *IEEE Signal Processing Letters*, vol. 29, pp. 1187–1191, 2022.

[11] A. K. Singh, S. Kumar, N. Kumar, and R. Radhakrishnan, "Bayesian approximation filtering with false data attack on network," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 2, pp. 976–988, 2021.

[12] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control (CDC)*. IEEE, 2010, pp. 5967–5972.

[13] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[15] K. Kumar, M. Iqbal, and S. Särkkä, "Risk-sensitive filtering under false data injection attacks," in *2024 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI)*. IEEE, 2024, pp. 1–6.

[16] S. Liu, G. Wei, Y. Song, and Y. Liu, "Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks," *Neurocomputing*, vol. 207, pp. 708–716, 2016.

[17] J. Lu, W. Wang, L. Li, and Y. Guo, "Unscented Kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks," *Asian Journal of Control*, vol. 23, no. 2, pp. 871–881, 2021.

[18] Y. W. Lv and G. H. Yang, "An adaptive cubature Kalman filter for nonlinear systems against randomly occurring injection attacks," *Applied Mathematics and Computation*, vol. 418, p. 126834, 2022.

[19] G. Kumar, A. K. Naik, R. Swaminathan, and A. K. Singh, "Gaussian filtering with cyber-attacked data," *IEEE Signal Processing Letters*, vol. 31, pp. 546–550, 2024.

[20] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation: Theory Algorithms and Software*. John Wiley & Sons, 2002.

[21] F. Tronarp, A. F. García-Fernández, and S. Särkkä, "Iterative filtering and smoothing in nonlinear and non-Gaussian systems using conditional moments," *IEEE Signal Processing Letters*, vol. 25, no. 3, pp. 408–412, 2018.

[22] R. Hostettler, F. Tronarp, A. F. García-Fernández, and S. Särkkä, "Importance densities for particle filtering using iterated conditional expectations," *IEEE Signal Processing Letters*, vol. 27, pp. 211–215, 2020.

[23] I. Arasaratnam and S. Haykin, "Cubature Kalman filters," *IEEE Transactions on Automatic Control*, vol. 54, no. 6, pp. 1254–1269, 2009.