2024 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI) | 979-8-3503-6803-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/MFI62651.2024.10705765

Risk-Sensitive Filtering under False Data Injection Attacks

Kundan Kumar, Muhammad Iqbal, and Simo Särkkä

***Abstract*— This paper addresses a risk-sensitive remote estimation problem for cyber-physical systems (CPSs) where the accurate model of a dynamic system is not completely known or may differ from the assumed model. In CPSs, sensors and the monitoring control center are remotely located. Sensors transmit the measurements via unreliable wireless communication channels that are vulnerable to cyber-attacks. Specifically, attackers can inject false data to alter the measurements in the communication channel or attack sensors. To tackle this, we design a risk-sensitive filtering algorithm to operate under false data injection attacks. The proposed estimator aims to minimize the risk-sensitive error criterion, defined as the expectation of the accumulated exponential quadratic error. Simulation results demonstrate the effectiveness of the proposed algorithm.**

I. INTRODUCTION

In recent years, addressing estimation issues within cyber-physical systems (CPSs) has become a topic of significant interest [1], [2]. This is owing to their extensive applications in diverse fields such as advanced healthcare, intelligent transportation, power grids, terrestrial exploration, hazardous environments, and among others [3]–[5]. The CPSs enable users to monitor and control physical systems remotely via wireless communication channels.

In the CPSs, the sensor measurements are transmitted to the remotely located computing units through unreliable wireless communication channels. In such scenarios, various interferences occur in measurements, such as random delay, packet dropout, measurement fading, and others, which degrade the performance of the estimators [6]–[9]. The strong dependencies on the wireless channel also make the CPSs vulnerable to cyber-attacks. Various attack models are considered in the literature, such as denial of service (DoS) attacks [10], replay attacks [11], and false data injection attacks (FDIA) [12]–[16]. Contrary to the DoS attacks, which target the communication network, FDIA targets sensors, actuators and communication channels [17]. In such case, the intruders have access to the measurement data and can alter the measurement arbitrarily [12], [15]. In addition, the false injection can be chosen such that the dynamical system can be destabilized [18]. Solving state estimation problems in CPSs becomes challenging in the presence of FDIA.

The state estimation algorithm computes the marginal posterior distribution of the state at each time step, given the history of measurements [19], [20]. For linear Gaussian systems, a closed-form solution can be exactly computed using the Kalman filter (KF) [19], [21]. The Kalman filter is developed based on the assumption that the system and measurement models are known. However, in practice, the system model is not completely known or slightly deviates from the assumed nominal model. For such kinds of problems, several robust estimation algorithms are developed [22]–[29]. These robust algorithms provide good performance under nominal conditions and acceptable performance under nonnominal conditions [27].

This paper addresses the risk-sensitive estimation problem for uncertain dynamic systems under false data injection attacks. The uncertainty in the model is related to the dynamics, which signifies the deviation from the assumed nominal model [27]. The model uncertainty is unknown and deterministic, and it is not related to the process noise. The measurement received at the remote estimator may be affected by the false data injection attacks on the communication channels or sensors in CPSs. In this paper, we derive a cost function by considering the exponential of the past and present squared estimation errors for the linear Gaussian state-space model, and by minimizing this cost function, we obtain a closed-form solution.

The primary contribution of this article is the development of a closed-form solution for linear Gaussian systems that accounts for model uncertainty and false data injection attacks in the measurements. We also demonstrate the performance of the proposed method through numerical simulations. A schematic diagram of the proposed method is illustrated in Fig. 1.

II. PROBLEM FORMULATION

Consider a discrete-time stochastic dynamic system with the following state-space model [19]:

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

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

where $x_k \in \mathbb{R}^{n_x}$ is the state of the dynamic system, and $z_k \in \mathbb{R}^{n_z}$ is the sensor measurement. The state transition matrix is $A_{k-1} \in \mathbb{R}^{n_x \times n_x}$, and the measurement matrix is $C_k \in \mathbb{R}^{n_z \times n_x}$. The process noise η_{k-1} and the measurement noise ν_k are assumed to be uncorrelated white Gaussian noise with mean zero and covariances Q_{k-1} and R_k, respectively. The initial state $x_0 \sim \mathcal{N}(\hat{x}_{0|0}, P^{xx}_{0|0})$, η_{k-1}, and ν_k are mutually independent.

A. Model mismatch scenario

In many applications, an accurate stochastic model of the system is unavailable; in such cases, the system model

The authors are with the Department of Electrical Engineering and Automation, Aalto University, Finland (kundan.kumar@aalto.fi; muhammad.iqbal@aalto.fi; simo.sarkka@aalto.fi).

Authorized licensed use limited to: AALTO UNIVERSITY. Downloaded on October 11,2024 at 11:33:13 UTC from IEEE Xplore. Restrictions apply.

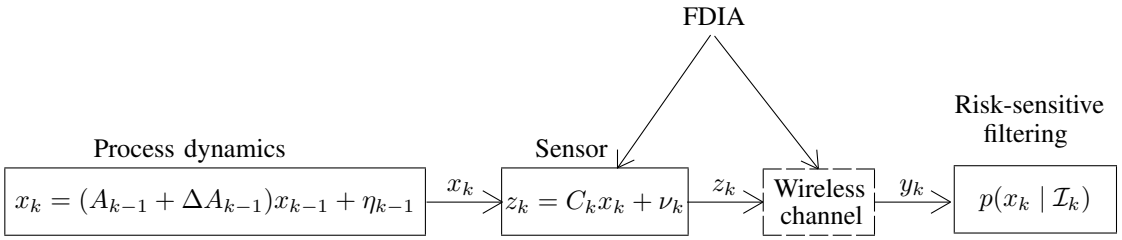


Fig. 1. Schematic diagram of the proposed risk-sensitive estimation algorithm under false data injection attacks.

differs from the assumed model. The process dynamics with uncertainty can be represented as [27], [29]

$$x_k = (A_{k-1} + \Delta A_{k-1})x_{k-1} + \eta_{k-1}, \tag{3}$$

where ΔA_{k-1} is an unknown, arbitrary, and deterministic model uncertainty. The model uncertainty in (3) is an intrinsic aspect of the plant dynamics, signifying that the values of one or more process parameters deviate from their nominal assumptions.

B. Measurement model under false data injection attacks

Refer to Fig. 1, sensors send measurements to the remotely located estimator through the unreliable communication network. The attacker may inject false data since wireless channels are vulnerable to cyber-attacks. The measurement equation under false data injection attacks (FDIA) can be expressed as

$$y_k = z_k + \xi_k a_k, \tag{4}$$

where $y_k \in \mathbb{R}^{n_z}$ is the measurement under FDIA, and $a_k \sim \mathcal{N}(\mu, \Sigma)$ is false data attack model. The measurement model is designed based on the Bernoulli random variable $\xi_k \in \{0, 1\}$ as follows:

$$\begin{aligned} &Pr(\xi_k = 1) = \mathbb{E}[\xi_k] = \mathbb{E}[\xi_k^m] = \mathrm{p}, \\ &Pr(\xi_k = 0) = \mathbb{E}[(1-\xi_k)^m] = \mathbb{E}[1-\xi_k] = 1-\mathrm{p}, \\ &\mathbb{E}[(\xi_k - \mathrm{p})^2] = (1-\mathrm{p})\mathrm{p}, \end{aligned} \tag{5}$$

where m is any positive integer, $Pr : \mathcal{F} \to [0, 1]$ is the probability measure in the probability space $(\Omega, \mathcal{F}, Pr)$ with sigma-algebra $\mathcal{F}$ of an event in the sample space Ω, and $\mathbb{E}$ is the expectation operator.

Remark 1: For the purpose of stealthiness, the attacker follows the Bernoulli model to manipulate the data abruptly.

III. Risk-Sensitive Filtering under False Data Injection Attacks

In this section, we develop a risk-sensitive KF under the FDIA based on the minimization of the risk-sensitive error criterion.

A. Objective

Our aim is to find an optimal posterior estimate $\hat{x}^*_{k|k}$ given the measurements $y_{1:k}, k \in \{1, 2, \ldots\}$ for (3)-(4). We consider a risk-sensitive cost function [27], [29]

$$\begin{aligned} \mathcal{L}_k(\hat{x}_{k|k}|y_{1:k}) =& \mathbb{E}\Bigg[\exp\Big(\sum_{i=0}^{k-1} \mu_i^1 (x_i - \hat{x}_{i|i})^\top (x_i - \hat{x}_{i|i}) \\ &+ \mu_k^2 (x_k - \hat{x}_{k|k})^\top (x_k - \hat{x}_{k|k})\Big)\Bigg], \end{aligned} \tag{6}$$

where $\mathbb{E}[\cdot]$ represent the expectation over the posterior density of x_k and the statistics of ξ_k. The error cost function is scaled by two time-varying risk-sensitive parameters $\mu_i^1 > 0$ and $\mu_k^2 > 0$, which are used for scaling the past errors and present error, respectively. Since $\hat{x}_{k|k}$ is unknown, and $\hat{x}_{i|i}$, $i = 0 : k-1$ is known and represented with $\hat{x}^*_{i|i}$, the cost function in (6) can be written as

$$\mathcal{L}_k(\hat{x}_{k|k} \mid y_{1:k}) = \mathbb{E}\left[\exp\Big(\sum_{i=0}^{k-1} \mu_i^1 e^{*\top}_{i|i} e^*_{i|i} + \mu_k^2 e^\top_{k|k} e_{k|k}\Big)\right], \tag{7}$$

where $e^*_{i|i} = (x_i - \hat{x}^*_{i|i})$, and $e_{k|k} = (x_k - \hat{x}_{k|k})$. Our objective is to estimate the state estimate at each time step, which minimizes (7)

$$\hat{x}^*_{k|k} = \arg\min_{\hat{x}_{k|k}} \mathcal{L}_k(\hat{x}_{k|k} \mid y_{1:k}). \tag{8}$$

B. Bayesian framework of filtering

The Kalman filter computes the marginal posterior distribution of the state x_k at each time step k provided the measurements $y_{1:k}$, that is, $p(x_k \mid y_{1:k})$. The density function $p(x_k \mid y_{1:k})$ is constructed recursively in two steps: (i) prediction step and (ii) update step. Using the information $p(x_{k-1} \mid y_{1:k-1})$, the predictive distribution of state x_k can be computed following the Chapman-Kolmogorov equation [19]

$$p(x_k \mid y_{1:k-1}) = \int p(x_k \mid x_{k-1})\, p(x_{k-1} \mid y_{1:k-1})\, \mathrm{d}x_{k-1}. \tag{9}$$

After receiving the measurement y_k, the posterior distribution of the state x_k is computed using Bayes' rule [19]

$$p(x_k \mid y_{1:k}) = \frac{p(y_k \mid x_k)\, p(x_k \mid y_{1:k-1})}{\gamma_k}, \tag{10}$$

Authorized licensed use limited to: AALTO UNIVERSITY. Downloaded on October 11,2024 at 11:33:13 UTC from IEEE Xplore. Restrictions apply.

where the normalization constant γ_k is

$$\gamma_k = \int p(y_k \mid x_k)\, p(x_k \mid y_{1:k-1}) \mathrm{d}x_k.$$

C. Background on risk-sensitive filtering

Consider the information set available at time step k is $\mathcal{I}_k = \{y_{1:k}, e_{1|1}, \ldots, e_{k-1|k-1}\}$. The conditional posterior information state is defined as [20, p. 373], [29]

$$\begin{aligned}\zeta_k &\triangleq p(x_k \mid \mathcal{I}_k) \\ &= \exp\Big(\sum_{i=0}^{k-1} \mu_i^1 e_{i|i}^\top e_{i|i}\Big)\, p(x_k \mid y_{1:k}),\ \forall\, k \in \{1, 2, \ldots\}\end{aligned} \tag{11}$$

where the initial posterior information state is $\zeta_0 = p(x_0) \sim \mathcal{N}(\hat{x}_{0|0},\, P_{0|0}^{xx})$. Next, substituting (9) and (10) into (11), we get

$$\begin{aligned}\zeta_k &= \frac{p(y_k \mid x_k)}{\gamma_k} \int p(x_k \mid x_{k-1})\ \exp(\mu_{k-1}^1 e_{k-1|k-1}^\top \\ &\quad \times e_{k-1|k-1})\ \exp\Big(\sum_{i=0}^{k-2} \mu_i^1 e_{i|i}^\top e_{i|i}\Big)\, p(x_{k-1} \mid y_{1:k-1})\, \mathrm{d}x_{k-1}, \\ &= \frac{p(y_k \mid x_k)}{\gamma_k} \int p(x_k \mid x_{k-1})\ \exp(\mu_{k-1}^1 e_{k-1|k-1}^\top \\ &\quad \times e_{k-1|k-1})\, \zeta_{k-1}\, \mathrm{d}x_{k-1}.\end{aligned} \tag{12}$$

Defining the predicted information state density $p(x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1})$, as follows [29]:

$$\begin{aligned}p(x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}) &= \int p(x_k \mid x_{k-1}) \\ &\quad \times \exp(\mu_{k-1}^1 e_{k-1|k-1}^\top e_{k-1|k-1})\, \zeta_{k-1} \mathrm{d}x_{k-1}.\end{aligned} \tag{13}$$

Using (13), the posterior density for the information state (12) can be written as

$$\zeta_k = \frac{p(y_k \mid x_k)}{\gamma_k} p(x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}). \tag{14}$$

The cost function (7) is re-written as

$$\begin{aligned}\mathcal{L}_k(\hat{x}_{k|k} \mid y_{1:k}) = \int \exp\Big(\sum_{i=0}^{k-1} \mu_i^1 e_{i|i}^\top e_{i|i} + \mu_k^2 e_{k|k}^\top e_{k|k}\Big) \\ \times\, p(x_k \mid y_{1:k})\, \mathrm{d}x_k.\end{aligned} \tag{15}$$

Using (11), (15) can be written as

$$\mathcal{L}_k(\hat{x}_{k|k} | y_{1:k}) = \int \exp(\mu_k^2 e_{k|k} e_{k|k}^\top)\, \zeta_k\, \mathrm{d}x_k. \tag{16}$$

In the sequel, we solve (8) using (13)-(16) to obtain risk-sensitive estimate of the dynamical system given in (3) with the measurement model (4) under the false data injection attacks.

D. Risk-sensitive filtering under FDIA

In this subsection, we derive a prediction and an update steps for the risk-sensitive filtering under FDIA. Since ζ_0 follows the Gaussian distribution with mean $\hat{x}_{0|0}$ and covariance $P_{0|0}^{xx}$. Consequently, ζ_{k-1} follows the unnormalized Gaussian distribution, represented as [27], [29]

$$\begin{aligned}\zeta_{k-1} = &\frac{C_1}{\sqrt{(2\pi)^{n_x} |P_{k-1|k-1}^{xx}|}} \exp\Big(-\frac{1}{2} e_{k-1|k-1}^\top \\ &\times (P_{k-1|k-1}^{xx})^{-1} e_{k-1|k-1}\Big),\end{aligned} \tag{17}$$

where $C_1 = \exp\big(\sum_{i=0}^{k-2} \mu_i^1 e_{i|i}^\top e_{i|i}\big)$. Substituting (17) into (13), we get

$$\begin{aligned}&p(x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}) \\ &= C_2 \int p(x_k \mid x_{k-1})\ \exp\big(e_{k-1|k-1}^\top (\mu_{k-1}^1 I) e_{k-1|k-1}\big) \\ &\quad \times \exp\big(-\frac{1}{2} e_{k-1|k-1}^\top (P_{k-1|k-1}^{xx})^{-1} e_{k-1|k-1}\big)\, \mathrm{d}x_{k-1} \\ &= C_2 \int p(x_k \mid x_{k-1}) \exp\Big[-\frac{1}{2}\Big\{ e_{k-1|k-1}^\top (P_{k-1|k-1}^{xx})^{-1} \\ &\times e_{k-1|k-1} + e_{k-1|k-1}^\top (-2\mu_{k-1}^1 I) e_{k-1|k-1}\Big\}\Big] \mathrm{d}x_{k-1} \\ &= C_2 \int p(x_k \mid x_{k-1}) \exp\Big[-\frac{1}{2}\Big\{ e_{k-1|k-1}^\top \Big((P_{k-1|k-1}^{xx})^{-1} \\ &\quad - 2\mu_{k-1}^1 I\Big) e_{k-1|k-1}\Big\}\Big] \mathrm{d}x_{k-1},\end{aligned} \tag{18}$$

where $C_2 = \dfrac{C_1}{\sqrt{(2\pi)^{n_x} |P_{k-1|k-1}^{xx}|}}$, μ_{k-1}^1 is a non-negative real number such that $2\mu_{k-1}^1 P_{k-1|k-1}^{xx} < I$ for every k, and I is an identity matrix. Denoting $\mathcal{P}_{k-1} = \Big((P_{k-1|k-1}^{xx})^{-1} - 2\mu_{k-1}^1 I\Big)^{-1}$, (18) can be rewritten as

$$\begin{aligned}&p(x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}) = \\ &C_2 \int p(x_k \mid x_{k-1})\, \mathcal{N}\big(x_{k-1} \mid \hat{x}_{k-1|k-1},\, \mathcal{P}_{k-1}\big)\, \mathrm{d}x_{k-1}.\end{aligned} \tag{19}$$

From (19), we write

$$p(x_{k-1} \mid \mathcal{I}_{k-1}, e_{k-1|k-1}) = \mathcal{N}\big(x_{k-1} \mid \hat{x}_{k-1|k-1},\, \mathcal{P}_{k-1}\big). \tag{20}$$

The joint distribution of x_k and x_{k-1} given $\mathcal{I}_{k-1}, e_{k-1|k-1}$ can be expressed as

$$\begin{aligned}&p(x_{k-1}, x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}) \\ &= p(x_k \mid x_{k-1})\, p(x_{k-1} | \mathcal{I}_{k-1}, e_{k-1|k-1}) \\ &= \mathcal{N}(x_k \mid A_{k-1} x_{k-1},\, Q_{k-1})\, \mathcal{N}(x_{k-1} \mid \hat{x}_{k-1|k-1},\, \mathcal{P}_{k-1}) \\ &= \mathcal{N}\left(\begin{bmatrix} x_{k-1} \\ x_k \end{bmatrix} \middle| \hat{x}_2',\, P_2'\right),\end{aligned} \tag{21}$$

Authorized licensed use limited to: AALTO UNIVERSITY. Downloaded on October 11,2024 at 11:33:13 UTC from IEEE Xplore. Restrictions apply.

where

$$\hat{x}_2' = \begin{bmatrix} \hat{x}_{k-1|k-1} \\ A_{k-1}\hat{x}_{k-1|k-1} \end{bmatrix}, \tag{22}$$

and

$$P_2' = \begin{bmatrix} \mathcal{P}_{k-1} & \mathcal{P}_{k-1}A_{k-1}^\top \\ A_{k-1}\mathcal{P}_{k-1} & A_{k-1}\mathcal{P}_{k-1}A_{k-1}^\top + Q_{k-1} \end{bmatrix}. \tag{23}$$

We compute the marginal distribution of x_k following [19, Lemma A.3] as

$$p(x_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}) = \mathcal{N}\big(x_k \mid \hat{x}_{k|k-1},\, P^{xx}_{k|k-1}\big), \tag{24}$$

where

$$\begin{aligned} \hat{x}_{k|k-1} &= A_{k-1}\hat{x}_{k-1|k-1}, \\ P^{xx}_{k|k-1} &= A_{k-1}\mathcal{P}_{k-1}A_{k-1}^\top + Q_{k-1}. \end{aligned}$$

Next, we approximate the joint distribution of x_k and y_k given $\mathcal{I}_{k-1}, e_{k-1:k-1}$ as follows:

$$\begin{aligned} &p(x_k, y_k \mid \mathcal{I}_{k-1}, e_{k-1:k-1}) \\ &= p(y_k \mid x_k)\, p(x_k \mid \mathcal{I}_{k-1}, e_{k-1:k-1}) \\ &= \mathcal{N}(y_k \mid C_k x_k + \mathrm{p}\mu,\, R_k + \mathrm{p}\Sigma + (1-\mathrm{p})\mathrm{p}\mu\mu^\top) \\ &\quad \times \mathcal{N}(x_k \mid \hat{x}_{k|k-1},\, P^{xx}_{k|k-1}) \\ &= \mathcal{N}\left(\begin{bmatrix} x_k \\ y_k \end{bmatrix} \middle| \begin{bmatrix} \hat{x}_{k|k-1} \\ C_k\hat{x}_{k|k-1} + p\mu \end{bmatrix}, \begin{bmatrix} P^{xx}_{k|k-1} & P^{xy}_{k|k-1} \\ P^{yx}_{k|k-1} & P^{yy}_{k|k-1} \end{bmatrix} \right). \end{aligned} \tag{25}$$

Following [19, Lemma A.3], we compute the conditional distribution of x_k as follows:

$$\begin{aligned} &p(x_k \mid y_k, \mathcal{I}_{k-1}, e_{k-1|k-1}) = p(x_k \mid \mathcal{I}_k) \\ &= \mathcal{N}(x_k \mid \hat{x}_{k|k},\, P^{xx}_{k|k}), \end{aligned}$$

where

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + P^{xy}_{k|k-1}(P^{yy}_{k|k-1})^{-1}(y_k - \hat{y}_{k|k-1}), \tag{26}$$

$$P^{xx}_{k|k} = P^{xx}_{k|k-1} - P^{xy}_{k|k-1}(P^{yy}_{k|k-1})^{-1}(P^{xy}_{k|k-1})^\top. \tag{27}$$

To compute the posterior mean and covariance (26)-(27), we evaluate $\hat{y}_{k|k-1}$, $P^{yy}_{k|k-1}$, and $P^{xy}_{k|k-1}$. To that end, we provide the following lemma.

Lemma 1: The second-moment of $\big(\xi_k(a_k-\mu)+(\xi_k-\mathrm{p})\mu\big)$ can be written as:

$$\begin{aligned} &\mathbb{E}\big[\big(\xi_k(a_k-\mu)+(\xi_k-\mathrm{p})\mu\big)\big(\xi_k(a_k-\mu)+ \\ &(\xi_k-\mathrm{p})\mu\big)^\top\big] = \mathrm{p}\Sigma + \mathrm{p}(1-\mathrm{p})\mu\mu^\top. \end{aligned} \tag{28}$$

Proof: The proof is provided in Appendix A. ∎

Theorem 1: The expected value of the measurement conditioned on $\mathcal{I}_{k-1}, e_{k-1|k-1}$ is expressed as

$$\hat{y}_{k|k-1} = \mathbb{E}[y_k \mid \mathcal{I}_{k-1}, e_{k-1|k-1}] = C_k\hat{x}_{k|k-1} + \mathrm{p}\mu, \tag{29}$$

the innovation covariance of y_k is

$$P^{yy}_{k|k-1} = C_k P^{xx}_{k|k-1} C_k^\top + R_k + \mathrm{p}\Sigma + \mathrm{p}(1-\mathrm{p})\mu\mu^\top, \tag{30}$$

and the cross-covariance between state x_k and measurement y_k is given by

$$P^{xy}_{k|k-1} = P^{xx}_{k|k-1} C_k^\top. \tag{31}$$

Proof: The detailed proof is provided in Appendix B. ∎

The developed risk-sensitive filter under false data injection attack is presented in Algorithm 1. For the sake of simplicity, in Algorithm 1, we introduce $\Theta = \{A_k, C_k, Q_k, R_k, \mu, \Sigma, \mu_k^1\}$ to represent all the required parameters at every iteration. Note that if $\mu_k^1 = 0$, the resulting algorithm becomes the Kalman filter under false data injection attacks.

Algorithm 1 Risk sensitive Kalman filter under FDIA

function $[\hat{x}_{k|k},\, P^{xx}_{k|k}] =$ RS-KF-FD$(\hat{x}_{0|0},\, P^{xx}_{0|0},\, \Theta)$.
  for $k = 1, 2, \ldots$ **do**
    $\hat{x}_{k|k-1} = A_{k-1}\hat{x}_{k-1|k-1}$.
    $P^{xx}_{k|k-1} = A_{k-1}\mathcal{P}_{k-1}A_{k-1}^\top + Q_{k-1}$.
    Compute $\hat{y}_{k|k-1}$, $P^{yy}_{k|k-1}$, and $P^{xy}_{k|k-1}$ using (29), (30), and (31).
    $\hat{x}_{k|k} = \hat{x}_{k|k-1} + P^{xy}_{k|k-1}(P^{yy}_{k|k-1})^{-1}(y_k - \hat{y}_{k|k-1})$.
    $P^{xx}_{k|k} = P^{xx}_{k|k-1} - P^{xy}_{k|k-1}(P^{yy}_{k|k-1})^{-1}(P^{xy}_{k|k-1})^\top$.
  end for
end function

IV. Simulation Results

Problem 1: Let us consider a linear system whose stochastic state-space model is given by [22], [29]

$$\begin{aligned} x_k &= \begin{bmatrix} 0 & -0.5 \\ 1 & 1 \end{bmatrix} x_{k-1} + \begin{bmatrix} -6 \\ 1 \end{bmatrix} \eta_{k-1}, \\ z_k &= \begin{bmatrix} -10 & 1 \end{bmatrix} x_k + \nu_k, \end{aligned}$$

where $x_k \in \mathbb{R}^2$ is the state, $z_k \in \mathbb{R}$ is sensor output, process noise $\eta_{k-1} \sim \mathcal{N}(0, 1)$ and measurement noise $\nu_k \sim \mathcal{N}(0, 3.6)$. In this problem, the uncertainty in system modelling is considered as $\Delta A = \mathrm{diag}(0, 0.25)$. The false data attack parameter is selected $a_k \sim \mathcal{N}(0.9, 50)$, and the attack probability is 0.5. The filter is initialized with $x_0 \sim \mathcal{N}(0_{2\times 1},\, P^{xx}_{0|0})$, where $P^{xx}_{0|0} = \mathrm{diag}(1, 5)$. The simulation is performed for 400 time steps.

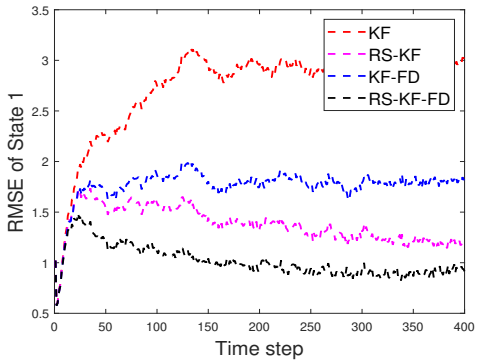
In this problem, we implemented the standard Kalman Filter (KF), the risk-sensitive Kalman Filter (RS-KF), the Kalman Filter under false data (FD) attacks (KF-FD), and the proposed risk-sensitive Kalman Filter under false data attacks (RS-KF-FD) with $\mu_k^1 = 0.005$. We compared the performance of these estimation algorithms using the root-mean-square error (RMSE) obtained from 500 Monte Carlo (MC) runs, as shown in Fig. 2. The results indicate that the proposed RS-KF-FD achieves the lowest RMSE.

V. Conclusion

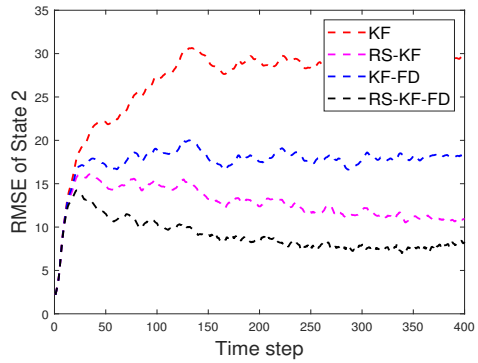
In this article, we developed the risk-sensitive filtering algorithm under the false data injection attacks. The developed algorithm minimized the expectation of the accumulated exponential quadratic estimation error. The efficacy of the proposed algorithm was illustrated in a simulated experiment.

In future, we will extend the proposed method to address multiplicative attacks. This will involve approximating the

Authorized licensed use limited to: AALTO UNIVERSITY. Downloaded on October 11,2024 at 11:33:13 UTC from IEEE Xplore. Restrictions apply.



(a) RMSE of State 1



(b) RMSE of State 2

Fig. 2. The RMSE values obtained from 500 MC runs are computed by different estimators.

false data injected measurement model using conditional expectation, employing the generalized statistics linear regression approach.

APPENDIX

Appendix A: Proof of Lemma 1

Proof: The second-moment of $\big(\xi_k(a_k-\mu)+(\xi_k-\mathrm{p})\mu\big)$ can be computed as

$$\begin{aligned}&\mathbb{E}\big[\big(\xi_k(a_k-\mu)+(\xi_k-\mathrm{p})\mu\big)\big(\xi_k(a_k-\mu)+(\xi_k\\&-\mathrm{p})\mu\big)^\top\big]=\mathbb{E}\big[\xi_k^2(a_k-\mu)(a_k-\mu)^\top\big]+\mathbb{E}\big[\xi_k\\&\times(\xi_k-\mathrm{p})(a_k-\mu)\mu^\top\big]+\mathbb{E}\big[\xi_k(\xi_k-\mathrm{p})\mu\\&\times(a_k-\mu)^\top\big]+\mathbb{E}\big[(\xi_k-\mathrm{p})^2\mu\mu^\top\big].\end{aligned}$$

Using the property of ξ_k and a_k, the above equation becomes (28). ■

Appendix B: Proof of Theorem 1

Proof: The measurement at k-th time step, y_k is independent of the past errors, $e_{1|1},\ldots,e_{k-1|k-1}$. Following (4), we calculate the conditional expectation of the measurement

$$\begin{aligned}\hat{y}_{k|k-1}&=\mathbb{E}[y_k\mid\mathcal{I}_{k-1},e_{k-1|k-1}]\\&=\mathbb{E}[(C_kx_k+\nu_k+\xi_ka_k)\mid y_{1:k-1}]\\&=C_k\hat{x}_{k|k-1}+\mathrm{p}\mu.\end{aligned}$$

Next, we calculate the innovation covariance of the measurement as follows:

$$\begin{aligned}&P^{yy}_{k|k-1}=\mathbb{E}\Big[(y_k-\hat{y}_{k|k-1})(y_k-\hat{y}_{k|k-1})^\top\mid\mathcal{I}_{k-1},e_{k-1|k-1}\Big]\\&=\mathbb{E}\Big[\Big\{C_k(x_k-\hat{x}_{k|k-1})+\nu_k+\xi_k(a_k-\mu)+(\xi_k-\mathrm{p})\mu\Big\}\\&\times\Big\{C_k(x_k-\hat{x}_{k|k-1})+\nu_k+\xi_k(a_k-\mu)+(\xi_k-\mathrm{p})\\&\times\mu\Big\}^\top\mid\mathcal{I}_{k-1},e_{k-1|k-1}\Big].\end{aligned}$$

Using Lemma 1, the above equation becomes (30). The cross-covariance between state and false-data injected measurement can be calculated as

$$\begin{aligned}&P^{xy}_{k|k-1}=E\Big[(x_k-\hat{x}_{k|k-1})(y_k-\hat{y}_{k|k-1})^\top\mid\mathcal{I}_{k-1},e_{k-1|k-1}\Big]\\&=E\Big[(x_k-\hat{x}_{k|k-1})\Big(C_k(x_k-\hat{x}_{k|k-1})+\nu_k+\xi_k(a_k-\mu)\\&+(\xi_k-\mathrm{p})\mu\Big)^\top\mid\mathcal{I}_{k-1},e_{k-1|k-1}\Big]=P^{xx}_{k|k-1}C_k^\top.\end{aligned}$$

■

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] A. Ray, L. Liou, and J. Shen, "State estimation using randomly delayed measurements," *Journal of Dynamic Systems, Measurement, and Control*, vol. 115, pp. 19–26, 1993.

[7] S. Sun, L. Xie, W. Xiao, and Y. C. Soh, "Optimal linear estimation for systems with multiple packet dropouts," *Automatica*, vol. 44, no. 5, pp. 1333–1342, 2008.

[8] J. Hu, Z. Wang, and H. Gao, "Recursive filtering with random parameter matrices, multiple fading measurements and correlated noises," *Automatica*, vol. 49, no. 11, pp. 3440–3448, 2013.

[9] A. Naha, A. M. Teixeira, A. Ahlén, and S. Dey, "Quickest detection of deception attacks on cyber–physical systems with a parsimonious watermarking policy," *Automatica*, vol. 155, p. 111147, 2023.

[10] 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.

[11] 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.

[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] L. Hu, Z. Wang, Q. L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, 2018.

[14] 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.

Authorized licensed use limited to: AALTO UNIVERSITY. Downloaded on October 11,2024 at 11:33:13 UTC from IEEE Xplore. Restrictions apply.

[15] 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.
[16] 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.
[17] S. Padhan and A. K. Turuk, "Design of false data injection attacks in cyber-physical systems," *Information Sciences*, vol. 608, pp. 825–843, 2022.
[18] M. Iqbal, Z. Qu, and A. Gusrialdi, "Resilient dynamic average-consensus of multiagent systems," *IEEE Control Systems Letters*, vol. 6, pp. 3487–3492, 2022.
[19] S. Särkkä and L. Svensson, *Bayesian filtering and smoothing*, 2nd ed. Cambridge University Press, 2023.
[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] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Transaction of the ASME, Journal of the Basic Enginnering*, vol. 82, no. 1, pp. 35–45, 1960.
[22] L. Xie, Y. C. Soh, and C. E. De Souza, "Robust Kalman filtering for uncertain discrete-time systems," *IEEE Transactions on Automatic Control*, vol. 39, no. 6, pp. 1310–1314, 1994.
[23] J. L. Speyer, C. H. Fan, and R. N. Banavar, "Optimal stochastic estimation with exponential cost criteria," in *Proceedings of the 31st IEEE Conference on Decision and Control*. IEEE, 1992, pp. 2293–2299.
[24] J. B. Moore, R. J. Elliott, and S. Dey, "Risk-sensitive generalizations of minimum variance estimation and control," *Journal of Mathematical Systems, Estimation, and Control*, vol. 7, no. 1, pp. 123–126, 1997.
[25] R. N. Banavar and J. L. Speyer, "Properties of risk-sensitive filters/estimators," *IEE Proceedings-Control Theory and Applications*, vol. 145, no. 1, pp. 106–112, 1998.
[26] I. B. Collings, M. R. James, and J. B. Moore, "An information-state approach to risk-sensitive tracking problems," *Journal of Mathematical Systems Estimation and Control*, vol. 6, pp. 343–346, 1996.
[27] R. K. Boel, M. R. James, and I. R. Petersen, "Robustness and risk-sensitive filtering," *IEEE Transactions on Automatic Control*, vol. 47, no. 3, pp. 451–461, 2002.
[28] U. Orguner and M. Demirekler, "Risk-sensitive filtering for jump Markov linear systems," *Automatica*, vol. 44, no. 1, pp. 109–118, 2008.
[29] R. K. Tiwari and S. Bhaumik, "Risk sensitive filtering with randomly delayed measurements," *Automatica*, vol. 142, p. 110409, 2022.

Authorized licensed use limited to: AALTO UNIVERSITY. Downloaded on October 11,2024 at 11:33:13 UTC from IEEE Xplore. Restrictions apply.