Research Article

Design of event-driven control strategy for spoofing attacks in wireless sensor networks

Liu He[1] · Yingjun Zhao[1]

Received: 9 September 2019 / Accepted: 29 April 2020 / Published online: 12 May 2020

Abstract
In this study, an event-driven control strategy is developed to counter the spoofing attacks in wireless sensor networks which is considered as a control strategy in stochastic system. We have also devised the corresponding spoofing-proof event-driven transmission mechanism. For this, first, an event-driven state estimator for the underlying stochastic system is designed. Then, using the stochastic stability theory, the event-triggered state estimator gain is derived by means of the stochastic Laypunov function, so that the corresponding state estimation mean square error is compensated. The estimator's output error is used to suppress the related spoofing attack. The devised event-driven transmission strategy applies some approximate quadratic performance indicators to ensure a measured balance between estimation error, data communication rate and sensor battery life time. Finally, numerical examples are presented to verify the validity of the theoretical results.

Keywords Wireless sensor networks · Spoofing attacks · Stochastic systems · Event-driven control · State estimator

1 Introduction

Wireless sensor network (WSN) comprises a collection of sensor nodes employed to monitor and record the status of the physical environment and organize the gathered data at a central location. The research on wireless sensor networks has made a great progress in recent years, where many solutions have been proposed to address various problems arose these architectures. One of the main concerns of wireless multimedia sensor networks (WMSNs) is the huge data size causing the higher energy consumption in transmission. The high energy consumption is a critical problem for lifetime of network includes sensor nodes with limited battery [1]. In [2], presents a deep learning based distributed data mining (DDM) model to achieve energy efficiency and optimal load balancing at the fusion centre of WSN. Peng et al. [3] consider a linear all-transmission scenario where the intermediate clusters act not only as forwarding clusters but also transmitting clusters. Database applications in wireless sensor networks very often demand data collection from sensor nodes of specific target regions. Design and development of spatial query expressions and energy-efficient query processing strategy are important issues for sensor network database systems [4, 5]. In a wireless sensor network (WSN), the usage of resources is usually highly related to the execution of tasks which consume a certain amount of computing and communication bandwidth [6]. Consumed life time monitoring of a structure during operation is a topic of increasing interest [7, 8]. Localization technology is crucial in wireless sensor networks (WSN) by forming the basis of various WSN applications. With the advancements of WSN, WSN attacks for node localization have increasingly become an important security issue [9]. Location based access in wireless sensor networks (WSN) are vulnerable to location spoofing attacks [10]. However, sensor nodes

✉ Yingjun Zhao, 34162192@qq.com | [1]Air and Missile Defense College, Air Force Engineering University, Xi'an 710051, People's Republic of China.

SN Applied Sciences (2020) 2:1066 | https://doi.org/10.1007/s42452-020-2854-5

are equipped with limited-capacity batteries due to their small form factor requirements. This necessitates frequent battery replenishments, i.e., maintenance tasks to be performed, which becomes impractical for some cases/ deployment areas. As a corollary of this issue, event-driven transmission mechanisms have recently attracted a great deal of attention from both the control and the communication network communities due to reduces the number of transmissions so the overall power consumption of the network, which significantly prolongs the network lifetime [11–13].

Meanwhile, a communication channel is shared between the various physical devices in the network. Due to the high openness of these shared networks, there is no security guarantee for the data transmission between the varied sensors, especially in networks where some data is transmitted in plaintext, and the problem is particularly serious. In this environment, the attackers can easily interfere to the information flow in the network and thereby destroy the control system. In recent years, such behaviors have received significant attention by, whereby considerable contribution has been made by the researchers [14]. It should be noted that the attackers with deceptive behavior are the most dangerous as they often inject the wrong data to destroy the control system. For example, in [15], an algorithm has been proposed to protect the system against such erroneous data transmission behavior, and its main research has been supplemented in [16]. The datasets in [17] are produced to evaluate the ability of intrusion detection systems to detect attacks that emulate normal non-periodical messages, at differing attack occurrence rates. In [18], author develop a spoofing process equation (SPE) that can be used to calculate the tracking point of the delay lock loop (DLL) at regular chip intervals for the entire spoofing process. Paper [19] presents a new approach to estimate the true position of an unmanned aerial vehicle (UAV) in the conditions of spoofing attacks on global positioning system (GPS) receivers. It is proposed the position/velocity-fusion-based integration system in Ref. [20], it can detect both MEAC and LOA attacks with high probability using the IMU error compensations. Paper [21] primarily details the step-by-step implementation of a low-cost GPS spoofing and high-level spoofing data collection apparatus to model a simplistic spoofing attack that could be implemented with limited resources. At the same time, when the system is in a spoofed attack condition, the node tend to generate high-frequency transmitting signals, thereby consuming a large amount of power and reducing the node's life time. To our knowledge, a corresponding security control strategy has not been proposed in the current literature, especially under the event-driven transmission scenarios.

This paper studies the event-driven control strategy to counter spoofing attacks. To devise an event-driven transmission control strategy aiming at detecting the anomalous events caused by spoofing attacks, the state estimator gain triggered by the event is derived by means of a stochastic Laypunov function using stochastic stability theory. Thus, the corresponding state estimation mean square erroris compensated and the corresponding spoofing attack is suppressed using the output error of the estimator. The corresponding event-driven transmission strategy is designed with the aid of approximate secondary performance indicators.

The main contributions of this paper include the following:

1. A new scheme is proposed to detect fraudulent node behavior in wireless sensor networks, including spoofing attacks and processes by estimating and measuring the stochastic system state under attack conditions.
2. Taking advantages of the stochastic mean square stability theory, the corresponding sufficient conditions are derived for the upper bound of the exponential mean square estimation error as $k \to \infty$, using which the stability of the designed estimator is proved. Additionally, the optimal estimator gain to suppress the corresponding spoofing attack is obtained via the linear estimator inequality.
3. An event-driven transmission strategy is proposed using some quadratic approximate system performance indexes. The purpose is to make a measured balance between estimation error, data communication rate and sensor battery life. In order to verify the effectiveness of the estimator-based event-driven attack prevention mechanism, a target tracking application is modeled.

2 Problem statement

In Fig. 1, the state estimation based on the measurement process by a battery-powered sensor is shown. A remote estimator receives measurements over the wireless channel, and it can observe current sensor measurements as well as current estimates. When an event is triggered, the current sensor measurement is sent to the remote estimator. Since there is a correlation between the spoofing attack measurements and the estimation error, the standard Kalman filter will no longer be applicable. Hence, the event-driven estimation mechanism is applied to reduce the data transmission of the sensor nodes, thereby achieving both energies saving and bandwidth reduction.

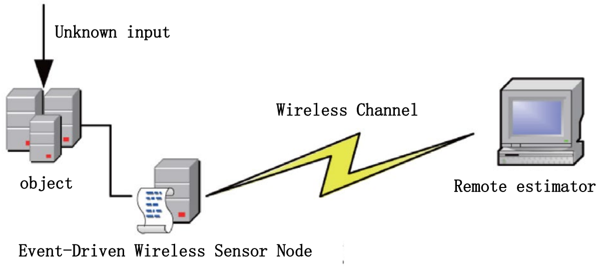

Fig. 1 The event-triggered state estimator driving the plan of sensor

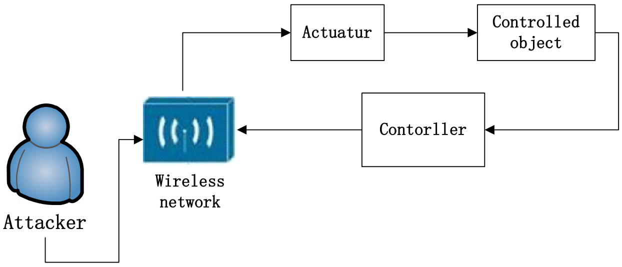

Fig. 2 Transmission scheme with external attacks

Figure 2 shows that the lithium battery powered controller can detect the tracked object and the remote actuator can obtain the control information over the wireless channel.

Symbols: $\mathcal{N}$ and $\mathcal{R}$ are collection of natural and real numbers, respectively. $\mathrm{R}^{m\times n}$ denotes a real value matrix of $m \times n$, and R^n is the abbreviation for $\mathrm{R}^{n\times 1}$. $\mathrm{R}_+^{n\times n}$ and $\mathrm{R}_{++}^{n\times n}$ is the positive semidefinite matrix and positive definite matrix of $n \times n$. When $X \in \mathrm{R}_+^{n\times n}$, we simply write $X \geq 0$ or $X > 0$. For $X \in \mathcal{R}^{m\times n}$, X^{T} denotes the transpose of X, $E[\cdot]$ denotes the mathematical expectation, and $\|\cdot\|$ is the Euclidean norm.

The process dynamics and sensor measurement equations are assumed to be as in the following:

$$\begin{aligned} x_{k+1} &= A_1x_k + u_{c,k} + D_1d_k + w_k \\ y_k &= Cx_k + D_2d_k \end{aligned} \tag{1}$$

In the equation, $x_k \in \mathrm{R}^n$ is the system state, $y_k \in \mathrm{R}^m$ is the system output, $u_{c,k} \in R^n$ is the control input, c is the control entity, $k \to \infty$ is time, and $d_k \in \mathcal{R}^n$ is the spoofing attack input. It is assumed that the random variable $\{w_k\}$ stands for spoofing attack behavior with zero mean and variance of Q_w. When x_k needs to be transmitted to the remote controller, the event-driven algorithm decides whether to send it to the executor. It is assumed that the matrix A_1, D_1, D_2 and C are known. We consider γ_k as a decision variable: when $\gamma_k = 1$, it indicates that $u_{c,k}$ is sent; and when $\gamma_k = 0$, it means $u_{c,k}$ is not sent. Therefore, only when $\gamma_k = 1$, the actuator will know the true value of $u_{c,k}$. Besides, we assume that the spoofing attack size and at the same time, the energy are both bounded: $\|d_k\| \leq \bar{d}$, $\sum_{k=0}^{\infty} d_k^T d_k \leq \rho$.

When the network does not have node protection measures, spoofing attacks may occur. The mathematical model for such attack is considered as follows:

$$u_{a,k} = u_k + \varepsilon_k \tag{2}$$

where u_k is the event-driven controller, ε_k is unknown but bounded signals that satisfy the $\|\varepsilon_k\| \leq \varepsilon$, the $\varepsilon > 0$ is known, and can be estimated by security requirements.

In actual applications, the behavior of an attacker is often unpredictable due to the nonlinearity of the physical device construction, bandwidth constraints and signal quantization, and physical constraints and randomness. The effects of such constructs should be added to the attack model. Doing so, the actual $u_{c,k}$ obtained by the actuator is as follows:

$$u_{c,k} = u_k + \alpha_k \mathit{\Gamma} u_{a,k} \tag{3}$$

where the matrix $\mathit{\Gamma}$ satisfying $\underline{\mathit{\Gamma}} \leq \mathit{\Gamma} \leq \bar{\mathit{\Gamma}}$, where $\underline{\mathit{\Gamma}}$ and $\bar{\mathit{\Gamma}}$ are respectively its upper and lower bounds, which satisfy the following nonlinear relations

$$\begin{cases} \mathit{\Gamma} u_{a,k} = \underline{\mathit{\Gamma}} u_{a,k} + \phi_k \\ \phi_k^T\left(\phi_k - \tilde{\mathit{\Gamma}} u_{a,k}\right) \leq 0 \end{cases} \tag{4}$$

where $\tilde{\mathit{\Gamma}} \triangleq \bar{\mathit{\Gamma}} - \underline{\mathit{\Gamma}} > 0$. In addition, α_k is a random variable obeying the Bernoulli distribution, where its probability satisfies

$$\begin{aligned} &\mathrm{Prob}\{\alpha_k = 1\} = \alpha \\ &\mathrm{Prob}\{\alpha_k = 0\} = \alpha_1 = 1 - \alpha \end{aligned} \tag{5}$$

where α_k has nothing to do with random variable $\{w_k\}, \gamma_k$.

Next, the event-driven controller form [7] is given as follow:

$$u_k = \begin{cases} BKx_kBKx_k & \gamma_k = 1 \\ 0 & \gamma_k = 0 \end{cases} \tag{6}$$

Then the closed-loop system x_k satisfies the following

$$\begin{aligned} x_{k+1} &= A_1x_k + \gamma_k u_{c,k} + D_1d_k + w_k \\ &= A_1x_k + \gamma_k\left(\left(1 - \alpha_k\underline{\mathit{\Gamma}}\right)u_k + \alpha_k\underline{\mathit{\Gamma}}\varepsilon_k + \alpha_k\phi_k\right) + D_1d_k + w_k \\ &= \left(A_1 + \gamma_k\left(1 - \alpha_k\underline{\mathit{\Gamma}}\right)BK\right)x_k + \gamma_k\left(\alpha_k\underline{\mathit{\Gamma}}\varepsilon_k + \alpha_k\phi_k\right) + D_1d_k + w_k \end{aligned} \tag{7}$$

Lemma 1 (Lemma 1 [8]) *Define $V(e_k)$ as a Lyapunov function. If there exist $\varepsilon_1 \geq 0, \varepsilon_2 > 0, \varepsilon_3 > 0$ and $0 < \varepsilon_4 \leq 1$, then*

$$\varepsilon_2 \|e_k\|^2 \leq V(e_k) \leq \varepsilon_3 \|e_k\|^2 \tag{8}$$

and

$$\mathrm{E}\{V(e_{k+1}|e_k)\} - V(e_k) \leq \varepsilon_1 - \varepsilon_4 V(e_k) \tag{9}$$

Then the mean e_k square is bounded. As shown in

$$\mathrm{E}\left\{\|e_k\|^2\right\} \leq \frac{\varepsilon_3}{\varepsilon_2}\|e_0\|^2 (1-\varepsilon_4)^k + \frac{\varepsilon_1}{\varepsilon_2 \varepsilon_4} \sum_{i=1}^{k} (1-\varepsilon_4)^k \tag{10}$$

Next, defining $T \in \mathrm{N}$ as the time domain, and selecting J as a cost function, we get

$$J = \limsup_{T \to \infty} \frac{1}{T} \sum_{k=0}^{T-1} \mathrm{E}(b(e_k)) \tag{11}$$

where the $b(e_k) = e_k^{\mathrm{T}} H e_k + \theta \gamma_k$, the system weight $H > 0$ and the communication weight $\theta > 0$.

The cost given by Formula (11) is called the approximate quadratic performance index [9]. Design in accordance with the secondary form defined by H and through setting the number of $\gamma_k = 1$transmitting times. The main tool used to determine the upper bound is given by the following lemma.

Lemma 2 (Theorem 1 [10]) *Suppose there is a Markov sequence that satisfies the state space X. Suppose that: $f : X \to \mathrm{R}, b : X \to \mathrm{R}$. Definition*:

$$J = \limsup_{T \to \infty} \frac{1}{T} \sum_{k=0}^{T-1} \mathrm{E}(b(x_k)) \tag{12}$$

If there is $c \in \mathrm{R}$ which satisfies

$$m(x) \geq c \quad x \in X, \tag{13}$$

then it can be concluded that

$$J \leq \sup_{\vartheta \in X} \left(b(\vartheta) + \mathrm{E}(m(x_{k+1})|x_k = \vartheta) - m(\vartheta)\right) \tag{14}$$

It can be seen that the corresponding sufficient conditions can make the system to reach a state of bounded exponential mean square error in $k \to \infty$, which proves the stability of the designed estimator. The event-driven mechanism is applied in the remote state estimation to reduce the data transmission of the sensor nodes and to ensure the performance of the remote state estimation simultaneously, thereby achieving the purpose of both energies saving and bandwidth reduction.

3 Design of event-driven controller

Here, the $\gamma_k = 1$controller gain K is derived by Lemma 1 to make the state x_k mean square convergence and suppress the effect of d_k.

Theorem 1 *If $\gamma_k = 1$is given a positive number γ_1, $P > 0$ is assumed to be a symmetric matrix, and the following linear inequality is satisfied*

$$\Omega = \begin{bmatrix} -X & 0 & 0 & X^T C^T D_2 & X^T A_1^T + R^T B^T S^T & -R^T B^T \underline{\Gamma}^T & X^T C^T \\ * & -I & 0 & 0 & \alpha \underline{\Gamma}^T & \underline{\Gamma}^T & 0 \\ * & * & -I & 0 & I & I & 0 \\ * & * & * & -\gamma_1^2 I + D_2^T D_2 & D_1^T & 0 & 0 \\ * & * & * & * & X & 0 & 0 \\ * & * & * & * & * & \alpha_2^{-1} X & 0 \\ * & * & * & * & * & * & -I \end{bmatrix} < 0 \tag{15}$$

then, the mean square of the state x_k is bounded when $d_k = 0$. In addition, when $d_k \neq 0$, under the initial condition of 0, the output satisfies: $\|y_k\| \leq \gamma_1 \|d_k\| + \varepsilon + trace(Q_w P)$.

The Controller Gain $K = RX^{-1}$.

Proof To satisfy the condition (8) of Lemma 1, we select the following Lyapunov function

$$V(x_k) = x_k^T P x_k,$$

where $P > 0$ is a symmetric matrix. When $d_k = 0$, by substituting formula (7) into the above formula

$$
\begin{aligned}
\Delta V_k = \mathrm{E}\left\{ \left(V_{_{k+1}} | x_k, \dots, x_0 \right) \right\} - V_k\left(x_k\right) = {} & x_k^T \left(\left(A_1 + SBK\right)^T P\left(A_1 + SBK\right) - P \right) x_k \\
& + \alpha^2 \varepsilon_k^T \underline{\Gamma}^T P \underline{\Gamma} \varepsilon_k + \alpha^2 \phi_k^T P \phi_k \\
& + 2\alpha x_k^T \left(A_1 + \left(1 - \alpha \underline{\Gamma}\right) BK \right)^T P \underline{\Gamma} \varepsilon_k \\
& + 2\alpha x_k^T \left(A_1 + \left(1 - \alpha \underline{\Gamma}\right) BK \right)^T P \phi_k + \alpha^2 \varepsilon_k^T \underline{\Gamma}^T P \phi_k \\
& + \alpha_2 K^T B^T \underline{\Gamma}^T P \underline{\Gamma} BK + \alpha_2 \varepsilon_k^T \underline{\Gamma}^T P \underline{\Gamma} \varepsilon_k + \alpha_2 \phi_k^T P \phi_k \\
& + 2\alpha_2 K^T B^T \underline{\Gamma}^T P \underline{\Gamma} \varepsilon_k + 2\alpha_2 K^T B^T \underline{\Gamma}^T P \phi_k \\
& + 2\alpha_2 \varepsilon_k^T \underline{\Gamma}^T P \phi_k + trace\left(Q_w P\right) \\
\le {} & x_k^T \left(\left(A_1 + SBK\right)^T P\left(A_1 + SBK\right) - P \right) x_k \\
& + \alpha^2 \varepsilon_k^T \left(\underline{\Gamma}^T P \underline{\Gamma} - I \right) \varepsilon_k + \alpha^2 \phi_k^T (P - I) \phi_k \\
& + 2\alpha x_k^T \left(A_1 + \left(1 - \alpha \underline{\Gamma}\right) BK \right)^T P \phi_k \\
& + \alpha^2 \varepsilon_k^T \underline{\Gamma}^T P \phi_k \\
& + \alpha_2 x_k^T K^T B^T \underline{\Gamma}^T P \underline{\Gamma} BK x_k + \alpha_2 \varepsilon_k^T \underline{\Gamma}^T P \underline{\Gamma} \varepsilon_k \\
& + \alpha_2 \phi_k^T P \phi_k \\
& + 2\alpha_2 x_k^T K^T B^T \underline{\Gamma}^T P \underline{\Gamma} \varepsilon_k + 2\alpha_2 x_k^T K^T B^T \underline{\Gamma}^T P \phi_k \\
& + 2\alpha_2 \varepsilon_k^T \underline{\Gamma}^T P \phi_k \\
& + 2\alpha x_k^T \left(A_1 + \left(1 - \alpha \underline{\Gamma}\right) BK \right)^T P \underline{\Gamma} \varepsilon_k - \phi_k^T \tilde{\Gamma} K x_k \\
& + \phi_k^T \tilde{\Gamma} \varepsilon_k + \varepsilon + trace\left(Q_w P\right) \\
= {} & \eta_k^T \Omega \eta_k + \varepsilon + trace\left(Q_w P\right)
\end{aligned}
\tag{16}
$$

where the $S = 1 - \alpha\underline{\Gamma}$, the $\eta_k = \left[x_k^T \;\; \varepsilon_k^T \;\; \phi_k^T \right]^T$ in order to satisfy the condition of Lemma 9, if $\Omega < 0$, the above formula can be simplified as

$$
\begin{aligned}
\mathrm{E}\left\{ \left(V_{_{k+1}} | x_k, \dots, x_0 \right) \right\} - V_k\left(x_k\right) &= \eta_k^T \Omega \eta_k + \varepsilon + trace\left(Q_w P\right) \\
&\le -\lambda_{\min}(-\Omega) \eta_k^T \eta_k + \varepsilon + trace\left(Q_w P\right) \\
&< -\sigma_{11} x_k^T x_k + \varepsilon + trace\left(Q_w P\right).
\end{aligned}
\tag{17}
$$

where the $0 < \sigma_{11} < \min\left\{ \lambda_{\min}(-\Omega),\ \lambda_{\max}(P) \right\}$, $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$ refer to minimum and maximum eigenvalues of the matrix, respectively.

By using Lemma 1 and Inequality (15), the above formula can be summarized as

$$
\begin{aligned}
\mathrm{E}\left\{ \left\|x_k\right\|^2 \right\} &\le \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)} \left\|x_0\right\|^2 \left(1 - \sigma_{11}\right)^k + \frac{\varepsilon + trace\left(Q_w P\right)}{\lambda_{\min}(P) \sigma_{11}} \sum_{i=1}^{k} \left(1 - \sigma_{11}\right)^k \\
&\le \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)} \left\|x_0\right\|^2 \left(1 - \sigma_{11}\right)^k + \frac{\varepsilon + trace\left(Q_w P\right)}{\lambda_{\min}(P) \sigma_{11}}.
\end{aligned}
\tag{18}
$$

Therefore, it is verified that when $d_k = 0$ and $\gamma_k = 1$, x_k is mean-square bounded.

Next, assuming $d_k \neq 0$ we reformulate ΔV_k as

$$\begin{aligned}\Delta V_k \leq{} & x_k^T\Big(\left(A_1 + SBK\right)^T P\left(A_1 + SBK\right) - P\Big)x_k \\ & + \alpha^2\varepsilon_k^T\left(\underline{\Gamma}^T P\underline{\Gamma} - I\right)\varepsilon_k + \alpha^2\phi_k^T(P - I)\phi_k \\ & + 2\alpha x_k^T\left(A_1 + \left(1 - \alpha\underline{\Gamma}\right)BK\right)^T P\phi_k + \alpha^2\varepsilon_k^T\underline{\Gamma}^T P\phi_k \\ & + \alpha_2 x_k^T K^T B^T \underline{\Gamma}^T P\underline{\Gamma}BKx_k + \alpha_2\varepsilon_k^T\underline{\Gamma}^T P\underline{\Gamma}\varepsilon_k + \alpha_2\phi_k^T P\phi_k \\ & + 2\alpha_2 x_k^T K^T B^T \underline{\Gamma}^T P\underline{\Gamma}\varepsilon_k + 2\alpha_2 x_k^T K^T B^T \underline{\Gamma}^T P\phi_k + 2\alpha_2\varepsilon_k^T\underline{\Gamma}^T P\phi_k \\ & + 2\alpha x_k^T\left(A_1 + \left(1 - \alpha\underline{\Gamma}\right)BK\right)^T P\underline{\Gamma}\varepsilon_k - \phi_k^T\tilde{\Gamma}Kx_k + \phi_k^T\tilde{\Gamma}\varepsilon_k \\ & + d_k^T D_1^T PD_1 d_k + 2x_k^T\left(A_1 + \left(1 - \alpha\underline{\Gamma}\right)BK\right)^T PD_1 d_k + trace\left(Q_w P\right) \\ & + 2\alpha\varepsilon_k^T\underline{\Gamma}^T PD_1 d_k + 2\alpha\phi_k^T PD_1 d_k\end{aligned} \tag{19}$$

Introducing performance index H_∞ to suppress the effect of unknown inputs d_k, we get

$$J_1 = \mathrm{E}\left\{\sum_{k=0}^{\infty} y_k^T y_k\right\} - \gamma_1^2\mathrm{E}\left\{\sum_{k=0}^{\infty} d_k^T d_k\right\} \tag{20}$$

Under the initial conditions of 0, J_1 is substituted in ΔV_k, as

$$J_1 \leq \mathrm{E}\left\{\sum_{k=0}^{\infty}\left(\begin{pmatrix} x_k^T & d_k^T\end{pmatrix}\Omega\begin{pmatrix} x_k \\ d_k\end{pmatrix}\right)\right\} + \varepsilon \tag{21}$$

If $\Omega < 0$, then the following inequality can be obtained

$$\mathrm{E}\left\{\sum_{k=0}^{\infty} y_k^T y_k\right\} - \gamma_1^2\mathrm{E}\left\{\sum_{k=0}^{\infty} d_k^T d_k\right\} \leq \varepsilon \tag{22}$$

Therefore, we can conclude the following

$$\left\|y_k\right\| \leq \gamma_1\left\|d_k\right\| + \varepsilon \tag{23}$$

With Schur complement, we can get the following matrix inequality constraints

$$\Omega = \begin{bmatrix} -P + C^T C & 0 & 0 & C^T D_2 & A_1^T + K^T B^T S^T & -K^T B^T \underline{\Gamma}^T \\ * & -I & 0 & 0 & \alpha\underline{\Gamma}^T & \underline{\Gamma}^T \\ * & * & -I & 0 & I & I \\ * & * & * & -\gamma_1^2 I + D_2^T D_2 & D_1^T & 0 \\ * & * & * & * & P^{-1} & 0 \\ * & * & * & * & * & \alpha_2^{-1}P^{-1}\end{bmatrix} < 0 \tag{24}$$

By multiplying both end sides of $diag\left\{P^{-1}, I\right\}$:

$$\Omega = \begin{bmatrix} -P^{-1} + \left(P^{-1}\right)^T C^T CP^{-1} & 0 & 0 & \left(P^{-1}\right)^T C^T D_2 & A_1^T + \left(P^{-1}\right)^T K^T B^T S^T & -\left(P^{-1}\right)^T K^T B^T \underline{\Gamma}^T \\ * & -I & 0 & 0 & \alpha\underline{\Gamma}^T & \underline{\Gamma}^T \\ * & * & -I & 0 & I & I \\ * & * & * & -\gamma_1^2 I + D_2^T D_2 & 0 & 0 \\ * & * & * & * & P^{-1} & 0 \\ * & * & * & * & * & \alpha_2^{-1}P^{-1}\end{bmatrix} < 0 \tag{25}$$

Again using Schur to complement

$$\Omega = \begin{bmatrix} -X & 0 & 0 & X^T C^T D_2 & X^T A_1^T + R^T B^T S^T & -R^T B^T \underline{\Gamma}^T & X^T C^T \\ * & -I & 0 & 0 & \alpha\underline{\Gamma}^T & \underline{\Gamma}^T & 0 \\ * & * & -I & 0 & I & I & 0 \\ * & * & * & -\gamma_1^2 I + D_2^T D_2 & D_1^T & 0 & 0 \\ * & * & * & * & X & 0 & 0 \\ * & * & * & * & * & \alpha_2^{-1}X & 0 \\ * & * & * & * & * & * & -I\end{bmatrix} < 0 \tag{26}$$

where the $X = P^{-1}$, the $R = KX$.

The proof is completed.

The method described so far uses the linear matrix inequality to obtain the corresponding estimator gain values, thus achieving high accuracy in suppressing the corresponding spoofing attack.

4 Design of event-driven strategy

In this section, we derive the event-driven transmission strategy by using Lemma 2 to prove the upper bound of the approximate quadratic performance.

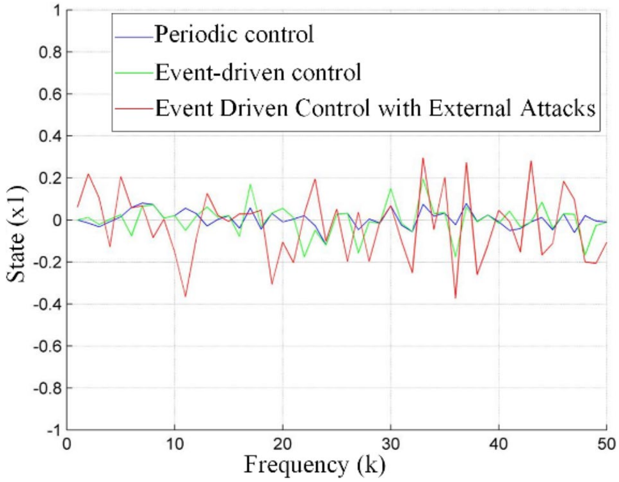

Fig. 3 The evolution of the state × 1

Theorem 2 *Given $H > 0$ as the system weight, $\theta > 0$ as communication weight. Suppose $M > 0$ is a symmetric matrix. If:*

$$\Lambda = \begin{bmatrix} -M+H & 0 & 0 & 0 & A_1^T + K^T B^T S^T M^T & -K^T B^T \underline{\varGamma}^T M^T \\ * & -I & 0 & 0 & \alpha \underline{\varGamma}^T M^T & \underline{\varGamma}^T M^T \\ * & * & -I & 0 & M^T & M^T \\ * & * & * & -\bar{d}^2 I & D_1^T M^T & 0 \\ * & * & * & * & -M & 0 \\ * & * & * & * & * & -\alpha_2^{-1} M \end{bmatrix} < 0 \tag{27}$$

and meet the following event-driven conditions

$$\gamma_k = \begin{cases} 0 \ \ if \ \vartheta^{\mathrm{T}}\left(A_1^T M A_1 - \Psi^{\mathrm{T}} M \Psi\right)\vartheta \le \tilde{\theta} + trace\left(MQ_w\right) \\ 1 \ \ otherwise \end{cases} \tag{28}$$

where the $\Psi = A_1 + SBK$, the $\tilde{\theta} = \varepsilon + \bar{d} + \theta$, then the approximate quadratic performance function satisfies

$$J \le \sup_{\vartheta \in \mathcal{R}^n} g(\vartheta) \le trace\left(MQ_w\right) + \tilde{\theta} \tag{29}$$

Proof Choose a function $m\left(x_k\right) = x_k^T M x_k$. It is easy to see that there is an upper bound, $m\left(x_{k+1}\right)$ can be calculated by (7)

$$x_{k+1} = \begin{cases} A_1 x_k + w_k & \gamma_k = 0, \\ \left(A_1 + SBK\right)x_k - \left(\alpha_k - \alpha\right)\underline{\varGamma} BKx_k & \\ \quad +\alpha \underline{\varGamma} \varepsilon_k + \alpha\phi_k + \left(\alpha_k - \alpha\right)\underline{\varGamma}\varepsilon_k & \\ \quad +\left(\alpha_k - \alpha\right)\phi_k + D_1 d_k + w_k & \gamma_k = 1. \end{cases} \tag{30}$$

Then the following formula can be obtained as

$$\begin{aligned} & \mathrm{E}\left(m\left(x_{k+1}\right) | x_k = \vartheta\right) \\ & = \begin{cases} \vartheta^{\mathrm{T}} A_1^T M A_1 \vartheta + trace\left(MQ_w\right) & \gamma_k = 0, \\ \vartheta_k^T\left(\left(A_1 + SBK\right)^T M\left(A_1 + SBK\right)\right)\vartheta_k & \\ +\alpha^2\varepsilon_k^T \underline{\varGamma}^T P \underline{\varGamma}\varepsilon_k + \alpha^2\phi_k^T P\phi_k + 2\alpha x_k^T\left(A_1 + \left(1 - \alpha\underline{\varGamma}\right)BK\right)^T P\underline{\varGamma}\varepsilon_k & \\ +2\alpha x_k^T\left(A_1 + \left(1 - \alpha\underline{\varGamma}\right)BK\right)^T P\phi_k + \alpha^2\varepsilon_k^T\underline{\varGamma}^T P\phi_k & \\ +\alpha_2 K^T B^T \underline{\varGamma}^T P \underline{\varGamma} BK + \alpha_2\varepsilon_k^T \underline{\varGamma}^T P \underline{\varGamma}\varepsilon_k + \alpha_2\phi_k^T P\phi_k & \\ +2\alpha_2 K^T B^T \underline{\varGamma}^T P \underline{\varGamma}\varepsilon_k + 2\alpha_2 K^T B^T \underline{\varGamma}^T P\phi_k & \\ +2\alpha_2\varepsilon_k^T \underline{\varGamma}^T P\phi_k + trace\left(MQ_w\right) & \\ & \gamma_k = 1. \end{cases} \end{aligned} \tag{31}$$

Define the function g:

$$g(\vartheta) = b(\vartheta) + \mathcal{E}\left(m\left(x_{k+1}\right) | x_k = \vartheta\right) - m(\vartheta) \tag{32}$$

Substituting the above formula, we get:

$$g(\vartheta) = \begin{cases} \vartheta^{\mathrm{T}} A_1^T M A_1 \vartheta + trace\left(MQ_w\right) - \vartheta^{\mathrm{T}} M\vartheta + \vartheta^{\mathrm{T}} H\vartheta & \gamma_k = 0, \\ \vartheta_k^T\left(\left(A_1 + SBK\right)^T M\left(A_1 + SBK\right) - M + H\right)\vartheta_k & \\ \quad +\alpha^2\varepsilon_k^T \underline{\varGamma}^T P \underline{\varGamma}\varepsilon_k + \alpha^2\phi_k^T P\phi_k + 2\alpha x_k^T\left(A_1 + \left(1 - \alpha\underline{\varGamma}\right)BK\right)^T P\underline{\varGamma}\varepsilon_k & \\ \quad +2\alpha x_k^T\left(A_1 + \left(1 - \alpha\underline{\varGamma}\right)BK\right)^T P\phi_k + \alpha^2\varepsilon_k^T\underline{\varGamma}^T P\phi_k & \\ \quad +\alpha_2 K^T B^T \underline{\varGamma}^T P \underline{\varGamma} BK + \alpha_2\varepsilon_k^T \underline{\varGamma}^T P \underline{\varGamma}\varepsilon_k + \alpha_2\phi_k^T P\phi_k & \\ \quad +2\alpha_2 K^T B^T \underline{\varGamma}^T P \underline{\varGamma}\varepsilon_k + 2\alpha_2 K^T B^T \underline{\varGamma}^T P\phi_k & \\ \quad +2\alpha_2\varepsilon_k^T \underline{\varGamma}^T P\phi_k + trace\left(MQ_w\right) + \theta & \\ & \gamma_k = 1. \end{cases} \tag{33}$$

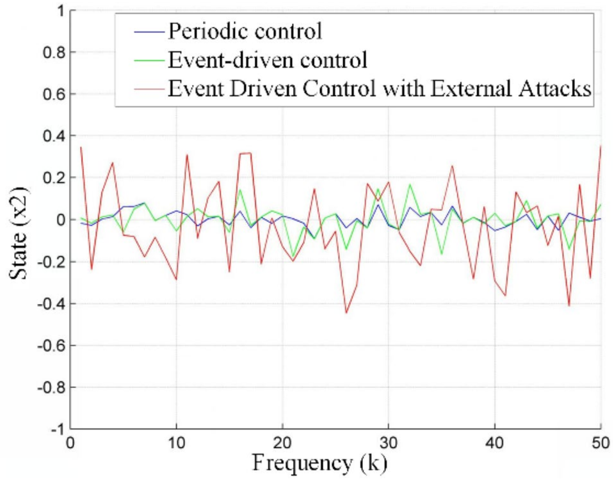

Fig. 4 The evolution of the state ×2

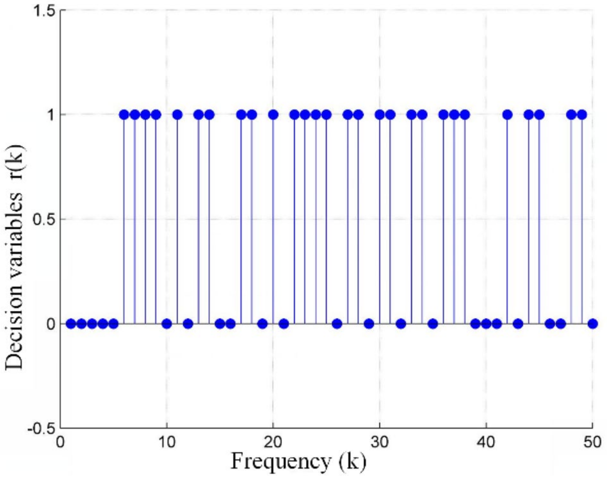

Fig. 5 Event-triggered transmission mode

In order to derive Lemma 2, we need to calculate the upper bound. First, when $\gamma_k = 1$, we get

$$g(\vartheta) \le \tilde{\vartheta}^T \Lambda \tilde{\vartheta} + trace(MQ_w) + \varepsilon + \theta + \bar{d} \tag{34}$$

where the $\tilde{\vartheta}_k = \left[\, \vartheta_k^T \;\; \varepsilon_k^T \;\; \phi_k^T \;\; d_k^T \,\right]^T$. Considering $\Lambda < 0$, we get

$$g(\vartheta) \le trace\left(MQ_w\right) + \varepsilon + \theta + \bar{d} \tag{35}$$

Next, when $\gamma_k = 0$, $g(\vartheta)$ is rewritten as follows

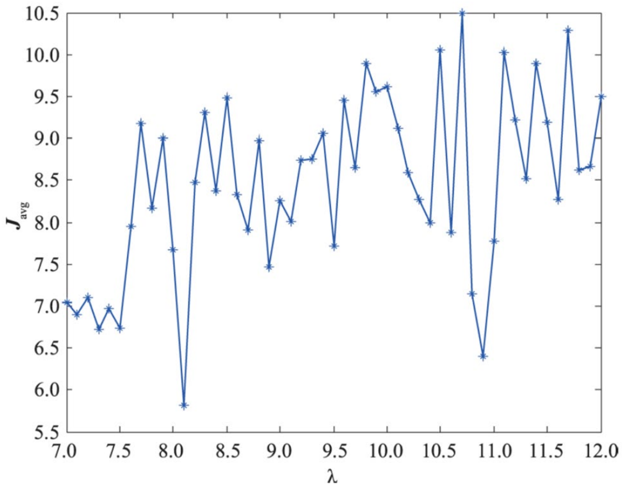

Fig. 6 The limit of the J_{avg}

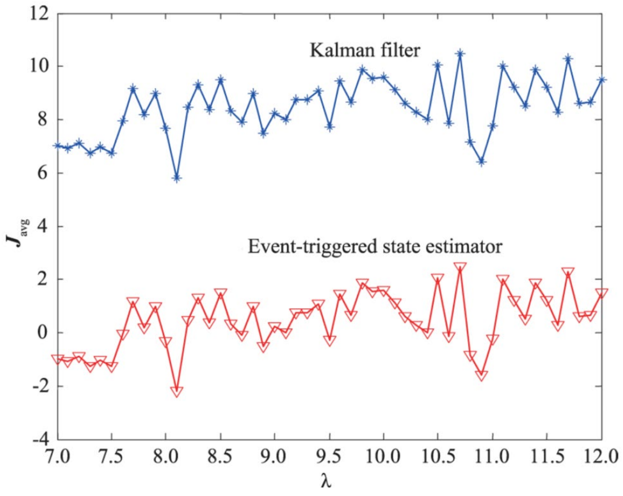

Fig. 7 Compared with the J_{avg} of Kalman filter

$$g(\vartheta) - trace\left(MQ_w\right) = \vartheta^{\mathrm{T}}\left(A_1^T M A_1 - M + H\right)\vartheta \tag{36}$$

Since $\gamma_k = 0$, the event-driven mechanism becomes

$$\vartheta^{\mathrm{T}}\left(A_1^T M A_1 - \Psi^{\mathrm{T}} M \Psi\right)\vartheta \le \theta + trace\left(MQ_w\right) + \varepsilon + \bar{d} \tag{37}$$

where by $\Psi = A_1 + SBK$ we can infer

$$g(\vartheta) - trace\left(MQ_w\right) = \vartheta^{\mathrm{T}}\left(A_1^T M A_1 - M + H\right)\vartheta < \theta + \bar{d} + \varepsilon \tag{38}$$

If the assumption (16) can be established, the following conclusions can be drawn

$$J \le \sup_{\vartheta \in \mathcal{R}^n} g(\vartheta) \le trace\left(MQ_w\right) + \tilde{\theta} \tag{39}$$

where the $\tilde{\theta} = \varepsilon + \bar{d} + \theta$.

The proof is completed. □

This section proposes a corresponding event-driven transmission strategy based on quadratic approximate system performance indicators. The event-driven transmission strategy is obtained by balancing the remote estimation error and the energy consumption of the sensors. This is performed by deriving an upper bound for a class of performance indicators, which provides a good balance between estimation error, data communication rate, and sensor battery life.

5 Simulation

System (1) has the following parametric form:

$$A_1 = \begin{bmatrix} 0 & 1 \\ -2 & -3 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad D_1 = D_2 = \begin{bmatrix} 0.115 \\ 0.12 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This example has been discussed in [11, 12]. In addition, suppose the $\underline{\Gamma} = 0.2$, the $\bar{\Gamma} = 1.2$, the $\bar{d} = \rho = \varepsilon = 0.15$, the $\gamma_1 = 0.7$, the variance $Q_w = \begin{bmatrix} 0.12 & 0 \\ 0 & 0.17 \end{bmatrix}$ for spoofing attack w_k, and spoofing attack $d_k = 0.013e^{-0.5k}$.

Solving the corresponding LMI in Theorems 1 and 2 through the LMI toolbox of MATLAB:

$$P = \begin{bmatrix} 1.0128 & 0 \\ 0 & 2.9180 \end{bmatrix}, \quad K = \begin{bmatrix} 2.0000 & 2.9554 \end{bmatrix}$$

Furthermore, the error weighted value, the transmission weighted value and the event-driven gain are calculated by Theorem 2, where we get

$$H = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}, \quad \theta = 11, \quad M \approx \begin{bmatrix} 0.8761 & 0 \\ 0 & 0.834 \end{bmatrix}.$$

In order to simplify the simulation complexity, the average approximate quadratic performance index is given in this paper:

$$J_{avg} = \frac{1}{T} \sum_{k=0}^{T-1} \left(\left(x_k - \hat{x}_k\right)^T H \left(x_k - \hat{x}_k\right) + \lambda \gamma_k \right)$$

The system simulations are implemented in MATLAB environment. Each scenario is repeated 50 times starting in the initial zero state and performs a periodical control according to the standard procedures. Figures 3 and 4 show the periodic state, event-driven transmission and spoofing attacks. It can be seen from these figures that the difference between the event-driven transmission mechanism under the spoofing attack, and the periodic transmission under the ordinary event-driven strategy is small, that is, the system performance is not greatly affected by the attack.

The corresponding event-driven transmission mode is plotted in Fig. 5, reflecting the actual transmission of data throughout the process. During the entire process, the sensor node sends 28 rounds of data, which is reduced to 22 rounds by the event-driven mechanism. That is to say, the resource usage is reduced by about 35% relative to the periodic transmission mechanism.

Under this performance indicator, by changing the transmission weight value λ, the upper performance limit of the estimator is shown in Fig. 6. Figure 7 shows the results of comparison with the standard Kalman estimator. It can be seen that the performance of the standard Kalman filter is similar to the estimator we designed, which further proves that the transmission strategy of this paper can well balance the estimated performance and communication rate compared to periodic transmission.

6 Conclusion

In this paper, an event-driven state estimator for a stochastic wireless sensor system under spoofing attacks is designed. Since the spoofing attack affects the state at time $k+1$ in the state model, a spoofing attack is defined as a process spoofing attack at time k and a measurement spoofing attack at time $k+1$. First of all, the quadratic Lyapunov function is chosen, and using the results of the stochastic Lyapunov stability theory, the homotopic boundedness of the error dynamics equation is derived. Second, considering the case where the spoofing attack is not zero, and using the classic H_∞ performance indicator, the impact of spoofing attacks is suppressed. Furthermore, the corresponding estimator gain is derived by means of linear matrix inequalities, thereby ensuring the stability of the mean square error when there are no spoofing attacks; while in the case of deceitful attacks, the performance indicators based on the mean square output error are used to resist the impact of spoofing attacks. Subsequently, an event-driven sensor transmission mechanism is derived to determine when to transmit the data by a sensor.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Tekin N, Gungor VC (2020) Analysis of compressive sensing and energy harvesting for wireless multimedia sensor networks. Ad Hoc Netw 103:102164
2. Mohanty SN, Lydia EL, Elhoseny M, Al-Otaibi MMG, Shankar K (2020) Deep learning with LSTM based distributed data mining model for energy efficient wireless sensor networks. Phys Commun 10:101097
3. Peng Y, Li J, Jiang XQ (2020) A hybrid energy efficient cooperative transmission scheme in multihop wireless sensor networks. IEEJ Trans Electr Electron Eng 15(5):771–772
4. Lim CS, Lee J-H, Park M, Hyun SJ (2015) Design and implementation of spatial operators and energy-efficient query processing strategy in wireless sensor network database system. Int J Distrib Sens Netw. https://doi.org/10.1155/2015/50947
5. Kailath T, Sayed AH, Hassibi B (2000) Linear estimation. Prentice-Hall, Englewood Cliffs
6. Wenzhong G, Naixue X, Han-Chieh C, Sajid H, Guolong C (2011) Design and analysis of self-adapted task scheduling strategies in wireless sensor networks. Sensors (Basel, Switzerland) 11(7):6533–6554
7. Heinrich C, Khalil M, Martynov K et al (2019) Online remaining lifetime estimation for structures. Mech Syst Signal Process 119:312–327
8. Ferng H-W, Hadiputro M, Kurniawan A (2011) Design of novel node distribution strategies in corona-based wireless sensor networks. IEEE Trans Mob Comput 10(9):1297–1311
9. Dong S, Zhang X-g, Zhou W-g (2020) A security localization algorithm based on DV-hop against Sybil attack in wireless sensor networks. J Electr Eng Technol 15(3):919–926
10. Gao N, Ni Q, Feng D et al (2020) Physical layer authentication under intelligent spoofing in wireless sensor networks. Signal Process 166:107272
11. Wang D, Mu C (2019) Overview of robust adaptive critic control design. In: Wang D, Mu C (eds) Adaptive critic control with robust stabilization for uncertain nonlinear systems. Springer, Singapore
12. Yuan Y, Zhang P, Wang Z, Chen Y (2019) Noncooperative event-triggered control strategy design with round. IEEE Trans Ind Electron. https://doi.org/10.1109/tie.2019.2903772
13. Cheng L, Tian K, Yao D, Sha L, Beyah RA (2019) Checking is believing: event-aware program anomaly detection in cyber-physical systems. IEEE Trans Depend Secure Comput. https://doi.org/10.1109/tdsc.2019.2906161
14. Ding D, Wang Z, Ho DWC, Wei G (2017) Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. Automatica 78:231–240
15. Hu J, Liu S, Ji D, Li S (2016) On co-design of filter and fault estimator against randomly occurring nonlinearities and randomly occurring deception attacks. Int J Gen Syst 45(5):619–632
16. Wang D, Wang Z, Shen B, Alsaadi FE (2016) Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks. Int J Robust Nonlinear Control 27(7):1194–1208
17. Beomju S, Minhuck P, Sanghoon J, Hyoungmin S, Gapjin K, Changdon K (2019) Spoofing attack results determination in code domain using a spoofing process equation. Sensors (Basel, Switzerland) 19(2):293
18. Rui X, Mengyu D, Ya Q, Shuai Y, Jianye L (2018) Performance analysis of GNSS/INS loosely coupled integration systems under spoofing attacks. Sensors. https://doi.org/10.3390/s18124108
19. Ran Y, David B, Alon S, Yonatan N, Maxim R, Angel P, Yuval E (2019) Datasets of RT spoofing attacks on MIL-STD-1553 communication traffic. Data Brief 23
20. Majidi M, Erfanian A, Khaloozadeh H (2018) A new approach to estimate true position of unmanned aerial vehicles in an INS/GPS integration system in GPS spoofing attack conditions. Int J Autom Comput 15(06):747–760
21. Horton E, Ranganathan P (2018) Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. J Glob Position Syst 16(1):9