Proceedings of the 7th International Conference of Control Systems, and Robotics (CDSR'20)
~~Niagara Falls, Canada~~ Virtual Conference – November, 2020
Paper No. 140
DOI: 10.11159/cdsr20.140

Accelerated Detection Method for Sensor and Actuator Intrusions in Cyber-Physical Systems Using Multiple Model Estimation Algorithm

Jiayi Su, Yuqin Weng, Susan Schneider, Edwin Yaz
Department of Electrical and Computer Engineering, Marquette University
1637 W Wisconsin Ave, Milwaukee, WI 53233, Milwaukee, USA
{jiayi.su, yuqin.weng, susan.schneider, edwin.yaz}@marquette.edu

Abstract – Although Cyber-Physical Systems play a critical role in industrial production and our daily life, the safety of the CPS sensor and actuator signals have not been given due attention. In our previous work, a new approach which successfully detects CPS sensor and actuator intrusion using the multiple model estimation (MME) algorithm with a bank of Kalman filters was described. Since the earlier detection is of importance in such applications, in the present paper, an accelerated detection method using the fading memory technique is applied to the MME resulting in significant faster detection of intrusion signals. To verify the algorithm introduced in this paper, a DC motor speed control system subject to attack by different types of sensor and actuator signals is simulated. Simulations verify that the addition of the fading memory technique allows for the faster detection of sensor and actuator intrusions.

***Keywords*:** Cyber-physical system, intrusion detection, cyber-attack models, adaptive estimation, system security

1. Introduction

Cyber-Physical Systems (CPS), Distributed control systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems are commonly deployed in factories, power grid systems and other infrastructures [1]. Usually, this type of systems is composed of smart sensors, actuators and networked communication devices, and these components can help measuring sensor and actuator signals and then feed it back to the computer-based system to control the physical part of the CPS. For example, the oil and gas industry uses integrated control systems to manage refining operations at plant sites, remotely monitor the pressure and flow of gas pipelines via different types of sensors and control the flow and pathways of gas transmission [2].

Since CPS plays an important role in a variety of critical infrastructures and intelligent distributed control systems, it is facing an increasing risk of receiving different type of cyberattacks, especially attacks targeting its sensors and actuators. Once hacker corrupts sensors, false signals will replace its original healthy signals and produce a fault control signal and cause damages to the physical part of the CPS. If healthy actuator signals are replaced by intrusion signals, CPS will also be damaged. One of the most well-known threat to the CPS is Stuxnet worm. Once finding flaws of a CPS, the Stuxnet worm can be easily implanted into sensors, or actuators of the CPS. Then false signals can be sent into CPS or even the controller can be reprogrammed affects the CPS [3]. Therefore, research on detection and protection against the cyberattacks of CPS has true significance.

Generally, methods for solving the security problem of CPS can be categorized into the following two perspectives: *information security*, which is mainly focused on encryption and data security, and *secure control theory*, which studies how various *cyberattacks* affect control systems' physical dynamics and take measures accordingly [4]. This work is focused on using multiple model estimation algorithm to detect unknown sensor and actuator attacks based on a general attack model, which is a challenging problem because of the uncertainty and erratic nature of cyberattacks [5].

Previous work: A lot of research targeting sensors and actuators intrusion, false date injection, and sensors or actuators failure has been done previously. In [6] the false data injection attacks to state estimation in power grids are studied and the vulnerabilities to such attacks are investigated. In [2] a nonparametric cumulative sum (CUSUM) detection algorithm is implemented to detect integrity attacks on a process control system. In [7] a bank of Kalman filters is implemented to detect current sensors faults for a doubly fed induction generator (DFIG) in wind turbines. In [8] a multiple model adaptive estimation (MMAE) algorithm is applied to detect the sensor and actuator failure in the VISTA F-16 flight control system.

In the current work, the focus will be on detecting intrusions from outside sources and not on internal faults occurring in sensors or actuators

Our previous work [9] contains a new approach to sensor and actuator intrusion detection by using an MME algorithm. State space models of control systems with and without sensor or actuator attacks are used to set up a bank of Kalman filters to estimate the probability of intrusion. It was found out that although the algorithm detects the intrusion successfully, sometimes, *the* speed of detection is not sufficiently high which may result in damage beyond repair. Sometimes the intrusion signals can be detected successfully, but the speed of the detection result is slow and slow detection speed will also cause damages to the CPS. For example, if hacker replaces a healthy DC motor's rotational speed of the shaft signal by an intrusion signal which makes the rotational speed increase a large amount in a very short period of time, then detection of such intrusion signal must be on time, otherwise the load of the motor will still cause significant damage because of the detection time delay. If the intrusion signal can be detected immediately, then the motor can be shut down immediately and the risk of the CPS being damaged can be reduced a lot.

In this work, a sensor and actuator intrusion detection method based on multiple model estimation algorithm is presented for systems that have stochastic disturbances both in the system state and output. Then the accelerated detection method will be presented to decrease the detection time. By modifying the Riccati equations implemented in the Kalman filters, the converge time for state and measurement estimates will be reduced and the detection time delay can also be reduced properly when certain types of the attack signal corrupt the healthy CPS sensor or actuator signal [10].

This work consists of five sections. In section 2, the generalized mathematical model for healthy CPS and CPS under sensor and actuator attacks are presented. Section 3 consists of the implementation of the traditional multiple model estimation *algorithm* for detecting sensor and actuator intrusion signals. In section 4, the fading memory acceleration method used to design the filters in the bank is defined and a comparison is made between the speed of detection of sensor and actuator intrusions using simulation results for a simple DC-motor model, where sensor (rotational speed of the shaft) and actuator (motor voltage source) signal are corrupted by a step-type intrusion signals. Simulation results for other types of intrusion signals have also been generated but could not be included here due to the space limitation. These together with robustness results on under- and over-estimation of intrusion signals will be presented at the conference. Simulation results show that intrusion signals can be detected with time delay when using non-accelerated multiple model estimation algorithm. The simulation results show that the accelerated detection method can detect the intrusion signals earlier comparing to the non-accelerated detection technique. Section 5 generalizes the previous sections and makes conclusion.

2. Problem Formulation

In our previous work, the generalized healthy CPS was modelled as a discrete time stochastic system, using state space representation with additive noise [9]. The generalized intrusion signals are also modelled using the same technique. By modelling the intrusion signal in a state-space form, almost any analytic signals or functions can be exactly or approximately represented for *arbitrary* (unknown) initial values. By augmenting the healthy CPS model with that of the appropriate intrusion signal, the CPS model when it is under arbitrary analytic sensor or actuator intrusions are also formulated. These two CPS models are used to design the Kalman filters for the multiple model estimation (MME) algorithm to detect the unknown intrusion signals. The detection algorithm itself is introduced in Section 3.

2.1. Modelling the Healthy CPS

A CPS *can* be modelled as a linear discrete time stochastic system with additive state and measurement noise

$$x_{k+1} = Ax_k + Bu_k + Fv_k \tag{1}$$

$$y_k = Cx_k + Du_k + Gw_k \tag{2}$$

where $x_k \in \mathbb{R}^n$ is the state vector, $y_k \in \mathbb{R}^p$ is the measurement vector, $u_k \in \mathbb{R}^m$ is the control input, A, B, C, D, F, G are CPS parameter matrices and $v_k \sim \mathcal{N}(0, V)$ represents CPS state noise, $w_k \sim \mathcal{N}(0, W)$ represents CPS measurement noise.

2.2. Modelling the Intrusion Signal

A *generalized* intrusion signal formulated in state-space representation is

$$h_{k+1} = \Phi h_k \tag{3}$$
$$z_k = \Gamma h_k \tag{4}$$

In this state-space representation, $h_k \in \mathbb{R}^n$ is the state vector, $z_k \in \mathbb{R}^p$ is the intrusion signal generated by the state vector h_k, Γ and Φ *are* system matrices. By choosing Φ to be

$$\Phi = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{bmatrix} \tag{5}$$

almost any analytic signals can be exactly or approximately represented as a power series by choosing a proper initial state vector h_k. For example, using $\Phi = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\Gamma = \begin{bmatrix} 1 & 0 \end{bmatrix}$ with initial arbitrary h_0

$$h_{k+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} h_k \tag{6}$$
$$z_k = \begin{bmatrix} 1 & 0 \end{bmatrix} h_k \tag{7}$$

equations (6) and (7) generates a ramp-type or a linear drift intrusion signal.

2.3. Modelling the CPS When Sensor Signal is Under Attack

If the sensor signal in a healthy CPS is under attack, the ‘sensor affected’ CPS model can be represented as

$$\begin{bmatrix} x_{k+1} \\ h_{k+1} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & \Phi \end{bmatrix} \begin{bmatrix} x_k \\ h_k \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} u_k + \begin{bmatrix} F \\ 0 \end{bmatrix} v_k \tag{8}$$
$$y_k = \begin{bmatrix} \Lambda_1 C & \Lambda_2 \Gamma \end{bmatrix} \begin{bmatrix} x_k \\ h_k \end{bmatrix} + Du_k + Gw_k \tag{9}$$

This augmented model combines equations (1) through (4), with weighting factors Λ_1 and Λ_2. In equation (8), x_k represents the healthy states generated by the healthy CPS model, h_k represents the intrusion state vector generated using equation (3). To simplify the notation, let $\mathcal{A} = \begin{bmatrix} A & 0 \\ 0 & \Phi \end{bmatrix}$, $\mathcal{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$, $\mathcal{F} = \begin{bmatrix} F \\ 0 \end{bmatrix}$ and $\mathcal{C} = \begin{bmatrix} \Lambda_1 C & \Lambda_2 \Gamma \end{bmatrix}$. In the augmented $\mathcal{A}$ matrix, Φ is the system matrix from equation (3) used to generate the state vector h_k. In the augmented $\mathcal{C}$ matrix, Γ is the system matrix from equation (4), where Λ_1 and Λ_2 are weighting factors of the sensor signals for the healthy system and the system with sensor intrusions respectively. For example, if the correct healthy sensor signal is completely replaced by an intrusion signal, then $\Lambda_1 = 0$ and $\Lambda_2 = 1$, and equation (9) becomes

$$y_k = \begin{bmatrix} 0 & \Gamma \end{bmatrix} \begin{bmatrix} x_k \\ h_k \end{bmatrix} + Du_k + Gw_k = z_k + Du_k + Gw_k \tag{10}$$

where $z_k = \Gamma h_k$, so the healthy sensor signal is completely replaced by the intrusion signal. The sum of the weighting factors does not have to be one; for example, $\Lambda_1 = \Lambda_2 = 1$, represents the case when the intrusion signal is added to the original sensor signal.

2.4. Modelling the CPS When Actuator Signal is Under Attack

Similarly, if the actuator signal is under attack, then CPS model can be represented as

$$\begin{bmatrix} x_{k+1} \\ h_{k+1} \end{bmatrix} = \begin{bmatrix} A & \Lambda_2 \mathrm{B}\Gamma \\ 0 & \Phi \end{bmatrix} \begin{bmatrix} x_k \\ h_k \end{bmatrix} + \begin{bmatrix} \Lambda_1 B \\ 0 \end{bmatrix} u_k + \begin{bmatrix} F \\ 0 \end{bmatrix} v_k \tag{11}$$

$$y_k = \begin{bmatrix} C & \Lambda_2 D\Gamma \end{bmatrix} \begin{bmatrix} x_k \\ h_k \end{bmatrix} + \Lambda_1 D u_k + G w_k \tag{12}$$

In equation (11) and (12), system matrices can be defined as $\mathcal{A}$ = $\begin{bmatrix} A & \Lambda_2 \mathrm{B}\Gamma \\ 0 & \Phi \end{bmatrix}$, $\mathcal{B} = \begin{bmatrix} \Lambda_1 B \\ 0 \end{bmatrix}$, $\mathcal{F} = \begin{bmatrix} F \\ 0 \end{bmatrix}$, $\mathcal{C} =$ and $\Lambda_1 D = \mathcal{D}$ for convenience. Like the form when CPS measurement signal is under attack, Φ and Γ are system matrices of the intrusion signal where Λ_1 and Λ_2 are weighting factors described previously.

3. Sensor or Actuator Intrusion Detection via Multiple Model Estimation Algorithm

Traditional sensor or actuator failure detection methods assume that sensor or actuator failures leads to a certain parameter of the system becoming unknown, and then transforms the sensor or actuator failures problem into an unknown parameter identification problem [11]. In this case, by implementing the adaptive estimation algorithm via a bank of Kalman filters, the unknown parameter can be estimated adaptively.

However, for the sensor and actuator intrusion problem, when sensors and actuators signal are replaced or modified by intrusion signals, the system dynamics does not change. Therefore, traditional parameter identification method needs to be modified in order to detect the intrusion signal.

In this work, only two Kalman filters are needed in the MME system. One Kalman filter is designed based on the healthy CPS model shown in equation (1) and (2), and another Kalman filter is designed based on the affected CPS model that is under either sensor (equation (8) and (9)) or actuator (equation (11) and (12)) intrusion. The Kalman filter equations are shown as

$$\hat{x}_{k+1} = A\hat{x}_k + Bu_k + K_k(y_k - \hat{y}_k) \tag{13}$$

where A and B are defined before, $\hat{x}_k$ is the estimate of the system state, u_k is the system input, y_k is system measurement signal, $\hat{y}_k = C\hat{x}_k + Du_k$ is system measurement estimate and K_k is Kalman gain. In equation (13), the Kalman gain is defined as

$$K_k = AP_kC^T\,(CP_kC^T + GWG^T)^{-1} \tag{14}$$

where C and G and W are defined before, P_k is the covariance matrix of the state estimates which can be found from Riccati equation

$$P_{k+1} = AP_kA^T + FVF_k^T - AP_kC^T\,(CP_kC^T + GWG^T)^{-1}(CP_kA^T) \tag{15}$$

where F and V are defined before. By setting up the initial value of $\hat{x}_0$ and P_0, the Kalman filter can work recursively to find the CPS state and measurement estimates $\hat{x}_k$ and $\hat{y}_k$ with respect to the given CPS dynamics. In the Kalman filter equations for the CPS under attack, the parameter matrices in (13)-(15) are replaced by their script values defined below equations (8)-(12).

When sensor or actuator intrusion signal is affecting the healthy CPS, the healthy measurement will change from one to another, and both filters can estimate the conditional states with given output signals. Then the conditional probabilities are adaptively calculated based on the given conditional state estimates from the two filters and whose output produces the highest probability represents the current sensor or actuator signal. The block diagram of the detection process is shown in Fig. 1.

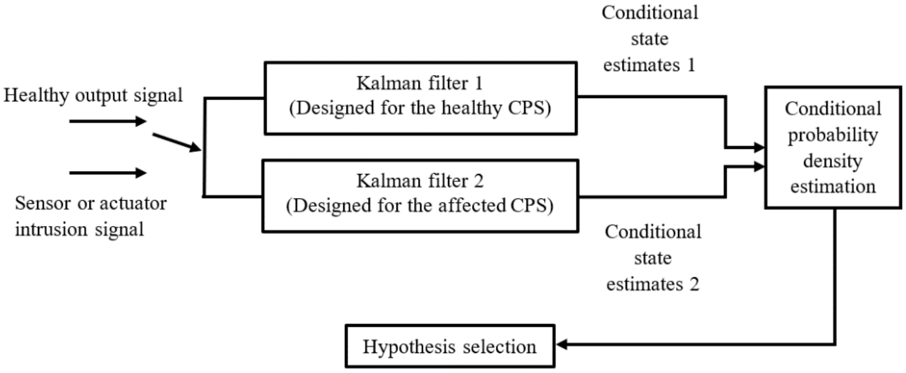
Healthy output signal
Sensor or actuator intrusion signal
Kalman filter 1 (Designed for the healthy CPS)
Kalman filter 2 (Designed for the affected CPS)
Conditional state estimates 1
Conditional state estimates 2
Conditional probability density estimation
Hypothesis selection

Fig. 1: Block diagram of the detection of sensor or actuator intrusions via multiple model estimation algorithm [12]

In Fig. 1, Kalman filter 1 is designed using the model for the healthy CPS using equations (1) and (2). When designing Kalman filter 2, equations (8) and (9) or (11) and (12) for CPS corrupted by either a sensor or actuator intrusion signals respectively are used. These two Kalman filters bank will each compute the state estimates. After that, by using Bayes rule, the conditional probability density for each conditional state estimates are calculated and the one with the highest probability represents whether or not an intrusion is present.

4. Simulation Result

4.1 State-Space Model of the Healthy CPS

In this section, a DC motor model is used as the healthy CPS, and the dynamic equations in state-space form are shown below

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} -\frac{b}{J} & \frac{K}{J} \\ -\frac{K}{L} & -\frac{R}{L} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{L} \end{bmatrix} u \tag{15}$$

$$y = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{16}$$

In this healthy CPS model, the motor voltage source u is the input signal applied to the motor's armature, the output signal is the rotational speed of the shaft x_1. The armature current is represented as x_2. The rotor and shaft are assumed to be rigid and the friction torque is assumed to be proportional to shaft angular velocity [13]. The physical parameters of this CPS model can be found in Appendix. After designing the state feedback controller and discretizing the healthy CPS with sampling time $T = 0.05s$, the healthy CPS model is shown

$$\begin{bmatrix} x_{k+1}^1 \\ x_{k+1}^2 \end{bmatrix} = \begin{bmatrix} 0.6565 & 0.03729 \\ -0.007458 & 0.9048 \end{bmatrix} \begin{bmatrix} x_k^1 \\ x_k^2 \end{bmatrix} + \begin{bmatrix} 0.002059 \\ 0.09516 \end{bmatrix} u_k + \begin{bmatrix} 1 \\ 1 \end{bmatrix} v_k \tag{17}$$

$$y = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_k^1 \\ x_k^2 \end{bmatrix} + w_k \tag{18}$$

where $F_d = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $G_d = 1$, v_k and w_k are zero mean Gaussian distributed noise with covariance $\sigma_v^2 = 0.001$, $\sigma_w^2 = 0.01$. After formulating the healthy CPS, the Kalman filter 1 can be designed accordingly.

4.2 Detection of Unknown Sensor and Actuator Signal

Our previous work showed that the unknown intrusion signal can still be detected even if the assumed attack CPS model does not match the actual CPS model [9]. By assuming $\Phi = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\Gamma = \begin{bmatrix} 0 & 1 \end{bmatrix}$, with $\Lambda_1 = 0.05$ and $\Lambda_2 = 0.95$, attack models targeting sensor, actuator or combined intrusion signal can be formulated, and by designing Kalman filters based on the desired attack CPS model, different type of intrusion signals can be detected properly using multiple model estimation technique. Fig. 2 and Fig. 3 show detection results of the healthy CPS under step-type sensor and actuator intrusion.

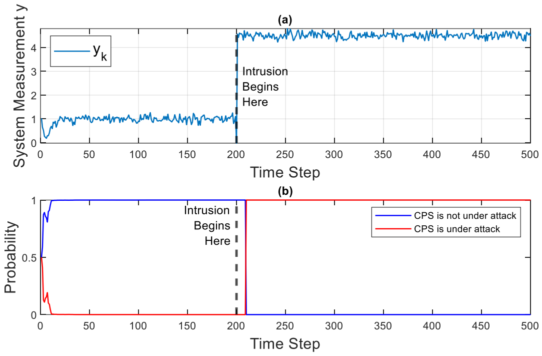

Fig. 2: Detection result of the step-type sensor intrusion

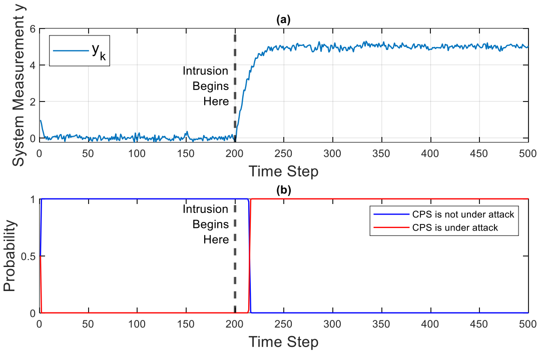

Fig. 3: Detection result of the step-type actuator intrusion

From Fig. 3 (a) and Fig. 4 (a), the step-type intrusion signal replaced the original healthy sensor (rotational speed of the shaft) and actuator (motor voltage source) signal at time step $k = 200$. From Fig. 3 (b) and Fig. 4 (b), by using multiple model estimation algorithm, the sensor intrusion signal is detected at time step $k = 209$ and the actuator intrusion signal is detected at time step $k = 216$.

However, there is a significant detection time delay for both sensor and actuator intrusions. Since the sampling time $T = 0.05s$, the detection time delay for the sensor intrusion is 0.45 seconds, and the time delay for the actuator intrusion signal is 0.8 seconds. Since the measurement signal of the DC-motor is the rotational speed of the shaft, 0.45 seconds detection time delay will still allow the intrusion signal to cause damage because the rotational speed changes for 0.45 seconds will result in the position error increase linearly during this time. If, for example, this DC-motor is used to control the position of a robotic arm in a production line, the position of the arm will continue its original path to cause damage during such short period of time. Similarly, if the actuator (voltage source) intrusion signal is detected 0.8 seconds after it has been injected into the CPS, the false actuator signal will create position error for the robotic arm potentially causing damage. Hence, the sooner the intrusion signals can be detected, the smaller error and the less possibility of damage will be.

4.3 Decrease the Detection Time Delay by Modifying the Riccati Equation

When a CPS is under attack, both Kalman filters in the bank need to respond to the change from the from the healthy measurement, and the new optimal Kalman gains for both filters are computed To this end, the estimation error covariance are updated automatically using the Riccati equation in both filters. This is the reason that the detection time delay occurs when the healthy measurement is replaced by the corrupt one. Thus, the way to decrease detection time delay is to let the optimal Kalman gain to be found earlier after the sudden change of CPSs measurement. If the optimal Kalman gain needs to be found earlier, then the Riccati equation must work faster to minimize the error covariance. One way to do is by adding a fading memory term α into the Riccati equation, which results in the error covariance to be minimized faster. Hence the

Kalman filters converge faster to the corrupted measurement [10]. If both filters can converge faster, then the time delay of the detection can be decreased. This technique involves the
Riccati equation to be modified as

$$P_{k+1} = \alpha^2 A P_k A^T + F V F_k^T - \alpha^2 A P_k C^T \left(C P_k C^T + G W G^T\right)^{-1} \left(C P_k A^T\right) \tag{19}$$

where $\alpha \in \mathbb{R}$ is slightly larger than 1. Of course, in the Kalman filter for the affected model, the parameter matrices will be replaced by the scripted capital letters as discussed before. By using this modified Riccati equation for both Kalman filters in a bank, the detection time delay can be decreased. Fig. 4 and Fig.5 show the detection of the step-type sensor and actuator intrusion signals using the modified Riccati equation when $\alpha = 1.1$.

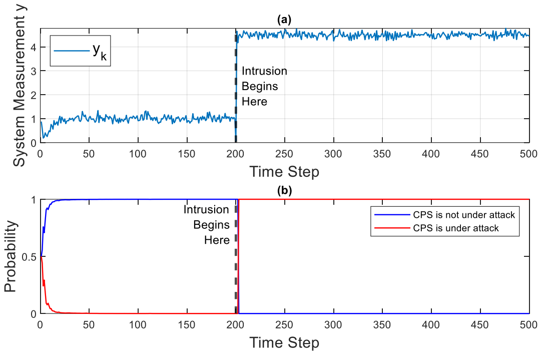

Fig. 4: Detection result of the step-type sensor intrusion using modified Riccati equation

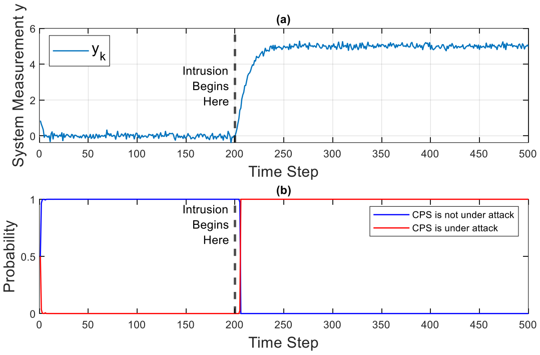

Fig. 5: Detection result of the step-type actuator intrusion using modified Riccati equation

From Fig. 4 (a) and Fig. 5 (a), the step-type intrusion signal replaced the original healthy sensor (rotational speed of the shaft) and actuator (motor voltage source) signal at time step $k = 200$. From Fig. 4 (b) and Fig. 5 (b), by using multiple model estimation algorithm with the modified Riccati equation, the sensor intrusion signal is detected at time step $k = 201$, and the actuator intrusion signal is detected at time step $k = 204$. In this case, for the sensor intrusion detection result, the detection time delay is only 0.05 seconds, and the actuator intrusion detection time delay is only 0.2 seconds. Comparing to Fig. 2 (b) and Fig. 3 (b), the detection time delay for the sensor intrusion signal is decreased by 8 time steps (0.4 seconds), and the detection time for the actuator intrusion signal is decreased for 12 time steps (0.6 seconds). Other methods of acceleration of detection including time-varying fading memory Kalman filters and noise covariance re-setting are being investigated and will be presented at the conference.

5. Conclusions

In this work, a new approach for accelerating detection of the unknown sensor and actuator intrusion signal is presented. The new approach relies on modifying the Riccati equations used to design the Kalman filters used in the MME method. Simulation results for a simple DC motor model shows the detection time is less when detecting sensor and actuator intrusions using the new method compared to the detection times which result when designing the filters using the non-modified Riccati equations. This work can also be expanded easily to decrease the detection time for detecting the CPS where sensor and actuator are both affected by intrusion signals. The conference presentation will include simulation results on robustness of over- and under-estimation (using erroneous intrusion models of respectively higher and lower order than the actual), other acceleration techniques such as time-varying fading memory techniques and noise covariance re-setting, which could not be included due to space limitation.

Appendix: Physical Parameters for the DC Motor [13]

- J: moment of inertia of the rotor, $0.01kg.m^2$
- b: motor viscous friction constant, $0.1N.m.s$
- R: electric resistance, 1 Ohm
- L: electric inductance, $0.5H$
- K_e: electromotive force constant, $0.01V/rad/sec$
- K_t: motor torque constant, $0.01N.m/Amp$
- K: In SI units, $K_t = K_e$; therefore, K is used to represent both the motor torque constant and the electromotive force constant.

References

[1] Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (Vol. 5, No. 1).

[2] Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. (2011, March). Attacks against process control systems: risk assessment, detection, and response. In Proceedings of the 6th ACM symposium on information, computer and communications security (pp. 355-366).

[3] Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), 29.

[4] Cardenas, A. A., Amin, S., & Sastry, S. (2008, June). Secure control: Towards survivable cyber-physical systems. In 2008 The 28th International Conference on Distributed Computing Systems Workshops (pp. 495-500). IEEE.

[5] Kwon, C., Liu, W., & Hwang, I. (2013, June). Security analysis for cyber-physical systems against stealthy deception attacks. In 2013 American control conference (pp. 3344-3349). IEEE.

[6] Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., & Sastry, S. S. (2010, December). Cyber security analysis of state estimators in electric power systems. In 49th IEEE conference on decision and control (CDC) (pp. 5991-5998). IEEE.

[7] Idrissi, I., & Chafouk, H. (2017, December). A bank of Kalman filters for current sensors faults detection and isolation of DFIG for wind turbine. In 2017 International Renewable and Sustainable Energy Conference (IRSEC) (pp. 1-6). IEEE.

[8] Menke, T. E., & Maybeck, P. S. (1995). Sensor/actuator failure detection in the Vista F-16 by multiple model adaptive estimation. IEEE Transactions on aerospace and electronic systems, 31(4), 1218-1229.

[9] Su, J., Weng, Y., Schneider, S. C., & Yaz, E. E, “Sensor and Actuator Intrusion Detection for Cyber-Physical Systems Via Adaptive Estimation Algorithm.” Accepted by DSCC 2020.

[10] Zhai, T., Ruan, H., & Yaz, E. E. (2003, December). Performance evaluation of extended Kalman filter based state estimation for first order nonlinear dynamic systems. In 42nd IEEE International Conference on Decision and Control (IEEE Cat. No. 03CH37475) (Vol. 2, pp. 1386-1391). IEEE.

[11] Sidhu, A., Izadian, A., & Anwar, S. (2014). Adaptive nonlinear model-based fault diagnosis of Li-ion batteries. IEEE Transactions on Industrial Electronics, 62(2), 1002-1011.

[12] Strandt, A. R., Strandt, A. P., Schneider, S. C., & Yaz, E. E. (2018, June). Stator Resistance Estimation Using Adaptive Estimation via a Bank of Kalman Filters. In 2018 Annual American Control Conference (ACC) (pp. 1078-1083). IEEE.

[13] Messner, B., D. T., 2019. Control tutorials for MATLAB and Simulink - motor speed: System modeling.