Observer-based Sensor Fault Detection and Identification with Application to Vehicle Lateral Control

Tesheng Hsiao and Masayoshi Tomizuka
Department of Mechanical Engineering,
University of California at Berkeley, Berkeley, CA94720-1740
tshsiao@uclink.berkeley.edu tomizuka@me.berkeley.edu

Abstract **-- Vehicle lateral control, a vital subsystem of Automated Highway Systems (AHS), acquires lateral position through two sets of on-board magnetometers. Accommodating magnetometer failures is a crucial task for the safety of AHS. Static relations between the two sets of sensors, however, are insufficient for determining the faulty set. In this paper we propose an observer-based method to deal with this problem. The proposed approach can *detect* and *identify* magnetometer failures right after failures took place. Then the output of the faulty sensor is *reconstructed* from the output of the healthy sensor. Therefore the same controller can stabilize the vehicle lateral control system in both normal case and sensor failure case. Simulations demonstrate that the vehicle maintains acceptable performance after either set of magnetometers has failed.**

1. Introduction

The goal of the research on Automatic Highway Systems (AHS) at California PATH (Partners for Advanced Transit and Highways) Program is to reduce congestion and increase safety on highways. In AHS vehicles are driven automatically by on-board sensors, actuators, and computers without human intervention. Longitudinal control allows multiple vehicles to form a platoon with close inter-vehicle distance (1~4m). Lane keeping control is one of the most fundamental operations of AHS; it involves sensing the vehicle's lateral position and calculating the required steering angle to keep the vehicle on the road centerline. The lateral sensing system consists of permanent magnets buried along the road centerline every 1.2 meter and two sets of magnetometers installed under the vehicle's front and rear bumpers. The outputs of the two magnetometer sets are both indispensable for implementing the "look-ahead" lateral controller [3]. Magnetometer failures will result in serious malfunctions of the AHS system. Therefore the lateral control system must have fault tolerant ability such that the system maintains stability and acceptable performance even when one set of magnetometers fails.

Fault tolerant control can be achieved with or without explicit fault detection and identification (FDI) [7][8]. In this paper we focus on fault tolerant control with FDI. By sensor fault *identification* we mean to distinguish the healthy sensor from the faulty one. We are more concerned about the *source* (front or rear magnetometers) of faults than its *types* (bias, disconnection, etc.).

For a system with only two sensors available, it is relatively easy to find out the inconsistency between two sensor measurements, but it is difficult to tell which one is correct. The proposed observer-based FDI in this paper can deal with this problem. After the faulty sensor is detected and identified, its output is replaced and synthesized by that of the healthy sensor; hence the same controller can be applied to both the normal and sensor failure cases.

This paper is organized as follows: section 2 describes the problem setting including models and assumptions. Section 3 illustrates details of the observer-based structure. Technical proofs are left in Appendix. Simulations are given in section 4 and the last section concludes this paper.

2. Problem Setting

2.1 Bicycle Model and Fault Model

The bicycle model is widely used for vehicle lateral control. Under the assumptions of a small steering angle and yaw angle, negligible roll and pitch motion, and linear tire model, the lateral motion can be expressed by a 4th order linear differential equation [4].

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}_1\delta + \mathbf{B}_2 d \tag{1}$$

where $\mathbf{x} = \begin{bmatrix} y & \dot{y} & \varepsilon & \dot{\varepsilon} \end{bmatrix}^T$ $\phi_1 = \dfrac{2C_{\alpha f}}{m}$, $\phi_2 = \dfrac{2C_{\alpha r}}{m}$

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -\dfrac{(\phi_1+\phi_2)}{v_x} & (\phi_1+\phi_2) & \dfrac{-\phi_1 l_1 + \phi_2 l_2}{v_x} \\ 0 & 0 & 0 & 1 \\ 0 & -\dfrac{2(l_1 C_{\alpha f} - l_2 C_{\alpha r})}{I_z v_x} & \dfrac{2(l_1 C_{\alpha f} - l_2 C_{\alpha r})}{I_z} & -\dfrac{2(C_{\alpha f} l_1^2 + C_{\alpha r} l_2^2)}{I_z v_x} \end{bmatrix}$$

$$\mathbf{B}_1 = \begin{bmatrix} 0 & \phi_1 & 0 & \dfrac{2C_{\alpha f} l_1}{I_z} \end{bmatrix}^T$$

$$\mathbf{B}_2 = \begin{bmatrix} 0 & \dfrac{\phi_2 l_2 - \phi_1 l_1 - v_x^{\,2}}{v_x} & 0 & -\dfrac{2(C_{\alpha f} l_1^2 + C_{\alpha r} l_2^2)}{I_z v_x} \end{bmatrix}^T$$

The meaning of each symbol is listed in Table 1.

The output vector of the system consists of measurements from the two sets of magnetometers. Sensor failures are modeled as additive signals to the sensor outputs, i.e.

$$\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \mathbf{C}\mathbf{x} + \mathbf{D}_f f = \begin{bmatrix} \mathbf{C}_1 \\ \mathbf{C}_2 \end{bmatrix} \mathbf{x} + \mathbf{D}_f f \qquad (2)$$

where y_1 and y_2 are the measurements from the front and rear magnetometers, respectively. f is the fault signal which is a function of time t and state $\mathbf{x}$ and

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & d_1 & 0 \\ 1 & 0 & -d_2 & 0 \end{bmatrix}, \quad \mathbf{D}_f = \begin{cases} \begin{bmatrix} 1 & 0 \end{bmatrix}^T & \text{for failure of sensor 1} \\ \begin{bmatrix} 0 & 1 \end{bmatrix}^T & \text{for failure of sensor 2} \end{cases}$$

For example, if the communication link between the front magnetometer and the controller is severed, the corresponding signal to the controller appears to be zero. We model this situation as $y_1 \equiv 0$, i.e. $f = -\mathbf{C}_1\mathbf{x}$. Another example is when the vehicle's on-board sensing module for y_1-which includes the magnetometers, a signal processing unit and a fault detection unit-has detected faults; in this case, y_1 is set to its maximum value(≈ 0.5), i.e. $f = -\mathbf{C}_1\mathbf{x} + 0.5$.

We point out some important features of the bicycle model ([4]) here: (i) $\mathbf{A}$ has two zero eigenvalues, and (ii) $(\mathbf{A},\mathbf{C}_1)$ and $(\mathbf{A},\mathbf{C}_2)$ are observable. (ii) implies that we can estimate the state through either y_1 or y_2. In other words, the two sets of magnetometers provide redundant information which makes FDI feasible.

ε	yaw angle	δ	steering angle
m	spring mass	v_x	longitudinal speed
I_z	yaw moment of inertia		
d	disturbance caused by the road curvature		
y	lateral deviation from CG to the road center line		
l_1/l_2	distance between the front/rear wheel and the CG		
d_1/d_2	distance between the CG and the front/rear bumper		
$C_{\alpha f}/C_{\alpha r}$	Cornering stiffness of the front/real wheels		

Table 1 nomenclature of the bicycle model

2.2 Assumptions and Problems

We make two assumptions about the faults we address in this paper.

(A1) Single failure assumption: at any time at most one sensor fails. This assumption has been implied by the two possible values of $\mathbf{D}_f$. This assumption does not exclude the possibility that both sensors fail intermittently or two sensors fail taking turns.

(A2) Hard fault assumption: All faults happen abruptly; thus we can clearly distinguish the normal operation period from the sensor failure period without ambiguity.

We also assume that there exists a lateral controller that achieves satisfactory performance in normal operation, and we focus on the following FDI problem: *given a system described by (1) and (2) and a stabilizing lateral controller, detect, identify and accommodate sensor failures under (A1) and (A2) such that the lateral control system maintains stability and acceptable performance after the failure of either sensor.*

The essential step in FDI is *residual generation*. Residuals are small when there are no faults and significantly large when faults occur. Residuals must be sensitive to faults while robust to disturbances as well as model uncertainties. Meanwhile, residuals should exhibit unique patterns (called *fault signatures*) for different faults. Faults can then be identified by recognizing these signatures. Due to the limited space, we skip the discussion of robustness issues and concentrate on generating recognizable fault signatures. Hence we assume that the vehicle is on the straight line and the disturbance d in (1) is zero.

Fault detection is relatively easy because the discrepancy between the information contained in both magnetometers indicates the occurrence of faults. Fault identification is difficult if only two sensors are available. How do we distinguish the healthy sensor from the faulty one when their measurements are inconsistent? Insufficient redundancy can be made up by exploiting dynamic relations between sensor outputs, i.e. observers should be involved in FDI.

3. Observer-based FDI

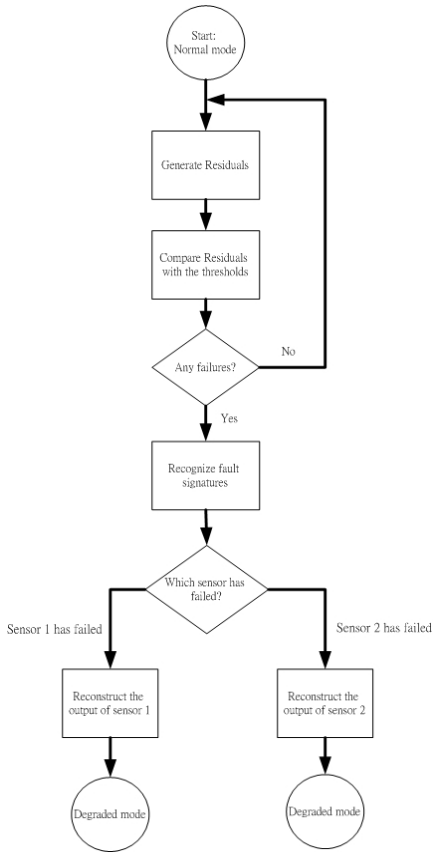
3.1 Overall Structure

Figure 1 is the flowchart of the proposed fault tolerant control system with observer-based FDI. The failure is *detected* first, and then the faulty sensor is *identified*. After that, the output of the faulty sensor is *reconstructed* from the output of the healthy sensor. The lateral control system enters the degraded mode that guarantees stability and an acceptable level of performance.

Figure 2 is the block diagram of the observer-based FDI. The observability properties of the bicycle model imply that we can build two observers, each of which is driven by a single sensor output. In order to avoid the state estimated by either observer totally becoming wrong under sensor failures, we fuse the sensor output and the estimated output from the other observer before they enter the observer. Fusion blocks in Figure 2 play the role of switches, which select the healthy signal. The post-filters are designed such that the transfer functions from fault signals to residuals r_i's have consistent behavior and facilitate fault identification.

The weight adjustment algorithm (WAA) adjusts the weighting factors in the fusion block. The details of each block are described in the following subsections.

Figure 1 Flowchart of the proposed fault tolerant control system



with observer-based FDI

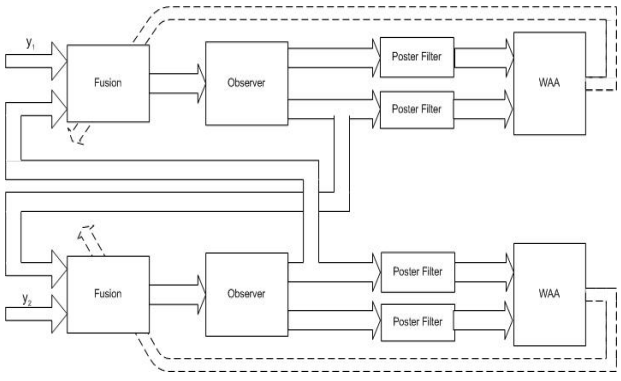


Figure 2 Block diagram of the observer-based FDI

3.2 Output Fusion

Output fusion is a convex combination of the sensor output and the estimated output from the other observer:

$$y_{fi} = (1-\lambda_i)y_i + \lambda_i \hat{y}_i^j \quad \text{i,j,=1,2,} \tag{3}$$

where $\hat{y}_i^j$ is the estimate of the i-th output from the j-th observer. The *weights* $\lambda_i \in [0,1]$ are adjusted on-line. When there is no fault, λ_i=0, i=1,2, the fused output y_{fi} is identical to the sensor output y_i. When faults occur, the corresponding λ_i increases towards 1. λ_i=1 indicates that the sensor output is incorrect and is not taken into account at all.

3.3 Observers

The observers switch between two configurations according to the relative size of weights λ_i:
If $\lambda_1 < \lambda_2$, then

$$\dot{\hat{\mathbf{x}}}_1 = \mathbf{A}\hat{\mathbf{x}}_1 + \mathbf{B}_1\delta + \mathbf{L}_1(y_{f1} - \hat{y}_1^1) + \lambda_1 \mathbf{L}_1\mathbf{C}_1(\hat{\mathbf{x}}_1 - \hat{\mathbf{x}}_2) \tag{4a}$$

$$\dot{\hat{\mathbf{x}}}_2 = \mathbf{A}\hat{\mathbf{x}}_2 + \mathbf{B}_1\delta + \mathbf{L}_2(y_{f2} - \hat{y}_2^2) \tag{4b}$$

else

$$\dot{\hat{\mathbf{x}}}_1 = \mathbf{A}\hat{\mathbf{x}}_1 + \mathbf{B}_1\delta + \mathbf{L}_1(y_{f1} - \hat{y}_1^1) \tag{4c}$$

$$\dot{\hat{\mathbf{x}}}_2 = \mathbf{A}\hat{\mathbf{x}}_2 + \mathbf{B}_1\delta + \mathbf{L}_2(y_{f2} - \hat{y}_2^2) + \lambda_2 \mathbf{L}_2\mathbf{C}_2(\hat{\mathbf{x}}_2 - \hat{\mathbf{x}}_1) \tag{4d}$$

Observers (4a)~(4d) are variations of the Luenberger observer with the fused outputs y_{fi} replacing the sensor outputs y_i. Observability of the bicycle model does not guarantee $\hat{\mathbf{x}}_i$'s converge to $\mathbf{x}$, i=1,2, because two observers are coupled via fusion blocks. A set of conditions for convergence of the estimated state are in Appendix.

3.4 Post-Filters

Let $\mathbf{e}_y^T = [e_{y1}\ e_{y2}\ e_{y3}\ e_{y4}] = [y_1 - \hat{y}_1^1, y_1 - \hat{y}_1^2, y_2 - \hat{y}_2^1, y_2 - \hat{y}_2^2]$ be the output estimation error. Residuals are generated by filtering $\mathbf{e}_y$ through post-filters $M_i(s)$, i.e. $r_i = M_i e_{yi}$, i=1,2,3,4. $M_i(s)$ shapes the transfer functions from the fault signal f to the residuals such that the residuals from the two observers are comparable in magnitude. Note that r_1 and r_2 are related to sensor 1 and r_3 and r_4 are related to sensor 2. Faults are detected according to the following rule:

Detection: If $\max\left(\left\| [r_1 \quad r_2]^T \right\|, \left\| [r_3 \quad r_4]^T \right\| \right) > T$ for some prescribed threshold T, then the fault has occurred. Here $\|\bullet\|$ denotes Euclidean norm at each time instant. Since model uncertainty and sensor noise also contribute to nonzero residuals under the normal operation, the threshold T must be large enough to alleviate false alarms while small enough to avoid missed alarms. In this paper we do not go further to discuss the selection of the threshold.

Fault identification is more elaborate. Notice that observers (4a) ~(4d) are coupled, i.e. failures of either sensor affect all residuals. The effects caused by the failures on the residuals are magnified or attenuated by the observers and post-filters. Therefore $\left\| [r_1 \quad r_2]^T \right\| > \left\| [r_3 \quad r_4]^T \right\|$ does not necessarily conclude the failure of sensor 1. However this problem can be solved by properly-designed post-filters. We explain the post-filter design issues in the remaining part of this subsection.

Let the transfer functions from fault signal f to $\mathbf{e}_y$ be

$$\mathbf{V}(s) = \mathbf{C}_e\left(s\mathbf{I} - \mathbf{A}_e\right)^{-1}\mathbf{B}_e + \mathbf{D}_e \qquad (5)$$

where $\mathbf{A}_e = \begin{cases} \mathbf{A}_{e1} = \begin{bmatrix} \mathbf{A} - (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1 & 0 \\ \lambda_2\mathbf{L}_2\mathbf{C}_2 & \mathbf{A} - \mathbf{L}_2\mathbf{C}_2 \end{bmatrix} & \lambda_1 < \lambda_2 \\ \mathbf{A}_{e2} = \begin{bmatrix} \mathbf{A} - \mathbf{L}_1\mathbf{C}_1 & \lambda_1\mathbf{L}_1\mathbf{C}_1 \\ 0 & \mathbf{A} - (1-\lambda_2)\mathbf{L}_2\mathbf{C}_2 \end{bmatrix} & \text{otherwise} \end{cases}$

$$\mathbf{B}_e = \begin{cases} \begin{bmatrix} -(1-\lambda_1)\mathbf{L}_1 \\ 0 \end{bmatrix} & \text{for failure of sensor 1} \\ \begin{bmatrix} 0 \\ -(1-\lambda_2)\mathbf{L}_2 \end{bmatrix} & \text{for failure of sensor 2} \end{cases}$$

$$\mathbf{C}_e = \begin{bmatrix} \mathbf{C}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_1 \\ \mathbf{C}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2 \end{bmatrix}, \quad \mathbf{D}_e = \begin{cases} [1100]^{\mathrm{T}} & \text{for failure of sensor 1} \\ [0011]^{\mathrm{T}} & \text{for failure of sensor 2} \end{cases},$$

Note that $\mathbf{A}_e$ and $\mathbf{B}_e$ change their values as weights are adapted and as failures take place at different sensors. It is not difficult to check that if $\lambda_1>\lambda_2$ and sensor 1 has failed, then $V_2(s)\equiv 1$ and $V_4(s)\equiv 0$. On the other hand, if $\lambda_1<\lambda_2$ and sensor 2 has failed, then $V_1(s)\equiv 0$ and $V_3(s)\equiv 1$. However, we have to find out which sensor has failed.

If we choose post-filters M_i's such that $a_1M_1V_1 = M_3V_3$ and $a_2M_4V_4 = M_2V_2$ for some real numbers $0<a_1,a_2<1$, we may claim the following identification rules:

Identification: If $\lambda_1<\lambda_2$, and a fault has been detected, $|r_1|>|r_3|$ implies that sensor 1 has failed while $|r_1|<|r_3|$ implies that sensor 2 has failed. Similarly, If $\lambda_1>\lambda_2$ and a fault has been detected, $|r_2|>|r_4|$ implies that sensor 1 has failed while $|r_2|<|r_4|$ implies that sensor 2 has failed. These rules are summarized in Table 2

To verify the identification rules, suppose we have detected any failure but do not know where it comes from. Suppose $\lambda_1<\lambda_2$. Under these circumstances, if sensor 1 has failed, then $|r_1|=|M_1V_1f|>|r_3|=|M_3V_3f|$ because of our choice of M_1 and M_3. If sensor 2 has failed, then $r_1=M_1V_1f\equiv 0$ and $r_3=M_3V_3f=M_3f$ due to the properties of V_1 and V_3. Therefore $|r_1|<|r_3|$. This illustrates the second column of Table 2. Similar arguments can be applied to the first column of Table 2.

$\lambda_1>\lambda_2$	$\lambda_1<\lambda_2$	
$\|r_2\|>\|r_4\|$	$\|r_1\|>\|r_3\|$	sensor 1 has failed
$\|r_2\|<\|r_4\|$	$\|r_1\|<\|r_3\|$	sensor 2 has failed

Table 2 Fault identification rules

Let us take a closer look at the post filter design problem. If sensor 1 has failed and $\lambda_1<\lambda_2$, from (5) we have:

$$V_1(s) = -(1-\lambda_1)\mathbf{C}_1\left(s\mathbf{I} - \mathbf{A} + (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1\right)^{-1}\mathbf{L}_1 + 1 = \frac{n_1(s)}{d(s)}$$

$$V_3(s) = -(1-\lambda_1)\mathbf{C}_2\left(s\mathbf{I} - \mathbf{A} + (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1\right)^{-1}\mathbf{L}_1 = \frac{(1-\lambda_1)n_3(s)}{d(s)}$$

where $(n_1(s),d(s))$ and $(n_3(s),d(s))$ are coprime pairs of polynomials. Since $n_1(s) = \det\begin{bmatrix} s\mathbf{I} - \mathbf{A} + (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1 & \mathbf{L}_1 \\ (1-\lambda_1)\mathbf{C}_1 & 1 \end{bmatrix}$, we have $n_1(s) = \det\left(\begin{bmatrix} s\mathbf{I} - \mathbf{A} & \mathbf{L}_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \mathbf{I} & 0 \\ (1-\lambda_1)\mathbf{C}_1 & 1 \end{bmatrix}\right) = \det(s\mathbf{I} - \mathbf{A})$, which is independent of λ_1 [2]. Similarly, $n_3(s)$ is also independent of λ_1. Now factorize $n_1(s) = n_1^+(s)n_1^-(s)$ and $n_3(s) = n_3^+(s)n_3^-(s)$, where $n_i^+(s)$ and $n_i^-(s)$, i=1,3, have their roots in the closed right half plane and open left plane, respectively. Choose $M_1(s) = \dfrac{n_3^+(s)}{n_1^-(s)k(s)}$ and $M_3(s) = \dfrac{n_1^+(s)}{n_3^-(s)k(s)}$, where $k(s)$ is a Hurwitz polynomial such that $M_1(s)$ and $M_3(s)$ are proper and stable. Then $(1-\lambda_1)M_1(s)V_1(s) = M_3(s)V_3(s)$. Notice that $0<1-\lambda_1<1$ as required.

Similarly, we can choose M_2 and M_4 such that $a_2M_4V_4=M_2V_2$ for some $0<a_2<1$, then the identification rule can be applied.

3.5 Weight Adjustment Algorithm (WAA)

If any fault has been detected and identified, weights λ_i, i=1,2, in fusion blocks will be adjusted on-line. Suppose sensor 1 has failed, then we adjust the weights according the

following 1st order differential equations:

$$\dot{\lambda}_1 = -\alpha(\lambda_1 - g(\left\| \begin{bmatrix} r_1 & r_2 \end{bmatrix}^T \right\|)) \quad (6a)$$

$$\dot{\lambda}_2 = -\alpha\lambda_2 \quad (6b)$$

If sensor 2 has failed, the adaption rule becomes

$$\dot{\lambda}_1 = -\alpha\lambda_1 \quad (6c)$$

$$\dot{\lambda}_2 = -\alpha(\lambda_2 - g(\left\| \begin{bmatrix} r_3 & r_4 \end{bmatrix}^T \right\|)) \quad (6d)$$

where $\alpha>0$ and g: R$\rightarrow$(0,1) is the *logistic function*:

$$g(x) = \frac{1}{1+e^{-ax-b}} \quad a,b>0 \quad (7)$$

The sufficient conditions for convergence of the estimated state are $|\dot{\lambda}_i| < \alpha$ and $\lambda_1+\lambda_2\leq 1$ (see Appendix). $|\dot{\lambda}_i| < \alpha$ may be concluded immediately from (6a)~(6d). We also show that $\lambda_1+\lambda_2\leq 1$ is always satisfied in Appendix. The parameter α is a trade-off between stability and FDI performance. Large α makes FDI respond quickly to faults while small α is required to satisfy the slowly-varying condition (see Appendix) such that stability can be guaranteed.

3.6 Fault Accommodation

In order to accommodate faults, we feed the lateral controller with fused outputs y_{f1} and y_{f2} rather than sensor outputs y_1 and y_2. As we mentioned in subsection 3.2, $y_{fi}=y_i$ when there is no fault. If the fault occurs, the faulty sensor output is replaced by the observer output. The same controller can be applied to both the normal case and the sensor failure cases.

4. Simulation Results

In the following simulations, we set the longitudinal speed to be 10 m/sec ≈ 22 mph. Measurement noise is added to each magnetometer output. The measurement noise is modeled as a zero-mean, Gaussian, white noise with standard deviation 0.0075, i.e. 99% of the noise is within the range (-0.02, 0.02).

Case I: Sensor 1 is disconnected for $t>10$ sec (Figure 3). In normal operation, $y_1\approx y_2\approx 0$ in steady state; hence the effect of the disconnected sensor is nearly unobservable at the beginning. The fault is detected at $t\approx 13$ sec when its effect is accumulated such that the corresponding residual exceeds the threshold. The lateral error remains small (<15cm). Also notice that both observers can estimate states correctly after the fault took place.

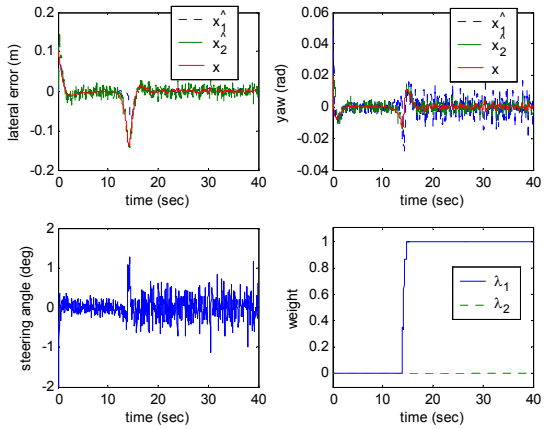


Figure 3 Sensor 1 is disconnect for $t>10$

Case II: Sensor 2 is set to its maximum value (0.5) for $t>10$ sec (Figure 4). The fault is detected immediately and the lateral error remains small. Both observers can estimate state correctly after the fault takes place.

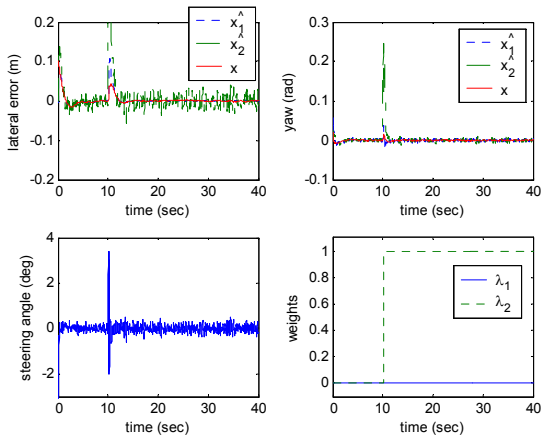


Figure 4 $y_2(t)=0.5$ for $t>10$

5. Conclusion

We proposed an observer-based FDI approach to accommodate magnetometer failures of the vehicle lateral control system. Redundant information is generated through two coupled observers. By employing post-filters and WAA, sensor failures are detected and identified, and good state estimation is achieved. Simulations demonstrate promising results. Experimental verification is currently underway.

6. Appendix

Theorem 1: Let **x** be the state of the bicycle model (1); let $\hat{\mathbf{x}}_1$ and $\hat{\mathbf{x}}_2$ be the estimated states of the observer (4a)~(4d). Then $\lim_{t\to\infty} \hat{\mathbf{x}}_i(t) = \mathbf{x}(t)$, i=1,2 provided that there is no sensor failure and all the following conditions are satisfied.

(a) There exist column vectors $\mathbf{L_1}$ and $\mathbf{L_2}$ such that $\mathbf{A}\text{-}k_1\mathbf{L}_1\mathbf{C}_1$ and $\mathbf{A}\text{-}k_2\mathbf{L}_2\mathbf{C}_2$ are Hurwitz for all $0.5 \le k_1, k_2 \le 1$.

(b) $\lambda_1+\lambda_2, \le 1$

(c) $|\dot{\lambda}_i| < \alpha_i$, i=1,2 for some constants α_i

(d) The frequency of switching between (4a)(4b) and (4c)(4d) is less than some constant γ.

Proof: Let $\mathbf{e}_1 = \mathbf{x} - \hat{\mathbf{x}}_1$ and $\mathbf{e}_2 = \mathbf{x} - \hat{\mathbf{x}}_2$ be the state estimation errors of the two observers. The error dynamics is:

$$\dot{\mathbf{e}} = \mathbf{A}_e\mathbf{e} \qquad (8)$$

where $\mathbf{e}^T = \begin{bmatrix}\mathbf{e}_1^T & \mathbf{e}_2^T\end{bmatrix}$ and $\mathbf{A}_e$ is as defined in (5).

Because λ_i's vary with time and $\mathbf{A}_e$ switches between $\mathbf{A}_{e1}$ and $\mathbf{A}_{e2}$, (8) is a *switched linear time-varying system*. Stable eigenvalues of $\mathbf{A}_e$ for all time do not necessarily guarantee stability [9]. To show stability, we first prove that $\dot{\mathbf{e}} = \mathbf{A}_{ei}\mathbf{e}$ is stable for i=1,2. This is achieved by imposing *slowly-varying conditions*. Then we show that the switching behavior does not hurt the stability if condition (d) holds.

Ilchmann [5] has shown that a linear time-varying system $\dot{\mathbf{e}} = \mathbf{A}_{ei}\mathbf{e}$ is *exponentially stable* if (i) all eigenvalues of $\mathbf{A}_{ei}$ have negative real parts for all time and do not approach to zero as $t\to\infty$; (ii) $\|\mathbf{A}_{ei}\|$ is bounded and (iii) $\|\dot{\mathbf{A}}_{ei}\| < \delta$, where δ>0 is sufficiently small. Condition (b) implies that $\min(\lambda_1,\lambda_2) \le 0.5$ and (b) together with (a) guarantee that $\mathbf{A}_{ei}$ is always Hurwitz for all time. $\|\mathbf{A}_{ei}\|$ is bounded since all its entries are bounded. We can also show that $\|\dot{\mathbf{A}}_{ei}\| \le \sqrt{\left(\dot{\lambda}_1\|\mathbf{L}_1\|_2\|\mathbf{C}_1\|_2\right)^2 + \left(\dot{\lambda}_2\|\mathbf{L}_2\|_2\|\mathbf{C}_2\|_2\right)^2}$.

Therefore (iii) is true if (c) holds for α_1, α_2 small enough. Hence $\dot{\mathbf{e}} = \mathbf{A}_{ei}\mathbf{e}$ is exponentially stable.

The exponential stability of each subsystem $\dot{\mathbf{e}} = \mathbf{A}_{ei}\mathbf{e}$ and condition (d) implies the stability of the switched system (8) [1][6]. Q.E.D.

Remark:

(a) $\lambda_1<\lambda_2$ reflects the fact that y_1 is more trustworthy than y_2. So condition (d) actually says that the two sensors may fail taking turns but they cannot switch too fast. This is a realistic assumption.

(b) When the sensor failure takes place, **e** does not converge to zero. However if the failure has been detected and identified correctly and quickly, WAA will block the influence of the sensor failure on **e** (see $\mathbf{B}_e$ in (5)). Good state estimation is still achievable after the sensor failure provided that the fault detection, identification and weight adjustment are fast enough.

Theorem 2: If λ_1 and λ_2 satisfy (6a)(6b) or (6c)(6d), and initially $\lambda_1(0)=\lambda_2(0)=0$, then $\lambda_1+\lambda_2, \le 1$ for all t≥0.

Proof: Let $s=\lambda_1+\lambda_2-1$ Then

$$\dot{s} = \dot{\lambda}_1 + \dot{\lambda}_2 = -\alpha(\lambda_1+\lambda_2) + \alpha g = -\alpha s + \alpha g - \alpha$$

$$\Rightarrow\ s\dot{s} = -\alpha s^2 + s\alpha(g-1) < 0 \quad \text{for } s>0.$$

Whenever s>0 WAA drives the weights toward s=0. Since $s(0)=\lambda_1(0)+\lambda_2(0)-1<0$, $s(t)<0$ for all t. Q.E.D.

7. References

[1] Branicky, M. S., *Multiple Lyapunov Functions and Other Analysis Tools for Switched and Hybrid Systems*, IEEE Transactions on Automatic Control, Vol. 43, No. 4, 1998, pp475~482

[2] Callier, F. and Desoer, C., *Linear System Theory*, Springer-Verlag, 1991

[3] Guldner, J. Tan, H. and Patwardhan, S., *Study of Design Directions for Lateral Vehicle Control,* Proc. of the Conference of Decision and Control 1997, pp4732~4737

[4] Hingwe, P. S., *Robustness and Performance Issues in the Lateral Control of Vehicles in Automated Highway Systems*, Ph. D. Dissertation, 1997

[5] Ilchmann, A. et al., *Sufficient Conditions for Stability of Linear Time-Varying Systems*, Systems and Control Letters, Vol. 9, 1987, pp157~163

[6] Morse, A. S., *Supervisory Control of Families of Linear Set-Point Controllers – Part 1: Exact matching*, IEEE Transactions on Automatic Control, Vol. 41, No. 10, 1996, pp1413~1431.

[7] Rajamani, R. et al, *A Complete Fault Diagnostic System for Automated Vehicles Operating in a Platoon*, IEEE Transaction on Control Systems Technology, Vol. 9, No. 4, 2000, pp553~564

[8] Suryanarayanan, S., Tomizuka, M. and Suzuki, T, *Fault Tolerant Lateral Control of Automated Vehicles Based on Simultaneous Stabilization,* Proceeding of the 1st IFAC Mechatronics Conference, 2000, pp. 899-904

[9] Vidyasagar, M., *Nonlinear Systems Analysis*, 2nd Ed., Prentice-Hall, 1993.