

A Multirate Adaptive Control for MIMO Systems with Application to Cyber-Physical Security

Hamidreza Jafarnejadsani¹, Hanmin Lee², Naira Hovakimyan³, and Petros Voulgaris⁴

Abstract—This paper proposes a multirate output-feedback controller for multi-input multi-output (MIMO) systems, possibly with non-minimum-phase zeros, using the $\mathcal{L}_1$ adaptive control structure. The analysis of stability and robustness of the sampled-data controller reveals that under certain conditions the performance of a continuous-time reference system is uniformly recovered as the sampling time goes to zero. The controller is designed for detection and mitigation of actuator attacks. By considering a multirate formulation, stealthy zero-dynamics attacks become detectable. The experimental results from the flight test of a small quadrotor are provided. The tests show that the multirate $\mathcal{L}_1$ controller can effectively detect the zero-dynamics actuator attack and recover stability of the quadrotor.

I. INTRODUCTION

Simplex design is recognized as a useful approach for protection of cyber-physical systems (CPSs) against cyber attacks [1], [2]. However, it relies on the system model and accurate measurements, which are not always available in real-world systems. Additionally, since most of the controllers are implemented on digital computers, equipped with sample and hold mechanisms for sending/receiving the physical system's input/output data, vulnerability to stealthy attacks due to the sampling zeros needs to be given serious attention [3]–[5]. This paper investigates the security of feedback systems in the case of stealthy zero-dynamics attacks, which are hard to detect and mitigate from a control theory perspective [5]. If a closed-loop system possesses an unstable zero, an (ultimately) unbounded actuator (or sensor) attack may not be observed by the monitoring data, i.e., the sampled outputs and the control command signals. In this regard, we propose a multirate robust adaptive controller for detection and mitigation of zero-dynamics actuator attacks, while also compensating for other uncertainties and disturbances in the CPSs.

As shown in [5], an interesting property of multirate sampling is its ability to remove certain unstable zeros of the discrete-time system when viewed in the lifted linear time-invariant (LTI) domain. Multirate sampling has been studied

extensively in the context of sampled-data control, and relevant analysis and synthesis results have been reported in [6], [7], to mention only a few. The problem of sampled-data (SD) output-feedback control is addressed by introducing high-gain observers to estimate the unmeasured states [8], [9]. SD output-feedback control of systems with uncertainties and disturbances has been addressed in [10]–[12] for a class of single-input single-output (SISO) nonlinear systems under a lower-triangular linear growth condition.

This paper aims to extend the $\mathcal{L}_1$ adaptive control theory to multirate SD systems, including systems with non-minimum-phase zeros. $\mathcal{L}_1$ adaptive control is known as a robust technique, with quantifiable performance bounds and robustness margins [13]–[15]. The controller compensates for uncertainties and disturbances within the bandwidth of a lowpass filter. In [16], $\mathcal{L}_1$ controllers has been developed for under-actuated MIMO systems with stable transmission zeros. Compared to continuous-time approach, the sampled-data framework of this paper provides a richer and more agile architecture for control of CPSs, which often involve digital computers interacting with physical plants. The preliminary results in [17] on multirate $\mathcal{L}_1$ control design are limited to square MIMO systems without unstable transmission zeros. The current paper extends to non-minimum phase under-actuated systems, where the number of outputs is greater than or equal to the number of inputs. We recognize that a few adaptive control schemes that study SISO non-minimum systems are given in [18]–[20].

In order to verify the effectiveness of the proposed approach, the multirate $\mathcal{L}_1$ adaptive controller is implemented for trajectory tracking control of a quadrotor in an indoor flight arena equipped with VICON cameras. By leveraging the multirate approach, the stealthy zero-dynamics attack becomes detectable. The controller recovers the stability of the quadrotor subject to such attack. The estimation loop in the control structure, which has faster rate than the control input, can timely detect the abnormality in the measured output data and trigger a switch to a safe mode control.

The rest of the paper is organized as follows. Section II presents the mathematical preliminaries and a few definitions. Section III formulates the problem. In Section IV, the structure of the multirate adaptive controller is presented. Section V demonstrates the experimental results. Finally, Section VI concludes the paper.

II. PRELIMINARIES

The notation $\|\cdot\|_p$ represents the vector or matrix p -norms with $1 \leq p \leq \infty$. The variable z denotes the z -transform

¹Hamidreza Jafarnejadsani is with the Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA jafarne2@illinois.edu

²Hanmin Lee is with the Department of Aerospace Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA hlee170@illinois.edu

³Naira Hovakimyan is with the Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA nhovakim@illinois.edu

⁴Petros Voulgaris is with the Department of Aerospace Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA voulgari@illinois.edu

variable, while s is used for the Laplace transform.

Consider a continuous-time LTI plant P_c , and the corresponding discrete time LTI plant $P_d = \mathcal{S}P_c\mathcal{H}$, which is defined with the standard zero-order hold and sample devices $\mathcal{H}$ and $\mathcal{S}$, respectively. The relationship between P_c and P_d follows from the following definition.

Definition 1: Given an LTI system P_c with the minimal realization (A_c, B_c, C_c, D_c) , the equivalent step-invariant discrete-time system P_d is given by the following state-space matrices:

$$A_d = e^{A_c T_s}, B_d = \int_0^{T_s} e^{A_c \tau} B_c d\tau, C_d = C_c, D_d = D_c, \quad (1)$$

where $T_s > 0$ is the sampling period.

Definition 2: (Zero-dynamics attack) Assume the system P_d with the state-space matrices in (1) has unstable transmission zero at $z_0 \in \mathbb{C}$. Then the unbounded actuator attack signal of the form $d[k] = \epsilon z_0^k$, which can be implemented as an additive input disturbance, can remain undetected for small enough ϵ at the sampled output, while causing the states of the system expand exponentially [5].

Definition 3: A MIMO system with the state-space realization (A_m, B_m, C_m) has relative degree $l > 1$, if

$$\begin{aligned} C_m A_m^i B_m &= 0, \quad i \in \{0, \dots, r-2\}, \\ C_m A_m^{l-1} B_m &\neq 0. \end{aligned}$$

III. PROBLEM FORMULATION

Consider the following MIMO system

$$\begin{aligned} \dot{x}(t) &= A_m x(t) + B_m (u(t) + d(t)), \quad x(0) = x_0, \\ y(t) &= C_m x(t), \end{aligned} \quad (2)$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^p$ is the input signal, and $y(t) \in \mathbb{R}^q$ is the system output vector, where $p \leq q$. Also, $\{A_m \in \mathbb{R}^{n \times n}, B_m \in \mathbb{R}^{n \times p}, C_m \in \mathbb{R}^{q \times n}\}$ is an observable-controllable triple, where A_m is Hurwitz, and B_m, C_m are full rank matrices. The unknown initial condition x_0 is assumed to be inside an arbitrarily large known set, so that $\|x_0\|_\infty \leq \rho_0 < \infty$ for some known $\rho_0 > 0$. The transfer function

$$M(s) \triangleq C_m (s\mathbb{I}_n - A_m)^{-1} B_m \quad (3)$$

represents the desired dynamics.

The control input, which is implemented via a zero-order hold mechanism with time period of $T_s > 0$, is given by

$$u(t) = u_d[k], \quad t \in [kT_s, (k+1)T_s), \quad k \in \mathbb{Z}_{\geq 0}, \quad (4)$$

where $u_d[k]$ is the discrete-time control law. The output is sampled N times faster with the sampling period of $\frac{T_s}{N}$. For each period T_s , the N sampled outputs are grouped in a vector form given by

$$\bar{y}_d[k] = \left[y^\top(kT_s), \dots, y^\top\left(\frac{(Nk + N - 1)T_s}{N}\right) \right]^\top. \quad (5)$$

Finally, the system uncertainties, disturbances, and the actuator attack are represented by

$$d(t) = f(kT_s, x(kT_s)), \quad t \in [kT_s, (k+1)T_s), \quad k \in \mathbb{Z}_{\geq 0}, \quad (6)$$

where $f(\cdot, \cdot) : (\mathbb{R}, \mathbb{R}^n) \rightarrow \mathbb{R}^p$ is an unknown function.

Assumption 1: The system $M(s)$ in (3) does not have a transmission zero at the origin.

Assumption 2: For arbitrary $\delta > 0$ there exist $K_\delta > 0$ and $L_0 > 0$, such that

$$\|f(t_2, x_2) - f(t_1, x_1)\|_\infty \leq L_0 |t_2 - t_1| + K_\delta \|x_2 - x_1\|_\infty$$

holds for all $\|x_i\| \leq \delta$, and $t_i \geq 0$, $i \in \{1, 2\}$.

Assumption 3: There exists constant $B_0 > 0$, such that

$$\|f(t, 0)\|_\infty \leq B_0$$

holds uniformly in $t \geq 0$.

Remark 1: In the case of zero-dynamics attack, the boundedness of the attack signal $d(t)$ can be realized by assuming a secure software/hardware structure for the CPS (Simplex architecture [1], [2], [21], [22]). In such structure, a backup controller will operate the system, when the normal mode controller is compromised due to a cyber attack. By switching from the normal mode to a secured backup controller, the unbounded stealthy attack can be removed (from the cyber space), rendering $d(t)$ bounded. However, sensor/actuator attacks, such as zero-dynamics attack, can undermine the effectiveness of model-based detection and control algorithms needed to operate the Simplex architecture. For example, the control design in [2] does not consider the sampled-data structure of CPSs and cannot deal with stealthy zero-dynamics attacks. This motivates to address the detection and control problem for Simplex architecture in the presence of zero-dynamics attacks.

The control objective is to design an output feedback controller $u(t)$ such that the system output $y(t)$ tracks the desired response $y_m(t)$ governed by $y_m(s) = M(s)r(s)$, where $r(s)$ is the Laplace transform of the piece-wise constant signal $r(t)$ given by

$$r(t) = r_d[k], \quad t \in [kT_s, (k+1)T_s), \quad k \in \mathbb{Z}_{\geq 0}, \quad (7)$$

with $r_d[k]$ being the discrete-time signal. Let $\|r\|_{\mathcal{L}_\infty} \leq M_r$, where M_r is a positive constant.

IV. CONTROL DESIGN

First, we define a few variables of interest and design constraints. For design of the controller, we consider a strictly proper stable transfer function $C(s)$ such that $C(0) = \mathbb{I}_p$. Let

$$\begin{aligned} H(s) &\triangleq (s\mathbb{I}_n - A_m)^{-1} B_m, \\ G(s) &\triangleq H(s) (\mathbb{I}_p - C(s)). \end{aligned} \quad (8)$$

The selection of $C(s)$ must ensure that for a given ρ_0 , there exists $\rho_r > 0$ such that the following $\mathcal{L}_1$ -norm condition holds:

$$\|G(s)\|_{\mathcal{L}_1} < \frac{\rho_r - \|H(s)C(s)K_g\|_{\mathcal{L}_1} M_r - \rho_{in}}{L_{\rho_r} \rho_r + B_0}, \quad (9)$$

where

$$\rho_{in} \triangleq \left\| s(s\mathbb{I}_n - A_m)^{-1} \right\|_{\mathcal{L}_1} \rho_0. \quad (10)$$

Further, for every $\delta > 0$, let

$$L_\delta \triangleq \frac{\bar{\gamma}_1 + \delta}{\delta} K_{(\bar{\gamma}_1 + \delta)}, \quad (11)$$

where K_δ is introduced in Assumption 2, and $\bar{\gamma}_1$ is an arbitrarily small positive constant.

To deal with the multirate structure of the controller, where the rate of sampling at the output is N times faster than the rate of hold at the input, we use the standard lifting technique to represent the system matrices. The desired plant $M(s)$ with dual-rate sampling and hold can be described by the discrete-time mapping, given by

$$\bar{M}_d = \mathcal{S}_N M \mathcal{H}.$$

One can obtain a step-invariant LTI description of the discrete-time system $\bar{M}_d$ by grouping the plant outputs as in (5). A state-space description of $\bar{M}_d$ can be obtained as follows:

$$\begin{aligned} \bar{A}_d &= A^N, \quad \bar{B}_d = \sum_{k=0}^{N-1} A^k B, \\ \bar{C}_d &= \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{N-1} \end{bmatrix}, \quad \bar{D}_d = \begin{bmatrix} 0_{q \times p} \\ CB \\ \vdots \\ C \sum_{k=0}^{N-2} A^k B \end{bmatrix}, \end{aligned} \quad (12)$$

where

$$A = e^{A_m \frac{T}{N}}, \quad B = \int_0^{\frac{T}{N}} e^{A_m \tau} B_m d\tau, \quad C = C_m. \quad (13)$$

For brevity the dependence of $\bar{A}_d$, $\bar{B}_d$, $\bar{C}_d$, and $\bar{D}_d$ on the parameter T_s has been dropped. Assuming that the sampling is not pathological [4], the realization (A, B, C) is controllable/observable. For the multirate control design, $N \in \mathbb{N}$ is selected such that

$$Z \triangleq \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{N-2} \end{bmatrix} \quad (14)$$

is full column rank, where matrices A , B , and C are given in (13). This condition holds for large enough N , in particular $N = n + 1$, since the pair (A, C) is observable. It ensures that $\bar{C}_d$ is also full rank.

Remark 2: Using the results obtained in [5], if $\text{rank}(Z) = n$ and Assumption 1 is true, it can be shown that the lifted system $\bar{M}_d$ does not have a non-minimum-phase zero. Therefore, a stealthy zero-dynamics attack is impossible.

Define

$$K(T_s) \triangleq ((\bar{A}_d - \mathbb{I})\bar{C}_d^\dagger \bar{D}_d - \bar{B}_d)^\dagger, \quad (15)$$

where $\dagger$ denotes the left pseudo inverse.

Let (A_f, B_f, C_f) be a minimal state-space realization such that

$$C_f(s\mathbb{I}_{n_c} - A_f)^{-1}B_f \triangleq C(s), \quad (16)$$

where n_c is the order of $C(s)$. Define the function $\Gamma(\cdot)$ as

$$\Gamma(T_s) \triangleq \alpha_1(T) \|(s\mathbb{I}_{n_c} - A_f)^{-1}B_f\|_{\mathcal{L}_1} + \alpha_2(T_s), \quad (17)$$

where

$$\begin{aligned} \alpha_1(T_s) &\triangleq \max_{t \in [0, T_s]} \|C_f(e^{A_f t} - \mathbb{I}_{n_c})\|_\infty, \\ \alpha_2(T_s) &\triangleq \max_{t \in [0, T_s]} \int_0^t \|C_f e^{A_f(t-\tau)} B_f\|_\infty d\tau. \end{aligned}$$

Let

$$\begin{aligned} \Omega(T_s) &= (\|\bar{A}_d \bar{C}_d^\dagger \bar{D}_d - \bar{B}_d\|_\infty + \|\bar{C}_d^\dagger \bar{D}_d\|_\infty) (B_0 + L_{\rho_r} \rho_r) \\ \rho_u(T_s) &= \|C(s)\|_{\mathcal{L}_1} \|K(T_s)\|_\infty \Omega(T_s), \\ \gamma_{dx}(T_s) &= L_{\rho_r} (\|\bar{A}_d - \mathbb{I}_n\|_\infty \rho_r + \|\bar{B}_d\|_\infty (\rho_u(T_s) + B_0 + L_{\rho_r} \rho_r)) \\ &\quad + L_0 T_s, \\ \gamma_0(T_s) &= \left\| \left(\mathbb{I}_p + K(T_s) \bar{C}_d^\dagger \bar{D}_d \right) \right\|_\infty \gamma_{dx}(T_s), \\ \gamma_C(T_s) &= \Gamma(T_s) \|C(s)\|_{\mathcal{L}_1} (B_0 + L_{\rho_r} \rho_r + \gamma_0(T_s)) \\ &\quad + \Gamma(T_s) \|K_g\|_\infty M_r, \\ \rho_{d_0} &= \|sH(s)C(s)\|_{\mathcal{L}_1} (B_0 + L_{\rho_r} \rho_r), \end{aligned} \quad (18)$$

where $K_g \triangleq -C_m A_m^{-1} B_m$, $H(s)$ is defined in (8), and $\Gamma(\cdot)$ is given in (17). Matrices $\bar{A}_d$, $\bar{B}_d$, $\bar{C}_d$, and $\bar{D}_d$ are introduced in (12). Also, $\bar{C}_d^\dagger$ denotes the pseudo-inverse of $\bar{C}_d$. Finally let

$$\gamma_x(T_s) = \frac{\|G(s)\|_{\mathcal{L}_1} \gamma_{dx}(T_s) + \|H(s)\|_{\mathcal{L}_1} \gamma_C(T_s) + \|H(s)C(s)\|_{\mathcal{L}_1} \gamma_0(T_s) + T_s \rho_{d_0}}{1 - L_{\rho_r} \|G(s)\|_{\mathcal{L}_1}}. \quad (19)$$

The sampling time T_s of the digital controller is chosen such that

$$\gamma_x(T_s) < \bar{\gamma}_1, \quad (20)$$

where $\bar{\gamma}_1 > 0$ is introduced in (11), and $\gamma_x(\cdot)$ is given in (19). Also, the sampling time T_s should not be pathological.

Remark 3: Existence of such T_s depends on the uncertainty bounds and the system parameters. For certain class of MIMO systems that additionally satisfy

$$\text{rank} \left(\begin{bmatrix} C_m \\ \vdots \\ C_m A_m^{l-1} \end{bmatrix} \right) = n, \quad (21)$$

where l and n are the relative degree and order of $M(s)$ in (3), respectively, it can be shown that the continuous-time function $\gamma_x(T_s)$ tends to zero as T_s goes to zero. As a result, if the relation (21) is true, the condition in (20) can be met by choosing small enough sampling time T_s .

The elements of the proposed multirate adaptive controller are given in the following.

Output Predictor: The predicted output $\hat{y}_d[k]$ is given by

$$\begin{aligned} \hat{x}_d[k+1] &= \bar{A}_d \hat{x}_d[k] + \bar{B}_d u_d[k] + \hat{d}_d[k], \quad \hat{x}_d[0] = \bar{C}_d^\dagger \bar{y}_0, \\ \hat{y}_d[k] &= \bar{C}_d \hat{x}_d[k] + \bar{D}_d u_d[k], \end{aligned} \quad (22)$$

where

$$\bar{y}_0 = \underbrace{[y_0, \dots, y_0]^\top}_N, \quad y_0 = C_m x_0, \quad (23)$$

and $\hat{d}_d[k] \in \mathbb{R}^n$, $u_d[k] \in \mathbb{R}^p$ are provided by adaptation and control laws, respectively. Also, $\bar{A}_d$, $\bar{B}_d$, $\bar{C}_d$, $\bar{D}_d$ are defined in (12).

Adaptation Law: The update law for $\hat{d}_d[k]$ is given by

$$\hat{d}[k] = -\bar{A}_d \bar{C}_d^\dagger \tilde{y}_d[k], \quad (24)$$

where $\tilde{y}_d[k] = \hat{y}_d - \bar{y}_d[k]$, and $C_d^\dagger$ is the left inverse of $\bar{C}_d$.

Control Law: The control signal is defined as

$$u_d[z] = C_d[z] \left(K_g r_d[z] + K(T_s) \bar{A}_d^{-1} \hat{d}_d[z] \right), \quad (25)$$

where

$$C_d[z] = C_f(z\mathbb{I}_{n_c} - e^{A_f T_s})^{-1} A_f^{-1} (e^{A_f T_s} - \mathbb{I}_{n_c}) B_f,$$

and (A_f, B_f, C_f) is a minimal state-space realization of $C(s)$. Also, $\hat{d}_d[z]$ is the z -transform of the discrete-time signal $\hat{d}_d[k]$ given by (24).

V. EXPERIMENTAL STUDY

We implemented the proposed controller for trajectory tracking of a Crazyflie quadrotor, in x - y plane. Also, the effectiveness of the multirate controller is compared with a standard $\mathcal{L}_1$ adaptive control, which is implemented with uniform sampling time [23]. In this experiment, we consider PID as the baseline control, augmented with $\mathcal{L}_1$ adaptive output-feedback to improve the tracking performance and robustness of the closed-loop system. Then, a zero-dynamics actuator attack is injected into the control input channel. In the following, the flight test results are provided to demonstrate the capability of the proposed multirate adaptive controller in timely detection and mitigation of actuator attacks.

In the multirate trajectory tracking control setup, the pitch and roll command signals are sent to the quadrotor from Simulink with the sampling period of $T_s = 0.03\text{sec}$, and the position measurement signal from Vicon is received with $N = 3$ times faster rate at the sampling period of $\frac{T_s}{N} = 0.01\text{sec}$. For comparison, we also implemented the $\mathcal{L}_1$ controller with uniform rate of $T_s = 0.03\text{sec}$. The rest of the closed-loop system parameters are chosen the same for the singlerate and multirate implementations. The desired dynamics and the low-pass filter are chosen as

$$\begin{aligned} M(s) &= \begin{bmatrix} \frac{4}{s^2+1.5s+4} & 0 \\ 0 & \frac{4}{s^2+1.5s+4} \end{bmatrix}, \\ C(s) &= \begin{bmatrix} \frac{2.5^3}{(s+2.5)^3} & 0 \\ 0 & \frac{2.5^3}{(s+2.5)^3} \end{bmatrix}. \end{aligned} \quad (26)$$

In this experiment, the pitch angle command navigates the quadrotor in x -axis direction, while the roll angle command controls the y -axis position. Therefore, the dynamics governing the position of the quadrotor are decoupled in x and y directions. Using Matlab system identification toolbox, and by collecting input/output data, the following transfer functions for the model of quadrotor dynamics with the baseline PID controller from the reference commands, R_x

and R_y , to the actual x -axis and y -axis positions, X and Y , are obtained

$$\frac{X(s)}{R_x(s)} = \frac{1.276s^2 + 12.33s + 7.058}{s^4 + 3.762s^3 + 8.984s^2 + 14.75s + 7.013}, \quad (27)$$

$$\frac{Y(s)}{R_y(s)} = \frac{-2675s^3 + 4.167s^2 + 3.556s + 13.39}{s^4 + 1.449s^3 + 7.796s^2 + 5.325s + 11.92}. \quad (28)$$

We notice that if the transfer functions in (27) and (28) are sampled at a single rate with sampling time $T_s = 0.03\text{sec}$, the discrete-time plants have unstable zeros at $z_x = -1.06$ and $z_y = 1.66$, respectively. These unstable zeros can be used to devise an attack signal in the form of

$$d[k] = [\epsilon_x z_x^k, \epsilon_y z_y^k]^\top, \quad (29)$$

where $\epsilon_x = 10^{-20}$ and $\epsilon_y = 5 \times 10^{-177}$ are small constants. Also, $z_x = -1.06$ and $z_y = 1.66$ are the unstable sampling zeros for the discrete-time model of quadrotor dynamics in (27) and (28), respectively. Using the multirate control approach of this paper, these unstable zeros can be removed.

Since a cyber attack, such as the zero-dynamics attack in (29), can involve unbounded signals (implemented in cyber space), the feedback control algorithm by itself cannot mitigate the attack. Therefore, the controller should be integrated with a secure software/hardware architecture such as Simplex structure [1], [2], [21], [22]. This structure includes normal control environment and a backup secure control environment. After a cyber attack is detected, the control is switched from normal mode to the safe mode. An ideal control algorithm for Simplex architecture should detect the attack fast enough, and maintain the stability of the perturbed system. This Simplex structure can be achieved using modern multicore processors and virtualization technology [24], which is out of scope of this paper. A simple way to simulate the Simplex structure for this experiment is to remove the attack signal as soon as it is detected.

In the following, we consider a residual for attack detection that triggers switching to a safe mode, which is calculated using the output prediction error. The one-time switch is triggered once the criteria

$$\left\| \begin{bmatrix} w \tilde{y}_d^\top[k+1], & \tilde{y}_d^\top[k+1] - \tilde{y}_d^\top[k] \end{bmatrix} \right\|_\infty > \Delta, \quad k \in \mathbb{N}, \quad (30)$$

is met, where the output prediction error $\tilde{y}_d[k]$ is defined in (24), Δ is the detection threshold, and $w \in \mathbb{R}$ is a weighting coefficient. The residual is a weighted norm of the output prediction error and its rate of change as defined in (30). In the multirate approach, $\Delta = 0.03$ is chosen, while the threshold is $\Delta = 0.02$ for the singlerate control. Also, the weighting coefficient is selected to be $w = 0$ in (30). Figure 1 shows the residuals over time calculated for multirate and singlerate controllers. As shown in Figure 1, the thresholds are chosen above the level of errors due to measurement noise or system uncertainties in order to reduce the number of false alarms. For the same attack signals, the multirate detection happens 0.45sec sooner than the singlerate detection (Figure 1), which is sufficient enough to save the

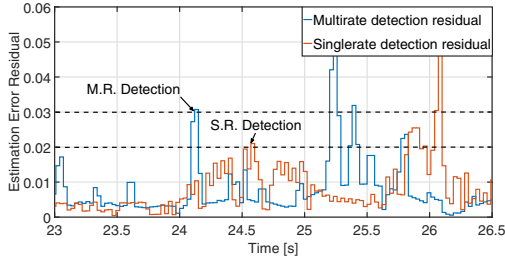


Fig. 1: Calculated residual given by (30) for attack detection. Residual history is shown over the active attack interval. For each flight test, the attack signals are removed as soon as the residual exceeds the threshold ($\Delta_{multirate} = 0.03$, $\Delta_{singlerate} = 0.02$). The multirate $\mathcal{L}_1$ controller provides a 0.45sec faster detection compared to the controller with uniform rate.

quadrotor from crash. Fast detection is particularly important to recover the stability in the case of exponentially growing attack signals. In addition, Figures 2a and 2b show the norm of the output prediction error $\|\tilde{y}_d[k]\|_\infty$ for multirate and singlerate $\mathcal{L}_1$ controllers, respectively. In Figure 2a for multirate approach, we can notice a change in the profile of prediction error norm, when the attack signal starts to grow to significant levels (after $t = 21.5\text{sec}$). However, a change in the prediction error norm can be detected from $t = 23.5\text{sec}$ in Figure 2b for singlerate method. This indicates that the singlerate detection has a considerable latency compared to multirate detection in the case of zero-dynamics attacks. In addition, comparison of Figures 2a and 2b reveals that the output prediction error norm is smaller under multirate controller, which indicates a better performance for tracking the $\mathcal{L}_1$ reference system.

The rest of the flight test results are illustrated in Figure 3. Figure 3a shows the zero-dynamics attack signals for pitch and roll commands, which become noticeable at around $t = 21.5\text{sec}$, and grow exponentially till $t = 24.12\text{sec}$, when attack is detected as the residual exceeds the threshold (Figure 1). After being detected, the attack signals can be removed by switching to a secure computing platform, which performs as a backup for the compromised controller software. Figure 3b shows the trajectory of the quadrotor in x - y plane under augmented single-rate and multirate $\mathcal{L}_1$ adaptive controllers, in two separate flight tests. We can see that the closed-loop system with single-rate controller crashes due to zero-dynamics attack, however the system with multirate controller is robust to the attack. The x and y trajectories of the quadrotor versus time are shown in Figures 3c and 3d, respectively.

Remark 4: The results of this experiment and choice of the threshold in (30) depend on the quality of the measurement outputs and the level of noise in the motion capture system. In the flight tests similar to above, false alarm cases can occur due to the inaccuracy in the measurements.

VI. CONCLUSION

A multirate adaptive output-feedback control approach is proposed for MIMO systems. Leveraging the fact that by

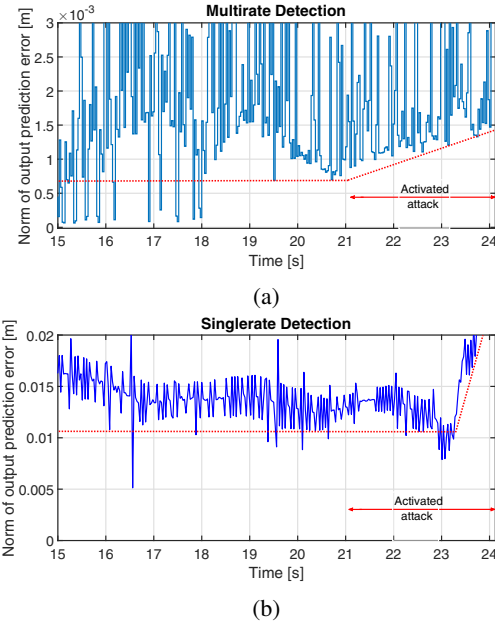


Fig. 2: Norm of the output prediction error $\|\tilde{y}_d[k]\|_\infty$ for multirate $\mathcal{L}_1$ controller in (a), and for singlerate $\mathcal{L}_1$ controller in (b). The active attack interval is marked in the plots. A change in the profile of prediction error norm can be observed in Figure 2a during the active attack interval, while the profile change in Figure 2b becomes noticeable with about 2sec delay.

multirate sampling the possible non-minimum-phase zeros of a system can be removed, the approach of this paper can be applied to systems with unstable zeros. A sufficient condition on the sampling time of the digital controller is obtained that ensures stability of the closed-loop system. Under the specified conditions in the paper, the closed-loop multirate system can uniformly recover the performance of a continuous-time reference system as the sampling time goes to zero. Results from an indoor quadrotor flight test are provided to demonstrate that the fast estimation loop in the multirate $\mathcal{L}_1$ control structure can detect zero-dynamics attacks, and maintain the stability of the quadrotor flight subject to disturbances, attacks, and system uncertainties.

VII. ACKNOWLEDGMENTS

This work has been supported in part by NSF (award numbers CMMI-1663460 and ECCS-1739732).

REFERENCES

- [1] L. Sha, "Using simplicity to control complexity," *IEEE Software*, vol. 18, no. 4, pp. 20–28, Jul 2001.
- [2] X. Wang, N. Hovakimyan, and L. Sha, "L1simplex: fault-tolerant control of cyber-physical systems," in *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems*. ACM, 2013, pp. 41–50.
- [3] K. J. Åström, P. Hagander, and J. Sternby, "Zeros of sampled systems," *Automatica*, vol. 20, no. 1, pp. 31–38, 1984.
- [4] T. Chen and B. Francis, *Optimal sampled-data control systems*, 1995.
- [5] M. Naghnaeian, N. Hirzallah, and P. G. Voulgaris, "Dual rate control for security in cyber-physical systems," in *2015 54th IEEE Conference on Decision and Control*, December 2015, pp. 1415–1420.

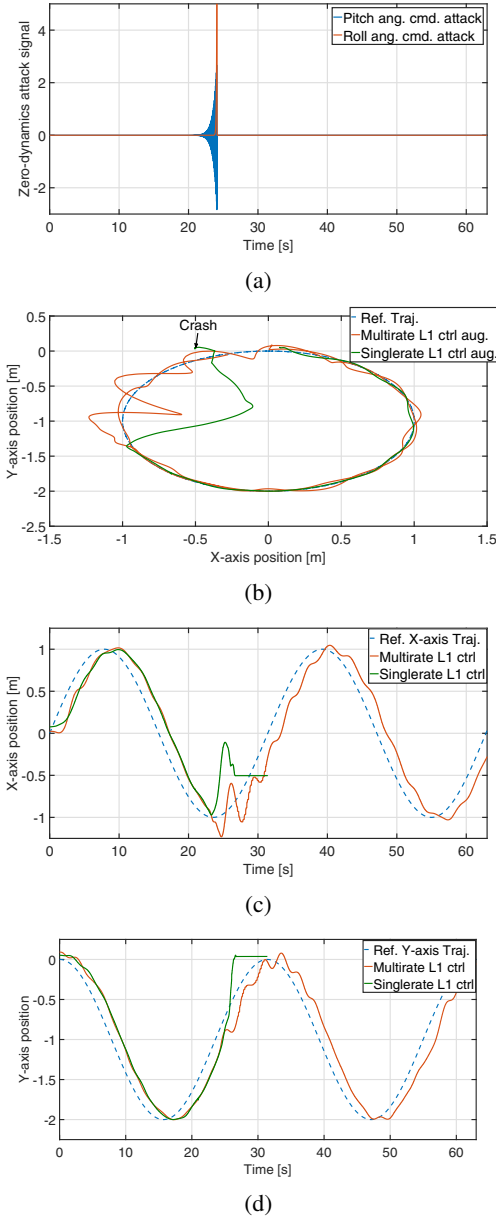


Fig. 3: Response of the closed-loop quadrotor system to the sinusoidal reference command $r_d[k] = [\sin(0.2kT_s), \cos(0.2kT_s) - 1]^T$, and the zero-dynamics attack of the form $d[k] = [\epsilon_x z_x^k, \epsilon_y z_y^k]^T$. (a) Zero-dynamics attack signal. (b) Quadrotor trajectory in x - y plane, under singlerate/multirate $\mathcal{L}_1$ controllers. (c) The x -axis position of Crazyflie vs. time measured by VICON system. (d) The y -axis position of Crazyflie vs. time. measured by VICON system.

- [6] P. G. Voulgaris, M. A. Dahleh, and L. S. Valavani, " H_∞ and H_2 optimal controllers for periodic and multi-rate systems," in *Proceedings of the 30th IEEE Conference on Decision and Control*, December 1991, pp. 214–216.
- [7] L. Qiu and T. Chen, " H_2 optimal design of multirate sampled-data systems," *IEEE Transactions on Automatic Control*, vol. 39, no. 12, pp. 2506–2511, December 1994.
- [8] H. K. Khalil, "Performance recovery under output feedback sampled-data stabilization of a class of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 49, no. 12, pp. 2173–2184, 2004.
- [9] S. Ahmed Ali, N. Langlois, and M. Guermouche, "Sampled-data disturbance observer for a class of nonlinear systems," in *19th World Congress*, vol. 19, no. 1, 2014, pp. 3346–3351.
- [10] C. Zhang and J. Yang, "Semi-global sampled-data output feedback disturbance rejection control for a class of uncertain nonlinear systems," *International Journal of Systems Science*, pp. 1–12, 2016.
- [11] H. Chu, C. Qian, J. Yang, S. Xu, and Y. Liu, "Almost disturbance decoupling for a class of nonlinear systems via sampled-data output feedback control," *International Journal of Robust and Nonlinear Control*, 2015.
- [12] W. Lin and W. Wei, "Robust stabilization of nonminimum-phase systems with uncertainty by sampled-data output feedback," in *55th IEEE Conference on Decision and Control*, Dec 2016, pp. 4078–4083.
- [13] C. Cao and N. Hovakimyan, "Design and analysis of a novel $\mathcal{L}_1$ adaptive control architecture with guaranteed transient performance," *IEEE Transactions on Automatic Control*, vol. 53, no. 2, pp. 586–591, March 2008.
- [14] N. Hovakimyan and C. Cao, *$\mathcal{L}_1$ Adaptive Control Theory: Guaranteed Robustness with Fast Adaptation*. Philadelphia, PA: Society for Industrial and Applied Mathematics, 2010.
- [15] C. Cao and N. Hovakimyan, " $\mathcal{L}_1$ adaptive output-feedback controller for non-strictly-positive-real reference systems: Missile longitudinal autopilot design," *Journal of guidance, control, and dynamics*, vol. 32, no. 3, pp. 717–726, 2009.
- [16] H. Lee, V. Cichella, and N. Hovakimyan, " $\mathcal{L}_1$ adaptive output feedback control for underactuated mimo systems," in *20th IFAC World Congress*, July 2017.
- [17] H. Jafarnejadsani, H. Lee, N. Hovakimyan, and P. G. Voulgaris, "Dual-rate $\mathcal{L}_1$ adaptive controller for cyber-physical sampled-data systems," in *IEEE Conference on Decision and Control*, Melbourne, Australia, December 2017.
- [18] G. Goodwin and K. Sin, "Adaptive control of nonminimum phase systems," *IEEE Transactions on Automatic Control*, vol. 26, no. 2, pp. 478–483, 1981.
- [19] S. Dai, Z. Ren, and D. S. Bernstein, "Adaptive control of nonminimum-phase systems using shifted laurent series," *International Journal of Control*, vol. 90, no. 3, pp. 407–427, 2017.
- [20] M. Makoudi and L. Radouane, "A robust model reference adaptive control for non-minimum phase systems with unknown or time-varying delay," *Automatica*, vol. 36, no. 7, pp. 1057–1065, 2000.
- [21] L. Sha, "Dependable system upgrade," in *Real-Time Systems Symposium, 1998. Proceedings. The 19th IEEE*. IEEE, 1998, pp. 440–448.
- [22] T. L. Crenshaw, E. Gunter, C. L. Robinson, L. Sha, and P. Kumar, "The simplex reference model: Limiting fault-propagation due to unreliable components in cyber-physical system architectures," in *Real-Time Systems Symposium, 2007. RTSS 2007. 28th IEEE International*. IEEE, 2007, pp. 400–412.
- [23] H. Jafarnejadsani, H. Lee, and N. Hovakimyan, "An $\mathcal{L}_1$ adaptive control design for output-feedback sampled-data systems," in *American Control Conference*, May 2017, pp. 5744–5749.
- [24] M.-K. Yoon, B. Liu, N. Hovakimyan, and L. Sha, "Virtualdrone: virtual sensing, actuation, and communication for attack-resilient unmanned aerial systems," in *Proceedings of the 8th International Conference on Cyber-Physical Systems*. ACM, 2017, pp. 143–154.