2015 IEEE 54th Annual Conference on Decision and Control (CDC)
December 15-18, 2015. Osaka, Japan

Dual Rate Control for Security in Cyber-physical Systems

Mohammad Naghnaeian, Nabil Hirzallah and Petros G. Voulgaris

Abstract— **We consider malicious attacks on actuators and sensors of a feedback system which can be modeled as additive, possibly unbounded, disturbances at the digital (cyber) part of the feedback loop. We precisely characterize the role of the unstable poles and zeros of the system in the ability to detect stealthy attacks in the context of the sampled data implementation of the controller in feedback with the continuous (physical) plant. We show that, if there is a single sensor that is guaranteed to be secure and the plant is observable from that sensor, then there exist a class of multirate sampled data controllers that ensure that all attacks remain detectable. These dual rate controllers are sampling the output faster than the zero order hold rate that operates on the control input and as such, they can even provide better nominal performance than single rate, at the price of higher sampling of the continuous output.**

I. Introduction

Security of cyber-physical systems has caught a lot of attention lately. Recent papers along with successful attacks on critical infrastructure together revealed many vulnerabilities in the practiced methods of control. For instance, [1] showed that if a hacker can access the cyber-space of the power grid, then it is easy for him to change the power state estimates without being detected by the traditional bad data detection methods provided that he knows the grid configuration. This led to many research papers investigating the security of the state estimates and suggesting protective measures in addition to investigating attacks on the actuators and/or the plant itself. For example, [2], [3] introduce security indices which quantify the minimum effort needed to change the state estimates without triggering bad-data detectors with perfect and imperfect knowledge of the system as constraints. In [4] the authors considered attacks on control system measurements that are not necessarily bounded or follow a certain distribution and without prior knowledge of the system. They show that it is impossible to reconstruct the states of the system if more than half of the sensors are attacked, generalizing some earlier results in [5]. However, an NP-hard problem has to be solved to detect the attacks. In [6], [7], the authors inject a signal (unknown to the attacker) into the system to detect replay attacks at the expense of increasing the cost of the LQG controller. However, if the plant has an unstable zero then it can be shown that an undetectable attack can still be designed. In [8], the authors suggest the use of dynamic filters that continuously monitor the states of the system at every instance of time. However, the filters have a serious limitation in that they cannot detect zero dynamics attacks. In [9], the authors investigate the class of zero dynamics attacks and suggest adding extra sensors or even perturbing the plant by adding extra connections to remove the unstable zeros. However this may not always be feasible in practice.

In this paper we focus on attacks on actuators and sensors, represented as additive and unbounded disturbances on the digital (i.e., "cyber") part of the controlled system. We examine from an input-output perspective the exact conditions under which such attacks can be stealthy, which brings up the pivotal role of unstable zeros and poles of the open loop, continuous time, physical plant. A key point that the paper brings is the sampled-data (SD) nature of a controlled cyberphysical system which consists of the continuous physical dynamics and the digital controller. The importance of the SD nature lies in the fact that typically, to ensure good intersample behavior, the rate of the sample and hold mechanism has to be high enough. It is known however that high sampling rate can lead to unstable zeros in the discrete plant dynamics. In particular, even if a continuous LTI plant P_c has no unstable zeros, its discrete representation P obtained by the sampled and hold operations will introduce unstable zeros if the relative degree of P_c is greater than two (e.g., [10]) and the sampling period $T \to 0$ (see Figure 1). Therefore, a SD implementation of the controller may create additional vulnerability to stealthy attacks and so, it is important to have ways that secure the safety of the system while achieving the required performance. As one such way, we propose a dual rate sampling approach, a special case of multirate sampling (MR), whereby the output is sampled at a multiple of the hold rate.

Multirate sampling has been studied extensively in the context of sampled-data control in the past and many relevant analysis and synthesis results were obtained in the mid 80s to mid 90s era (e.g., [11], [12], [13], [14], [15] to mention only a few). An interesting property of multi-rate sampling is its ability to remove certain unstable zeros of the discrete-time system when viewed in the lifted LTI domain, which in turn allows for fulfilling certain potential design requirements such as gain margin levels, or, strong stabilization, that are not possible to satisfy with single rate. It is precisely this property that we utilize and study in detail in the context of stealthy attack detection. We show that dual rate control is

M. Naghnaeian is a PhD candidate with the Mechanical Science and Engineering Department, University of Illinois, Urbana, IL, USA naghnae2@illinois.edu

N. Hirzallah is a PhD candidate with the Electrical and Computer Engineering Department, University of Illinois, Urbana, IL, USA hirzall2@illinois.edu

P. G. Voulgaris is with the Aerospace Engineering Department and the Coordinated Science Laboratory, University of Illinois, Urbana, IL, USA voulgari@illinois.edu

This work was supported in part by the National Science Foundation under NSF Award NSF ECCS 10-27437 and AFOSR under award AF FA 9550-12-1-0193

978-1-4799-7886-1/15/$31.00 ©2015 IEEE

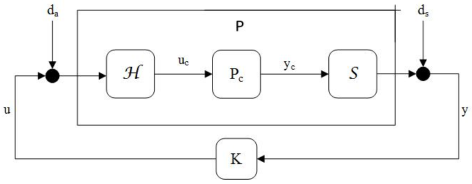


Fig. 1: The standard SD system

sufficient to remove all the vulnerabilities to stealthy actuator attacks. Of course, if all sensors are attacked as well then there is no way to detect attacks. On the other hand, we show that if a single measurement output remains secure, and if the modes of the system are observable from this output, then dual rate systems always provide the ability to detect combined sensor-actuator attacks.

Some standard notation we use is as follows: $\mathbb{Z}_+$, $\mathbb{R}^n$, $\mathbb{C}^n$ and $\mathbb{R}^{n\times m}$ denote the sets of non-negative integers, n-dimensional real vectors, n-dimensional complex vectors and $n \times m$ dimensional real matrices, respectively. For any $\mathbb{R}^n$ or $\mathbb{C}^n$ vector x we denote x' its transpose and $|x| := \max_i \sqrt{x_i^2}$ where $x' = [x_1, x_2, ..., x_n]$; for a sequence of real n-dimensional vectors, $x = \{x(k)\}_{k\in\mathbb{Z}_+}$ we denote $||x|| := \sup_k |x(k)|$; for a sequence of real $n\times m$ dimensional real matrices $G = \{G_k\}_{k\in\mathbb{Z}_+}$ we denote its λ-transform $G(\lambda) := \sum_{k=0}^{\infty} G_k\lambda^k$. For a λ-transform $x(\lambda)$ of a sequence x of n-dimensional vectors $||x(\lambda)|| = ||x||$.

II. System Model

We consider the physical, continuous-time, LTI plant $P_c = [A_c, B_c, C_c, D_c]$ of Figure 1 that is controlled by a digital controller K using the standard zero order hold and sampling devices $\mathcal{H}$ and $\mathcal{S}$ respectively . In particular, in the absence of any disturbances d_a and d_s, the digital controller input $u = \{u(k)\}$ converts to the continuous time input $u_c(t) = (\mathcal{H}u)(t) = u(k)$ for $kT \leq t < (k+1)T$ where T is the hold period, and the digital output $y = \{y(k)\}$ sequence is obtained by sampling the continuous time output y_c with the same period T, i.e., $y(k) = (\mathcal{S}y_c)(k) = y_c(kT)$. The corresponding discrete time LTI plant P is defined by the relation $y = Pu$, i.e., $P = \mathcal{S}P_c\mathcal{H}$, and has a description $P = [A_d, B_d, C_d, D_d]$ where the state space matrices are obtained from the corresponding continuous time as

$$\begin{aligned} A_d &:= e^{A_cT} \in \mathbb{R}^{n\times n}, \quad B_d := \int_0^T e^{A_c\tau}B_c \mathrm{d}\tau \in \mathbb{R}^{n\times n_u}, \\ C_d &:= C_c \in \mathbb{R}^{n_y\times n}, \qquad D_d := D_c \in \mathbb{R}^{n_y\times n_u}. \end{aligned} \tag{1}$$

We assume that the employed realization of the continuous plant P_c is minimal, which implies that the same holds true for the discrete plant P in the absence of pathological sampling (e.g., [10],) i.e., for almost all periods T.

Also in this figure, we consider the possibility of attacks in terms of additive disturbances d_a and d_s respectively at the digital input u and at the output y of P. These attacks on the digital part of the system can be on actuators only ($d_s = 0$), sensors only ($d_a = 0$), or on both, coordinated or not. As they act on the cyber part of the system we allow them to be unbounded sequences.

We assume that there is an attack detection mechanism in place that monitors u and y and can detect an attack only if the effect of d_a and/or d_s on these signals is beyond a given noise level threshold $\theta > 0$, i.e., only if $\left|\begin{bmatrix} y \\ u \end{bmatrix}(k)\right| > \theta$ for some k. Note that we implicitly assume that there are other inputs such as noise, not shown in Figure 1, that have some effect on u and y which is what relates to the nonzero noise level θ. Accordingly, a stealthy attack will be the case when the attack inputs d_a and/or d_s can grow unbounded while maintaining their effect on u and y below the detection limit. Specifically, if d represents any of d_a or d_s, then the attack is stealthy if $\limsup_{k\to\infty} |d(k)| = \infty$ while $\left|\begin{bmatrix} y \\ u \end{bmatrix}(k)\right| \leq \theta$ all $k = 0, 1, 2, \ldots$. In the sequel we consider various attack scenarios and analyze the conditions of their detectability.

III. Actuator Attacks

We start with the case when only actuator attacks d_a are present ($d_s = 0$) and proceed in characterizing their effect on the monitoring vector $\begin{bmatrix} y \\ u \end{bmatrix}$. Towards this end, let P be factored as $P = \tilde{M}^{-1}\tilde{N} = NM^{-1}$ where $\tilde{N}, \tilde{M}$ and N, M are left and right coprime respectively, and consider the controller K with a similar coprime factorization as $K = \tilde{X}^{-1}\tilde{Y} = YX^{-1}$. The mappings from d_a to y and u are given respectively as $(I - PK)^{-1}P$ and $K(I - PK)^{-1}P$. Given that K stabilizes P, it holds that $\tilde{M}X - \tilde{N}Y =: W$ is a stable and stably invertible map (unit). Moreover, it can be easily checked that

$$\begin{bmatrix} y \\ u \end{bmatrix} = \begin{bmatrix} X \\ Y \end{bmatrix} W\tilde{N}d_a. \tag{2}$$

As X and Y are right coprime and W is a unit, it follows that a stealthy attack is possible if and only if $\tilde{N}d_a$ is bounded for an unbounded d_a. That is, when $\limsup_{k\to\infty} |d_a(k)| = \infty$ it holds that $\left\|\begin{bmatrix} y \\ u \end{bmatrix}\right\| < \infty$ if and only if $\left\|\tilde{N}d_a\right\| < \infty$. The following proposition is a direct consequence of the previous analysis.

Proposition 1: Let P be a "tall" system, i.e., the number of outputs is greater or equal to the number of inputs. Assume further that $P(\lambda)$ has no zero on the unit circle $|\lambda| = 1$. Then, an (unbounded) actuator stealthy attack is possible if and only if $P(\lambda)$ has a non-minimum phase zero other than at $\lambda = 0$, i.e., a zero for $0 < |\lambda| < 1$.

Proof: The proof is omitted and can be found in [16]. ■

Remark 2: We remark here that if P has zeros on the boundary $|\lambda| = 1$ with no multiplicity but no other unstable zeros (other than at $\lambda = 0$,) then stealth attacks are not possible. Indeed, if z_0 is a simple zero with $|z_0| = 1$, then the corresponding input that can be masked ("zeroed out") is of the form $d_a(k) = \epsilon d_0 {z_0}^{-k}$ which is bounded with $|d_a(k)| < \epsilon$, and becomes undetected for small enough ϵ. But this case is uninteresting, as the disturbance has a level of noise (which can be taken care by any reasonably robust controller.) On the other hand, if there are multiplicities, stealthy attacks are possible. For example, if P is SISO and $z_0 = 1$ is a zero with multiplicity 2, then an unbounded input of the form $d_a(k) = \epsilon k$, $k = 0, 1, \dots$ remains undetected for small enough ϵ. More generally, in the MIMO case when a zero at the boundary has multiplicity, one has to check the Smith-McMillan form of $P(\lambda)$ for invariant factors with multiplicity corresponding to these zeros: stealthy attacks are possible if and only if there are such factors.

Remark 3: When there is a zero of P at $\lambda = 0$ there is no corresponding (causal) input signal to be "zeroed out."

The case when P is "fat", i.e. when the number of outputs y is less than the number of inputs u, is always conducive to stealthy attacks as one input can mask the effect of the other. Indeed, consider a two input one output $P = [P_1 \; P_2]$; the effect of attacks at the individual control channels d_{a1} and d_{a2} on the output y is $y = P_1 d_{a1} + P_2 d_{a2} + [P_1 \; P_2]u$ and thus, picking for example, $d_{a2} = -P_2^{-1} P_1 d_{a1}$ with d_{a1} arbitrary and unbounded leads to $y = [P_1 \; P_2]u$, i.e. complete masking of the attacks. [1]

IV. Sensor Attacks

The case of sensor only attack $d_s \neq 0, d_a = 0$ can be viewed in a similar spirit. In particular, by considering coprime factorizations for P and K as before, the effect of d_s on the monitor vector is as

$$\begin{bmatrix} y \\ u \end{bmatrix} = \begin{bmatrix} (I - PK)^{-1} \\ K(I - PK)^{-1} \end{bmatrix} d_s = \begin{bmatrix} X \\ Y \end{bmatrix} W \tilde{M} d_s. \qquad (3)$$

Therefore, using the same rationale as in the previous case, we can claim that an attack is detectable if and only if there are no d_s with $\|d_s\| = \infty$ and $\left\|\tilde{M} d_s\right\| < \infty$. This in turn means that attacks are detectable if and only if $\tilde{M}$ has no unstable zeros, which is equivalent that P is a stable system. More specifically, we have the following which can be proved as in the Proposition 1.

Proposition 4: Assume that $P(\lambda)$ has no pole on the unit circle $|\lambda| = 1$. Then, a sensor stealthy attack is possible if and only if $P(\lambda)$ has a pole with $0 < |\lambda| < 1$, i.e., an unstable pole other than $\lambda = 0$.

Regarding poles of $P(\lambda)$ on the boundary $|\lambda| = 1$ similar remarks hold as in the actuator attack case. Namely, if these poles are simple then there is no stealthy attack. If they have multiplicities, then their multiplicities in the corresponding invariant factors in the Smith-McMillan form determine whether stealthy attacks are possible.

V. Coordinated Actuator Sensor Attacks

In the case when a coordination of actuator and sensor attack is possible, stealthy attacks are always possible even in the case where P is stable and minimum phase. Indeed, in this case the effect of d_a can be completely masked by canceling its effect at the output via d_s: just pick $d_s = -P d_a$ with d_a arbitrary and unbounded, then $y = Pu$. Therefore, unless there are outputs that are not attacked, this situation is not of interest as there is no hope to detect the attack. If there are such attack-free outputs, then the problem reverts to the actuator only attack case, with these outputs used for analysis and design. As a consequence, in the sequel we consider the actuator only attack case where the secure sensor outputs are assumed to provide an observable continuous time system P_c.

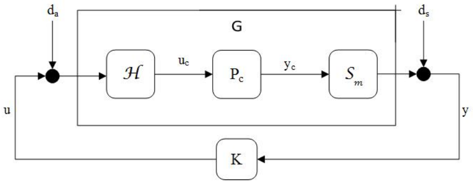


Fig. 2: A dual rate SD system

VI. Dual Rate Control

In this paper, we focus on a particular MR scheme that allows attacks to be detected by ensuring that there are no relevant unstable zeros in the lifted system. This scheme is similer to the single rate one with periodic controller obtained in the context of gain margin maximization in [17]. More specifically, we consider the SD scheme of Figure 2 (temporarily without any disturbances) where the output is sampled with period T/m where m is a sufficiently large integer, i.e., $y(k) = (\mathcal{S}_m y_c)(t) := y_c(kT/m)$. A similar scheme has been used in [11] in the context of strong stabilization. Herein, we provide certain properties of the unstable zeros of the lifted system that guarantee detectability of actuator attacks.

To this end, let the corresponding discrete-time system mapping u to y be

$$G = \mathcal{S}_m P_c \mathcal{H}.$$

For this MR discrete system we have that

$$\Lambda^m G = G \Lambda$$

where Λ is the 1-step right shift operator on discrete sequences $\{x(k)\}$, i.e., $(\Lambda x)(k+1) = x(k)$ with $(\Lambda x)(0) = 0$. Using standard lifting techniques (e.g., [10]) one can obtain a shift invariant (LTI) description $\tilde{G}$ of the discrete dynamics by grouping the plant input and output signals as $\tilde{u}(k) = u(k)$ and $\tilde{y}(k) = [y_c'(kT/m) \; y_c'((k+1)T/m) \dots y_c'((k+m-1)T/m)]'$ (similarly for $\tilde{d}_a$ and $\tilde{d}_s$.) A state space description for $\tilde{G}$ can be obtained as follows:

Define state space matrices

$$A := e^{A_c T/m} \in \mathbb{R}^{n \times n}, \quad B := \int_0^{T/m} e^{A_c \tau} B_c \mathrm{d}\tau \in \mathbb{R}^{n \times n_u},$$
$$C := C_c \in \mathbb{R}^{n_y \times n}, \qquad D := D_c \in \mathbb{R}^{n_y \times n_u}.$$

Then

$$\tilde{G} = \left[\begin{array}{c|c} \tilde{A} & \tilde{B} \\ \hline \tilde{C} & \tilde{D} \end{array} \right], \qquad (4)$$

[1] Strictly speaking, P_2^{-1} may not exist if P_2 is strictly proper , i.e., P_2 has a zero at $\lambda = 0$; but one can always pick $d_{a1}(\lambda) = \lambda \bar{d}_{a1}(\lambda)$ with $\bar{d}_{a1}$ unbounded and make $(P_2^{-1} P_1 d_{a1})(\lambda)$ meaningful.

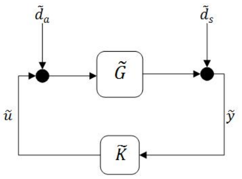


Fig. 3: The lifted system

where

$$\begin{aligned}\tilde{A} &= A^m \in \mathbb{R}^{n\times n}, \tilde{B} = \sum_{k=0}^{m-1} A^k B \in \mathbb{R}^{n\times n_u},\\ \tilde{C} &= \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{m-1} \end{bmatrix} \in \mathbb{R}^{mn_y \times n},\\ \tilde{D} &= \begin{bmatrix} D \\ CB + D \\ \vdots \\ C\sum_{k=0}^{m-2} A^k B + D \end{bmatrix} \in \mathbb{R}^{mn_y \times n_u}.\end{aligned}$$

Also, it becomes useful to define a discrete-time system $P_m := \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$. This system corresponds to the single-rate sampling and hold scheme of the original plant P_c with a period of T/m, i.e., $P_m = \mathcal{S}_m P_c \mathcal{H}_m$ where $\mathcal{H}_m$ is accordingly generating a continuous signal u_c from the discrete u as $u_c(t) = (\mathcal{H}_m u)(t) = u(k)$ for $kT/m \le t < (k+1)T/m$. It is clear that P_m has the same dimension as P_c, i.e. it maps n_u inputs to n_y outputs. Moreover, given that P_c holds a controllable and observable realization, and the sampling is not pathological, it follows that the inherited realization of P_m is also controllable and observable. Based on our assumptions on the sampling, it is also easily verified that the realization of $\tilde{G}$ as above is controllable and observable. Let $\tilde{M}_{\tilde{G}}$ and $\tilde{N}_{\tilde{G}}$ be the left coprime factors of $\tilde{G}$. We will use the state-space realization of $\tilde{N}_{\tilde{G}}$ as

$$\tilde{N}_{\tilde{G}} = \left[\begin{array}{c|c} \tilde{A} + H\tilde{C} & \tilde{B} + H\tilde{D} \\ \hline \tilde{C} & \tilde{D} \end{array}\right], \tag{5}$$

where H is chosen such that $\tilde{A} + H\tilde{C}$ is Schur stable. It is easy to show that $\tilde{G}$ and $\tilde{N}_{\tilde{G}}$ have the same non-minimum phase zeros. We consider now the closed loop in the lifted domain in Figure 3 where the controller is $\tilde{K}$ and proceed to argue that the lifted loop is not susceptible to stealthy actuator attacks $\tilde{d}_a$, and thus the original MR loop of Figure 2 is not susceptible either. To this end, the integer m is chosen such that the following assumptions are satisfied.

Assumption 5: The matrix B is full column rank.

Assumption 6: The matrix $\mathcal{O} : = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{m-2} \end{bmatrix}$ is full column rank.

The first assumption is standard and holds generically if B_c is full column rank in the continuous system. The second assumption holds for large enough m, in particular $m = n + 1$, if the pair (A, C) is observable, which is true as P_m is minimal. It can also hold however, even with a small m generically. Also, if Assumption 6 holds, $\tilde{G}$ is a tall system. Then the following lemma characterizes the zeros of $\tilde{G}$.

Lemma 7: Consider the lifted system $\tilde{G}$ as in (4) together with Assumptions (5) and (6). Then $\tilde{G}$ has at most one non-minimum zero and is located at $\lambda = 1$.

Proof: The proof is omitted and can be found in [16]. ■

According to Lemma 7, the lifted system, $\tilde{G}$, has no zeros inside the unit circle. However, it may have a zero at $\lambda = 1$. Based on Proposition 1 and Remark 2, an (unbounded) actuator stealthy attack will not possible if $\lambda = 1$ is zero of $\tilde{G}$ with multiplicity of at most one. Indeed, this is the case as it is proved in the following theorem:

Theorem 8: Consider the dual rate SD scheme as in Figure 3. Then, there does not exist any (unbounded) actuator stealthy attack if Assumptions 5 and 6 are met.

Proof: The proof is omitted and can be found in [16]. ■

As a final comment from the previous analysis, we offer conditions when $\tilde{G}$ has a zero $\lambda = 1$. We note that, as proved in the previous theorem, these zeros are not a problem since they cannot generate stealthy attacks.

Proposition 9: Let P_c be "tall." Then $\tilde{G}$ has a zero at $\lambda = 1$ if and only if P_m does.

Proof: The proof can be found in [16]. ■

Proposition 10: Let P_c be "fat." Then $\tilde{G}$ has always a zero at $\lambda = 1$.

Proof: The proof can be found in [16]. ■

Remark 11: We would like to point out that an equivalent way of obtaining the same results, i.e., ability to detect zero attacks, is to hold the control input longer rather than sampling the output faster. That is, if we consider a dual rate system where the hold operates with a period of mT while the output is sampled with T, then the corresponding lifted system will enjoy the same properties as before in terms of unstable zeros. Obviously, the (nominal) controller performance will be reduced as the control is slower. On the other hand, there is a potential benefit of lower cost of actuation in this case. An example offered in the next session illustrates this point.

VII. Example

In this section we provide an example of a system that is insecure under zero dynamics attacks, then we apply the techniques presented in the previous sections to defend the system.

A. Automatic Voltage Regulator

The system is the automatic voltage regulator (AVR) or the generator excitation control. AVR specifies the terminal voltage magnitude of a synchronous generator by controlling the reactive power. A simplified block diagram of a linearized

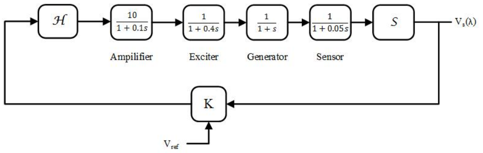


Fig. 4: A simplified automatic voltage regulator block diagram

AVR is shown in Figure 4 [18]. An increase in the reactive power load of the generator results in a drop in the voltage magnitude across its terminals. The voltage drop is sensed by a potential transformer which then is rectified and compared to the reference voltage magnitude. The error signal is then amplified and raises the generator terminal voltage by controlling the excitation field. The open loop state space representation of the single rate system after discretization at a sample rate $T = 0.5$secs is

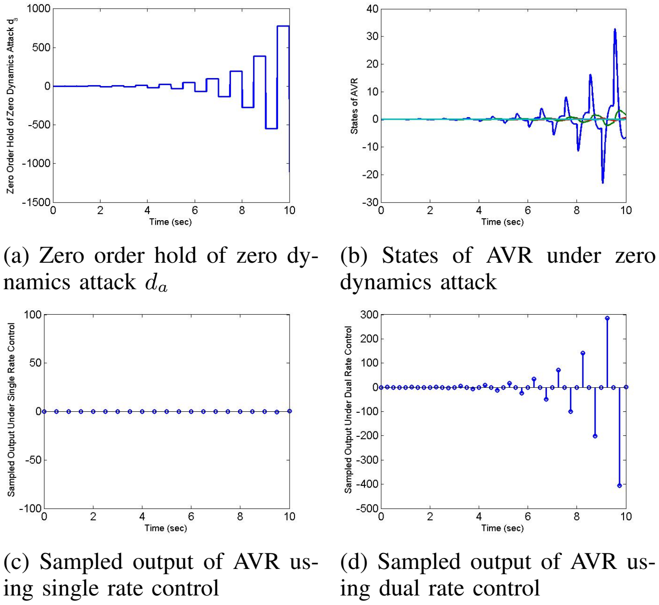
$$A_d = \begin{bmatrix} 0.0105 & 0.3949 & 3.86 & 2.869 \\ -0.0057 & -0.1817 & -1.369 & -0.587 \\ 0.00117 & 0.03359 & 0.1793 & -0.4597 \\ 0.00092 & 0.03197 & 0.3163 & 0.8918 \end{bmatrix},$$
$$B_d = \begin{bmatrix} -0.005738 \\ 0.001174 \\ 0.0009193 \\ 0.0002165 \end{bmatrix}, C_d = \begin{bmatrix} 0 & 0 & 0 & 5000 \end{bmatrix}, D_d = [0]$$

which has an unstable zero at $\lambda = -0.7045$. We note that although the continuous system has no unstable zeros, sampling at the relative slow rate of 0.5secs per sample created an unstable zero. Next we consider an attack input of the form $d_a(k) = \epsilon {z_0}^{-k}$ where ϵ is a small number and z_0 is the zero of the system. Figures 5a–5c shows a plot of the attack held at $T = 0.5$secs along with the states and the sampled output of the system. We can notice that while the states of the system are exploding, the sampled output remains zero and no attack is detected.

Next, we change the single rate block diagram to a multirate architecture to move the unstable zero to the safe region. We sample faster at rate $T/m = 0.5/2 = 0.25$secs per sample while keeping the hold at rate $T = 0.5$secs. The resulting open loop state space representation after lifting is

$$\tilde{A} = A_d, \ \tilde{B} = B_d,$$
$$\tilde{C} = \begin{bmatrix} 0 & 0 & 0 & 5000 \\ 2.185 & 86.13 & 1092 & 4902 \end{bmatrix}, \tilde{D} = \begin{bmatrix} 0 \\ 0.196 \end{bmatrix}$$

The resulting open loop system has no unstable zeros. We note that only a small m is enough to accomplish our goal, i.e., $m = 2$. In fact, Assumption 6, a sufficient condition for Theorem 1 to hold, is not even satisfied in this case and yet the unstable zeros are removed. We consider the same attack input as above and simulate the system. The sampled output at rate $T = 0.25$sec is shown in Figure 5d. It is obvious that the multirate scheme detects the attack on the system



(a) Zero order hold of zero dynamics attack d_a

(b) States of AVR under zero dynamics attack

(c) Sampled output of AVR using single rate control

(d) Sampled output of AVR using dual rate control

Fig. 5: Figures 5a–5c Show simulation of zero dynamics attack on a sampled-data AVR system under signle rate control. Figure 5d Show the sampled output under dual rate control

B. Optimal LQG Control

In this section we revisit the automatic voltage regulation system previously discussed in order to investigate trade offs in the controller design. In particular, we will close the control loop by designing linear quadratic Gaussian (LQG) controllers for the dual rate system and compare the cost with single rate LQG controllers. We set up a baseline LQG formulation for the dynamics of the open loop AVR with sampled measurements of period s as

$$\begin{aligned} \mathrm{d}x(t) &= A_c x(t)\mathrm{d}t + B_c \omega_c(t)\mathrm{d}t + B_c u_c(t)\mathrm{d}t, \\ y(k) &= C_c x(ks) \ + v(k), \ k = 0, 1, \ldots \end{aligned}$$

We assume that the process noise $\{\omega_c(t), t \geq 0\}$ is a Brownian motion with $\mathcal{E}\{\mathrm{d}\omega_c(t)\mathrm{d}\omega_c(t)'\} = \Xi_c$, the observation noise $\{v(k), k = 0, 1...\}$ is a zero mean white Gaussian sequence with covariance $\Theta = \mathcal{E}\{v(k)v(k)'\}$, and $x(0)$ is zero mean Gaussian with covariance $S_0 = \mathcal{E}\{x(0)x(0)'\}$. Moreover, it is assumed that the random variables $x(0), v(k), \omega_c(t)$ are independent. We assume that the hold period is h. The objective is to minimize the following cost

$$J = \mathcal{E}\Big\{ \limsup_{k\to\infty} (1/kh) \int_0^{kh} (x' Q_c x + u_c R_c u_c')\mathrm{d}t \Big\}$$

with the usual positive definiteness conditions $Q_c = Q_c' \geq 0$ and $R_c = R_c' > 0$, which transforms to

$$J = \mathcal{E}\Big\{ \limsup_{k\to\infty} (1/k) \sum_{k=0}^{\infty} (x_k' Q x_k + 2x_k' S u_k + u_k' R u_k) \Big\}$$

with $x_k := x(kh)$, $u_k := u_c(kh)$ and

$$\begin{aligned} &Q = \textstyle\int_0^h e^{A_c'\tau} Q_c e^{A_c \tau} \mathrm{d}\tau \\ &S = \textstyle\int_0^h e^{A_c' t} Q_c \big(\int_0^t e^{A_c(t-\tau)} B_c \mathrm{d}\tau \big) \mathrm{d}t \\ &R = \textstyle\int_0^h \big[\big(\int_0^t B_c' e^{A_c'(t-\tau)} \mathrm{d}\tau \big) Q_c \\ &\qquad\qquad\qquad\qquad \big(\textstyle\int_0^t e^{A_c(t-\tau)} B_c \mathrm{d}\tau \big) + R_c \big] \mathrm{d}t \\ &\Xi = \textstyle\int_0^s e^{A_c(s-\tau)} B_c \Xi_c B_c' e^{A_c'(s-\tau)} \mathrm{d}\tau \end{aligned}$$

TABLE I: LQG Cost

$s\backslash h$	0.5	1
0.25	0.6704	-
0.5	0.6868	0.6877
1	-	0.7047

The hold and sample periods h and s are assumed to be integer related and in particular $h = ms$ with $m = 1, 2, \ldots$. In this synchronous dual rate case, rather than using lifting techniques to solve the problem, we take the separation principle approach which applies also to asynchronous sampling (e.g., [19]) to find the optimal cost by computing

$$J_o = \text{trace}\big[PF'(R + B_h'X)B_hF + X\Xi\big]$$

where X and P are the unique positive semidefinite symmetric solutions of the algebraic Riccati equations

$$\begin{aligned} X &= A_h'XA_h - (S + A_h'B_hX)(R + B_h'XB_h)^{-1} \\ &\qquad\qquad\qquad\qquad (XB_h'A_h + S') + Q \\ P &= A_sPA_s' - A_sPC_s'(C_sPC_s' + \Theta)^{-1}C_sPA_s' + \Xi \end{aligned}$$

and

$$F = (B_h'XB_h + R)^{-1}(B_h'XA_h + S')$$

where the various A, B, C-matrices above are corresponding to the matrices in Equation (1) for $T = h$ and $T = s$, i.e., $A_h = e^{A_ch}$, $A_s = e^{A_cs}$, etc. Table I summarizes the LQG cost for different single rate and dual rate sample and hold for the case $\Xi_c = 10^3$, $\Theta = 10$, $Q_c = I_4$ and $R_c = I$. We notice that, because of faster sampling, we get better performance in dual rate control than single rate control. Also, as expected, we get better performance between dual rate controllers when we increase the rate of sampling rather than decreasing the rate of the zero order hold. Faster sampling however may require more expensive devices and so a trade-off is present.

VIII. Conclusion

We presented a simple dual rate sampled data scheme which guarantees detectability of actuator and/or sensor attacks, if a secure output that maintains observability of the open loop modes is available. The main observation is that the sampled data nature in the implementation of the cybephysical system cannot be ignored as sampling can generate additional vulnerabilities due to the extra unstable zeros it may introduce, particularly if high rates are necessary to achieve certain performance level. The proposed method takes care of this issue by the use of multirate sampling that ensures that zeros exist only in harmless locations in the lifted domain. We gave certain precise conditions on the detectability of stealthy attacks in terms of the open loop unstable poles and zeros and showed how the vulnerabilities can be eradicated by the use of the dual rate scheme. An example was also presented.

Several other possibilities can be studied in this context. The use of asynchronous sampling (e.g., [19], [20]) can provide alternative ways to detect stealthy attacks; or even the network's random delays can be helpful in that respect; the speed of detecting however needs to be brought into consideration, even if the attack is detectable. The methods of generalized holds [21] are also relevant as they move zeros, and with careful analysis of their robustness properties (e.g., [22]) can provide acceptable and simple solutions as well. All of these are subjects of current investigations by the authors and are documented in forthcoming publications.

References

[1] Y. Liu, M. K. Reiter, and P. Ning. "False data injection attacks against state estimation in electric power grids". *ACM Conference on Computer and Communications Security*, Chicago, IL, USA, Nov. 2009, pp. 21,32.

[2] H. Sandberg, A. Teixeira, and K. H. Johansson. "On security indices for state estimators in power networks". *First Workshop on Secure Control Systems,* Stockholm, Sweden, 2010.

[3] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry. "Cyber security analysis of state estimators in electric power systems". *IEEE Conference on Decisions and Control,* Atlanta, GA, USA, Dec. 2010.

[4] H. Fawzi, P. Tabuada, P. Diggavi. "Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks". *IEEE Transactions on Automatic Control,* vol.59, no.6, pp.1454,1467, June 2014.

[5] S. Sundaram, C.N. Hadjicostis. "Distributed Function Calculation via Linear Iterative Strategies in the Presence of Malicious Agents". *IEEE Transactions on Automatic Control*, vol.56, no.7, pp.1495,1508, July 2011.

[6] Y. Mo and B. Sinopoli. "Secure control against replay attacks". *Allerton Conf. on Communications, Control and Computing,* Monticello, IL, USA, Sept. 2010, pp. 911-918.

[7] R. Chabukswar, Y. Mo, and B. Sinopoli. "Detecting Integrity Attacks on SCADA Systems". *IEEE Transactions on Control Systems Technology: a Publication of the IEEE Control Systems Society*, vol.22, no.4, pp.1396,1407, July 2014.

[8] F. Pasqualetti and F. Dorfler and F. Bullo. "Attack Detection and Identification in Cyber-Physical Systems". *IEEE Transactions on Automatic Control,* vol.58, no.11, pp.2715-2729, 2013.

[9] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. "Revealing Stealthy Attacks in Control Systems". *Allerton Conf. on Communication, Control, and Computing,* Allerton, IL, USA, 2012.

[10] T. Chen and B. Francis. *Optimal Sampled-Data Control Systems*. (errerta). Springer, 1995.

[11] T. Hagiwara, M. Araki, "Design of a stable state feedback controller based on the multirate sampling of the plant output". *IEEE Transactions on Automatic Control,* vol.33, no.9, pp.812,819, Sep 1988.

[12] P.G. Voulgaris, M.A. Dahleh and L.S. Valavani. "H_∞ and H_2 optimal controllers for periodic and multirate systems". *Automatica,* vol. 30, no. 2, pp. 252-263, 1994.

[13] P.G. Voulgaris, B. Bamieh. "Optimal H_∞ and H_2 control of hybrid multirate systems". *Systems and Control Letters,* no. 20, pp. 249-261, 1993.

[14] T. Chen., L. Qiu. "H_∞ design of general multirate sampled-data control systems". *IEEE Transactions on Automatic Control,* vol.39, no.12, pp.2506-2511, 1994.

[15] L. Qiu, T. Chen. "H_2 optimal design of multirate sampled-data systems". *Automatica,* Volume 30, Issue 7, July 1994, Pages 1139-1152.

[16] M. Naghnaeian, N. Hirzallah, and P. G. Voulgaris. "Dual Rate Control for Security in Cyber-physical Systems". arXiv:1504.07586, 2015.

[17] B.A. Francis,, T.T. Georgiou. "Stability theory for linear time-invariant plants with periodic digital controllers". *IEEE Transactions on Automatic Control,* vol.33, no.9, pp.820,832, Sep 1988.

[18] H. Saadat. *Power System Analysis*. McGraw-Hill Companies, 2002.

[19] P.G. Voulgaris. "Control of asynchronous sampled-data systems". *IEEE Transactions on Automatic Control,* vol. 39, no. 7, pp. 1451-1455, July 1994.

[20] M. F. Sagfors, H. T. Toivonen. "H_∞ and LQG control of asynchronous sampled-data systems". *Automatica,* Volume 33, Issue 9, September 1997, Pages 1663-1668.

[21] P.T. Kabamba. "Control of linear systems using generalized sampled-data hold functions". *IEEE Transactions on Automatic Control,* vol.32, no.9, pp.772,783, Sep 1987.

[22] J.S Freudenberg, R.H. Middleton, J.H. Braslavsky. "Robustness of zero shifting via generalized sampled-data hold functions". *IEEE Transactions on Automatic Control,* vol.42, no.12, pp.1681,1692, Dec 1997.