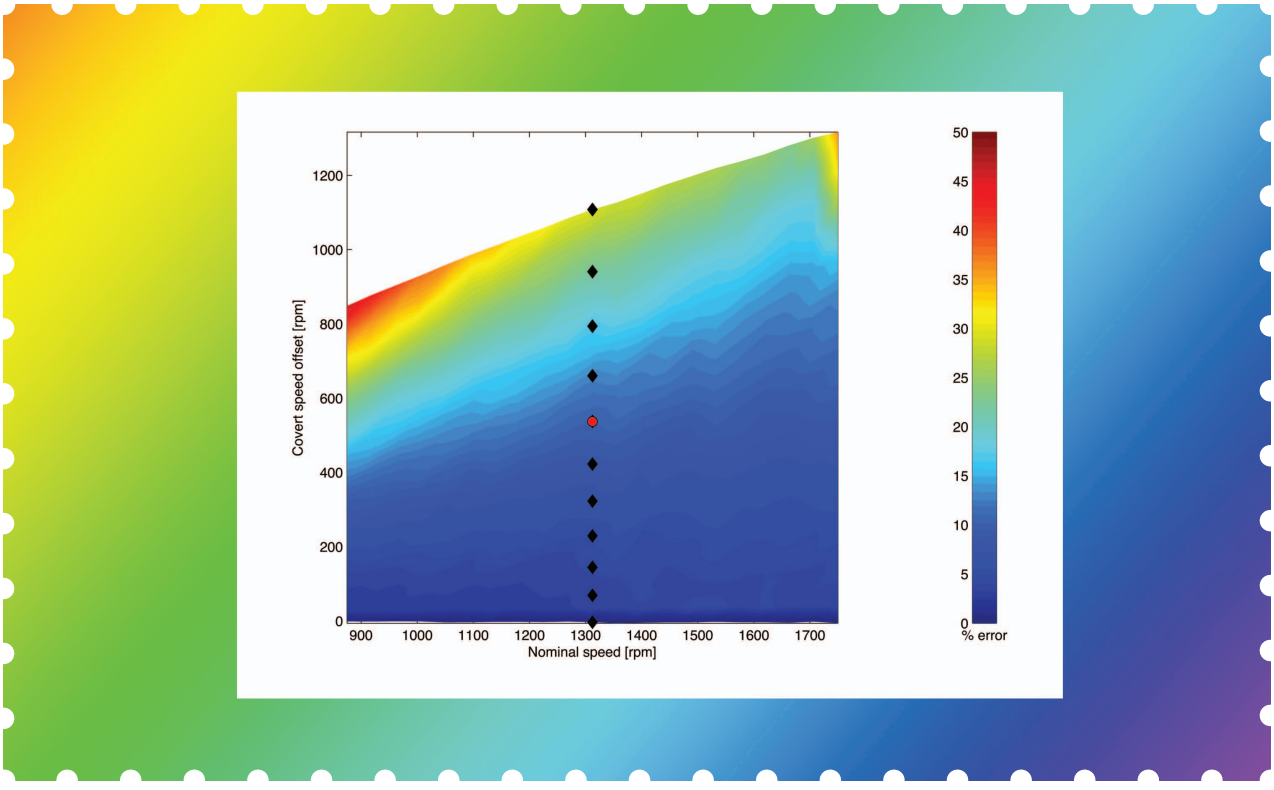
Covert Misappropriation of Networked Control Systems

PRESENTING A FEEDBACK STRUCTURE



ROY S. SMITH

The increasing availability of Internet connectivity and networked actuation and sensing components has supported the growth in control systems operated over public networks. Controllers and plants no longer need to be physically colocated as measurements and actuation signals can be sent digitally. Supervisory systems can monitor and control geographically widespread components. However, such systems are now exposed to the risk of remote interference. A feedback structure that allows an attacker to take over control of the plant while remaining hidden from the control and supervisory system(s) is presented. The objective is not to facilitate such attacks but rather to make clear the degree to which the takeover of plant control can be hidden when a sophisticated attacker has some plant knowledge and signal intervention capabilities.

Digital Object Identifier 10.1109/MCS.2014.2364723
Date of publication: 19 January 2015

1066-033X/15©2015IEEE

From a control engineer's point of view, the Stuxnet attack was rather naïve.

Network security has been an active topic of research for many years with a variety of network and infrastructure attacks having already been perpetrated. The most dramatic in recent times—and the most relevant from a control perspective—was the Stuxnet virus, directed primarily at the controllers operating motor-driven centrifuges in the Iranian nuclear program. The compromised equipment in this case included programmable logic controllers (PLCs), which are in widespread use in many industrial control systems.

The Stuxnet attack was a replay attack. The virus recorded data from normal plant operation over several months and replayed it to the supervisory system while it was issuing its own, ultimately destructive, commands to the plant. The analysis of Stuxnet in [1] focused primarily on its infection capabilities, mechanisms for gaining root access, and, to a lesser extent, the state-machine specifying its attack strategy. Furthermore, detection of the attack was considered only in the context of the detection of corrupted code on the control and supervisory computers.

Conversely, this article looks at attacks of this form from a control-systems perspective. From a control engineer's point of view, the Stuxnet attack was rather naïve; it could have been easily detected using probing signals or a careful analysis of the noise and disturbance characteristics. A supervisory system looking for such attacks would use knowledge of the plant dynamics, noise statistics, and disturbance characteristics in its analysis of the measurement and actuation signals. The supervisory system could, for example, superimpose probing signals on the actuation signals and then check the dynamic response observed in the measurements. It could also collect statistics about the noise and characterize the typical disturbances. These should be similar—but obviously not identical—to previously recorded signal characteristics. There are many variants to the signal-based attack detection problem, and examples can be found in [2] and the references therein. The question considered here is whether or not such measures are sufficient to detect a determined attacker with sufficient resources. Unfortunately, the answer is "probably not."

There is a growing interest, within the control community, in research on attacks on control systems. One area, studied by several groups, is the security of supervisory control and data acquisition (SCADA) systems [3]–[6], typically within the context of power distribution networks [7]–[9]. More recently, [10] gives a detailed general framework for the analysis of a wide variety of methods of control system attack. A covert attack for linear systems that requires (in the classification framework of [10]) high levels of system knowledge as well as high disclosure and disruption resources is described in [11], where the attacker has the ability to both read and replace communicated signals within the loop. This article examines the effects of lower levels of system knowledge and nonlinear plants on the ability to detect covert attacks.

The method of attack considered here is a covert misappropriation of the plant. The ability of a covert agent to remain undetected is key and requires more sophisticated resources and more plant knowledge than a brute-force disruptive attack (for example, a denial-of-service attack). There is a potential economic motivation for covert misappropriation attacks. In networked control systems where the control and plant(s) are owned by different entities, there is a monetary advantage—albeit an illegal one—in deceiving the controller about the consumption of resources or the quality of the plant's performance. Obvious examples include diverting water in irrigation schemes and minimizing measured consumption in electrical grids. In such cases, the attacker clearly wants to remain undetected. It is perhaps unsurprising that we are unaware of any reported instances of this form of attack in practice.

COVERT NETWORKED CONTROL SYSTEM MISAPPROPRIATION

Nominal Networked Control System

The networked control system scenario to be considered is illustrated in Figure 1. Both the actuation and the measurement signals are transmitted between the plant and the controller over a communication network. Details of the

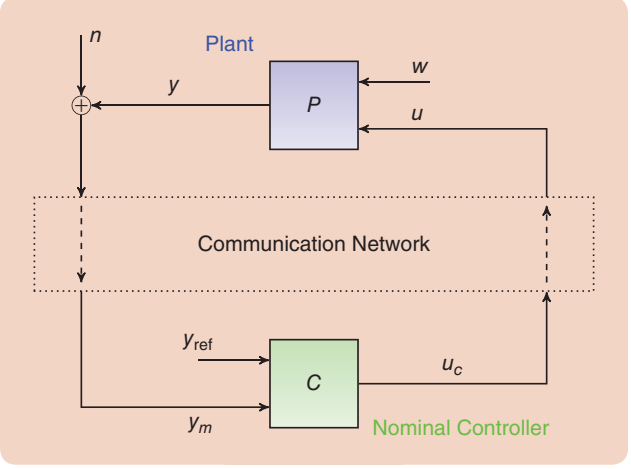


FIGURE 1 A networked control system. The nominal controller is assumed to have been designed to be sufficiently robust to the usual delays that may occur in the communication network. The nominal operating case is $u = u_c$ and $y_m = y + n$.

encoding and decoding of the signals are not discussed here, and, for simplicity, communication delays or packet losses are not considered. These will, of course, occur, and a well-designed nominal controller would be expected to have a certain robustness to delays as well as a backup strategy for handling missing information due to packet loss.

Assume that the plant is linear time-invariant (LTI) and driven by disturbances w, and control actuation u_c,

$$y = P_u u_c + P_w w. \tag{1}$$

The notation here considers P_u and P_w to be LTI operators that map signals u_c and w to the output y. Since the results that follow depend only on linearity, the signals and systems can be viewed in either the time or frequency domains, and so the operation given above can denote either convolution or multiplication depending on the domain. The systems may be multiple-input, multiple-output (MIMO), in which case the operators in (1) are matrix valued and the corresponding input and output signals are vector valued of the appropriate dimensions.

The output measured by the nominal controller is, in the nominal case, corrupted by noise

$$y_m = y + n. \tag{2}$$

The nominal controller generates the actuation command via

$$u_c = C_y y_m + C_{\text{ref}} y_{\text{ref}}. \tag{3}$$

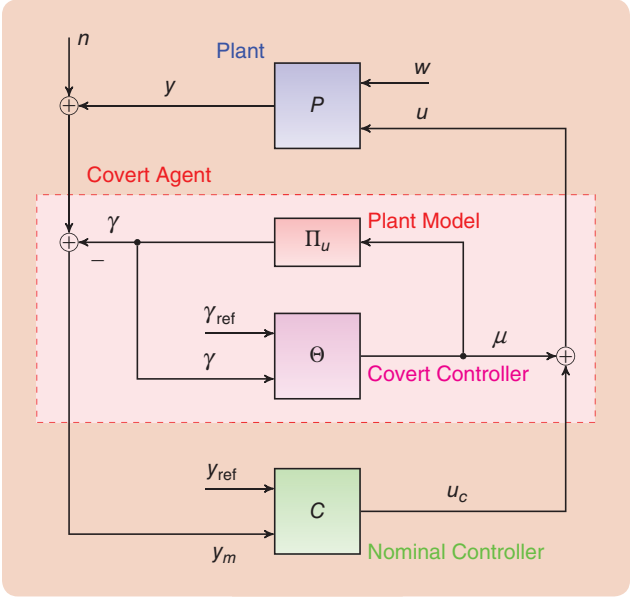


FIGURE 2 A covert agent structure for linear plants. The covert agent calculates its effect on the plant output measurements and subtracts those effects from the measured plant output. A feedback structure is used so that the covert agent's objectives can be specified with respect to the plant outputs. Any plant or control action constraints that must be respected can be taken into consideration in the design of the covert agent's feedback controller Θ.

The following results do not require the nominal controller to be linear, but linearity is assumed so that transfer functions may be written compactly for comparison purposes.

Combining (1)–(3) gives, in the nominal case, the closed-loop response of the system

$$y = SP_u C_{\text{ref}} y_{\text{ref}} + SP_w w + Tn,$$

and the nominal measurement seen by the nominal controller

$$y_m = SP_u C_{\text{ref}} y_{\text{ref}} + SP_w w + Sn, \tag{4}$$

where

$$T = (I - P_u C_y)^{-1} P_u C_y, \text{ and } S = (I - P_u C_y)^{-1}.$$

The nominal controller is assumed to be designed to satisfy stability and performance requirements for the reference y_{ref}, the exogenous disturbance w, and the noise n.

Covert Agent Structure

The misappropriation strategy described here is effectively a man-in-the-middle attack. The covert agent is assumed to have the resources to read and add to both the control actuation commands and the output measurements. In practice, this could also be accomplished by augmenting the physical actuators or modifying the sensors. Examples of such modifications include installing a controlled-flow bypass around a sluice gate in an irrigation system and connecting a controlled voltage source between a voltage measuring device and its intended connection point in an electrical network. Another potential mode of attack would involve corrupting the PLCs used by the nominal controller to implement the control and sensing operations. This was the implementation strategy used in the Stuxnet attack [1].

Figure 2 illustrates a structure for the covert agent and indicates how it is connected within the communication network. The two major components are a model of the plant's actuation to output response Π_u and a covert controller Θ. The parameterization of the covert agent, in terms of a feedback system, leads to a characterization of the extent to which the covert action is detectable, in terms of the design of the $\Pi_u - \Theta$ feedback loop.

The covert misappropriation of the plant is performed by augmenting the commanded actuation with the covert controller command μ, making the actual plant actuation

$$u = u_c + \mu. \tag{5}$$

The communicated output signal, including the sensor noise n, is modified by subtracting the covert agent's signal γ, giving the measured output

$$y_m = y + n - \gamma. \tag{6}$$

The covert agent generates the signals μ and γ via the feedback loop

$$\gamma = \Pi_u \mu, \tag{7}$$
$$\mu = \Theta_\gamma \gamma + \Theta_{\text{ref}} \gamma_{\text{ref}}. \tag{8}$$

This feedback loop is driven by the γ_{ref} input giving

$$\mu = (I - \Theta_\gamma \Pi_u)^{-1} \Theta_{\text{ref}} \gamma_{\text{ref}}, \tag{9}$$
$$\gamma = (I - \Theta_\gamma \Pi_u)^{-1} \Pi_u \Theta_{\text{ref}} \gamma_{\text{ref}}. \tag{10}$$

The covert controller is designed for reference tracking, with γ_{ref} as the reference input.

To see the consequences of the nested closed-loop systems in Figure 2, replace (3) by (5) and (2) by (6) and rearrange to get

$$y - y_m = (I - \Theta_\gamma \Pi_u)^{-1} \Theta_{\text{ref}} \Pi_u \gamma_{\text{ref}} - n \tag{11}$$

and

$$y_m = SP_u C_{\text{ref}} y_{\text{ref}} + SP_w w + Sn + S(P_u - \Pi_u)\mu. \tag{12}$$

Note that in (11), the relative offset of the actual plant output y from that measured—and controlled—by the nominal controller y_m is the output of the covert agent's γ_{ref}-reference tracking controller. This gives the covert agent the ability to drive the actual plant output to a desired offset with respect to its nominal controlled value y_{ref}.

To examine the nominal controller's ability to detect the actions of the covert agent, the nominal controller's measurement y_m in the nominal case [given by (4)] is compared to the covert misappropriation strategy case [given by (12)]. The only difference between these two appears to the nominal controller as an output disturbance w_{covert}, given by

$$w_{\text{covert}} = S(P_u - \Pi_u)(I - \Theta_\gamma \Pi_u)^{-1} \Theta_{\text{ref}} \gamma_{\text{ref}}. \tag{13}$$

If the covert agent has perfect knowledge of the plant's input response, $\Pi_u = P_u$, then $w_{\text{covert}} = 0$ and the covert misappropriation is undetectable. This case was studied in [11] as a particular case of a slightly more general parameterization of the covert agent. It is important to note that the covert agent needs no knowledge of the nominal controller to execute an undetectable misappropriation strategy.

Specifying the covert agent's actions via the feedback structure in Figure 2 ensures that the covert controller's plant input signal μ is appropriate for the plant. Any feedback or actuation limitations imposed by the plant are taken into account in the design of the $\Pi_u - \Theta_\gamma$ feedback loop within the covert agent and will limit the range of γ_{ref} offset values that the covert controller can effectively command. These limitations make no difference to the extent to which the convert controller's actions can be detected.

It is more realistic to consider that the covert agent's knowledge of the plant is not perfect. In this case, define the covert agent's model error Δ via

$$\Pi_u + \Delta = P_u. \tag{14}$$

The size of w_{covert} is a significant consideration in determining whether or not the covert controller's actions will be detected. This is the product of four factors:

1) The nominal sensitivity function S. The better the performance of the nominal control system, the harder it will be to detect a covert action. From the covert agent's point of view, band-limiting the frequency content of γ_{ref} to those frequencies where the network control system operates well will make the covert actions harder to detect.
2) The size of the covert agent's model error Δ. The higher the quality of the covert agent's knowledge of the plant, the harder it will be to detect covert actions.
3) The covert agent's reference to actuation transfer function $(I - \Theta_\gamma \Pi_u)^{-1} \Theta_{\text{ref}}$. This is a function of the design of the covert agent and can be used to further hide the covert action. For example, by designing the bandwidth of $(I - \Theta_\gamma \Pi_u)^{-1} \Theta_{\text{ref}}$ to be lower than that of T the frequency components of μ will be in the range where S is small, reducing the size of w_{covert}.
4) The size of the covert offset command γ_{ref}.

Even if the covert agent's knowledge of the plant is not perfect, the nominal controller still sees, and responds to, the actual measurement noise and the actual plant disturbances. Furthermore, the dynamics of the controlled plant appear unchanged from the nominal case. The effect on the measured plant output y_m of any nominal controller control signal u_c is the same whether or not the covert controller is operating. These features hinder the nominal controller's ability to detect covert actions through probing signals, such as watermarks, or signal analysis, such as noise or disturbance statistics characterization.

A LINEAR FLOW CANAL CONTROL EXAMPLE

Nominal Model and Operation

To illustrate the action of the covert agent with an incorrect plant model, an irrigation canal example, originally described in [12], is studied. The geographical separation in this application explains the need for a networked control system. The security of similar applications has been studied in [4] and [5]. The irrigation system is illustrated in Figure 3. A reservoir at a fixed height feeds a flow canal through a controlled sluice gate. The outlet flow of the reservoir is proportional to the gate height u_1. The water flows through a narrow sloping canal to a second sluice gate with controlled height u_2 and from there into a second canal. The second canal ends in a spillway. The water heights at the ends of each canal are the measured variables and the outputs of interest in the control problem.

This system can be modeled by two partial differential equations, known as the Saint-Venant equations. The simplified model used here can be found in [12]

$$y = \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-t_2 s} \end{bmatrix} \begin{bmatrix} \dfrac{4.87}{1800s+1} & \dfrac{-4.35}{2100s+1} \\ \dfrac{1.20}{1900s+1} & \dfrac{1.40}{1500s+1} \end{bmatrix} \begin{bmatrix} e^{-t_1 s} & 0 \\ 0 & 1 \end{bmatrix} u,$$

where the delays are $t_1 = 7$ min and $t_2 = 15$ min.

The nominal controller uses the two sluice gate actuators to control the end heights of each canal. A robust MIMO Smith-predictor method [12] is used for the design. This controller has an integral term in each channel and is robust with respect to delays, which can include communication delays as well as those already present in the plant. The controller is implemented using an internal model control (IMC) approach [13]. Figure 4 shows the nominal response to a step reference in the h_1 channel. To make the comparisons clearer, noise has not been included in these simulations. Because the covert agent's actions do not depend on y, it is unaffected by measurement noise. From the nominal controller's point of view, measurement noise makes it harder to detect the apparent disturbances due to covert action under uncertainty. In this respect, this illustrates a best-case scenario for the nominal controller.

The nominal closed-loop response is well damped and shows zero steady-state tracking error in both channels. The cross-channel errors are small due to the decoupling design of the controller. The flow disturbance results in a height peak error of 0.024 in h_1 and 0.007 in h_2.

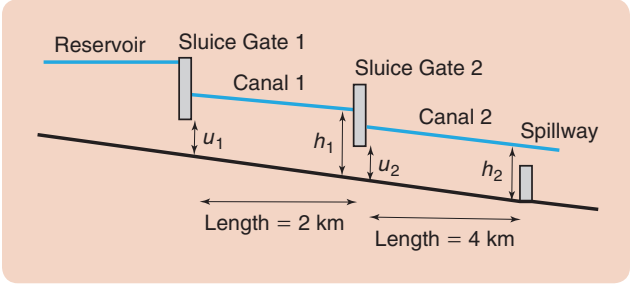


FIGURE 3 A schematic illustration of the canal control problem. The reservoir height is 3.5 m. Both sluice gates are constrained to a maximum opening of 0.9 m. The height of the spillway is 0.7 m. The canals are narrow (2.5 m wide) compared to their lengths.

Covert Agent Design

The design of the covert agent will be based on an incorrect plant model. The covert agent's plant model, Π_u in Figure 2, is taken to be

$$\Pi_u = \begin{bmatrix} 1 & 0 \\ 0 & e^{-\alpha_2 t_2 s} \end{bmatrix} \begin{bmatrix} \dfrac{\alpha_2 4.87}{\alpha_2 1800s+1} & \dfrac{-\alpha_1 4.35}{\alpha_1 2100s+1} \\ \dfrac{\alpha_2 1.20}{\alpha_1 1900s+1} & \dfrac{\alpha_1 1.40}{\alpha_2 1500s+1} \end{bmatrix} \begin{bmatrix} e^{-\alpha_1 t_1 s} & 0 \\ 0 & 1 \end{bmatrix},$$

with $\alpha_1 = 2.0$ and $\alpha_2 = 0.5$. The Π_u model errors are significant, up to a factor of two in the gains, time constants, and delays. This gives an additive error, Δ in (14), of size $\|\Delta\|_{\mathcal{H}_\infty} = 5.08$. For comparison $\|P_u\|_{\mathcal{H}_\infty} = 6.53$. An IMC structure is used for the design and implementation of Θ, and the internal plant model contains the same model errors.

The simulation scenario of Figure 4 is repeated and shown for the covertly misappropriated case in Figure 5. The height levels measured by the nominal controller are shown along with the actual height levels. The misappropriation is clear; the level of h_1 is 0.1 m lower than the reference intended by the nominal controller. Note that the disturbance in h_1 is not controlled by the covert agent and the nominal disturbance response is superimposed upon the trajectory of h_1 in the misappropriated case.

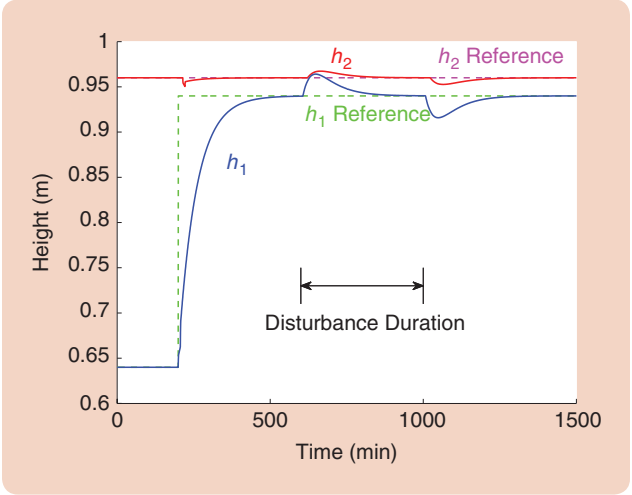


FIGURE 4 A nominal canal control system response. A reference step change of 0.1 m in h_1 is applied at 200 min. The h_2 reference is held constant throughout. From 600 min to 1000 min, an unmeasured flow disturbance (equivalent to raising the sluice gate u_1 by 0.01 m) is applied.

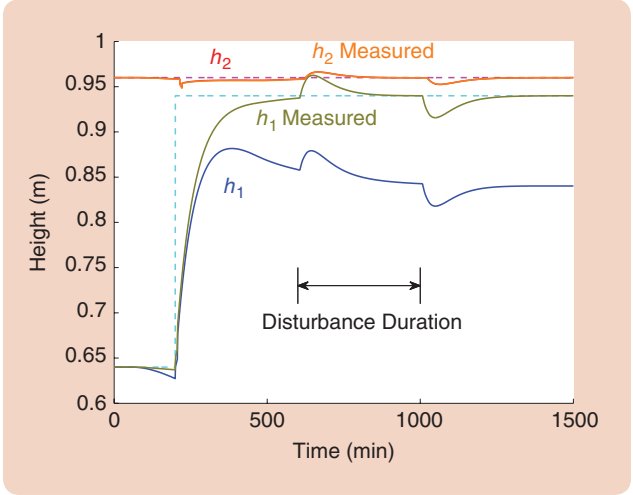


FIGURE 5 A misappropriated canal control system response. The reference and disturbances signals are identical to those in Figure 4. At 50 min, the covert agent's offset reference ξ_{ref} applies a ramp signal of 400 min duration setting the covert h_1 offset to -0.1 m.

The ability of a covert agent to remain undetected is key and requires more sophisticated resources and more plant knowledge than a brute-force disruptive attack.

The effect of the covert misappropriation on the height output signals measured by the controller can be seen by considering the difference between the reference tracking errors in the nominal and misappropriated cases shown in Figure 6. The reference tracking errors can be calculated by the nominal controller and could be used as a part of a covert agent detection scheme. In the absence of noise n or disturbances w, the reference tracking error differences are equal to the apparent disturbance signal w_{covert} in (13). For the covert controller's ramp offset of -0.1 m, the discrepancies between the nominal and misappropriated responses have a peak value of 0.005 m, which is a factor of five smaller than the effect of the disturbance in the nominal case. This would be unlikely to be detected in the presence of noise, disturbances, and the nominal controller's uncertainty about the exact plant model. To illustrate the frequency dependence effects in (13), the difference in reference tracking errors is also shown for ξ_{ref} equal to a -0.1-m step function. In this case, the higher frequency content in the ξ_{ref} step is amplified by the nominal control loop's higher sensitivity at these frequencies. The resulting peak tracking error difference is 0.011 m.

Figure 6 also illustrates that the flow disturbance between 600 and 1000 min is similar (from the point of view of the nominal controller's measurements) in both the nominal and misappropriated cases. Another feature is that these error differences are effectively zero from 1000 min onward, even though the covert controller is maintaining a height offset of -0.1 m. This is due to the integral action of the nominal controller; it removes the steady-state offset due to the effective disturbance w_{covert} caused by the covert agent. Doing this requires the nominal controller to adjust its commanded outputs and this gives a potential opportunity for detection. The nominal equilibrium point (at 1500 min) is

$$h = \begin{bmatrix} 0.940 \\ 0.960 \end{bmatrix}$$

with a commanded input of

$$u_c = \begin{bmatrix} 0.135 \\ 0.470 \end{bmatrix}.$$

In the misappropriated case, the commanded input required to maintain the same apparent height levels is

$$u_c = \begin{bmatrix} 0.146 \\ 0.475 \end{bmatrix}.$$

This equilibrium change of approximately 1% of full scale is the nominal controller's best opportunity to detect the covert misappropriation. The simulation example presented here did not include noise. Because the covert agent's control actions do not depend on output signal measurements, noise affects only the nominal controller and further hinders any efforts at detecting covert misappropriation. In this example, the presence of noise, disturbances, and the nominal controller's own uncertainty about the plant's low frequency gain, it is highly likely that large height offsets commanded by the covert agent (even with significant plant uncertainty) will go undetected.

COVERT CONTROL STRUCTURE FOR NONLINEAR PLANTS

The covert agent design presented above relies on linearity of the plant to reduce the possibility of its actions being detected. The basic idea behind the formulation is that the covert agent is able to calculate its effect on the plant and subtract its effect from the signals measured by the nominal controller. This approach can be applied to nonlinear plants, and one possible covert agent structure for doing this is illustrated in Figure 7. Two models of the plant input response are used by the covert agent. One calculates the expected response from the nominal controller's actuation commands u_c, and the other calculates the output effect of

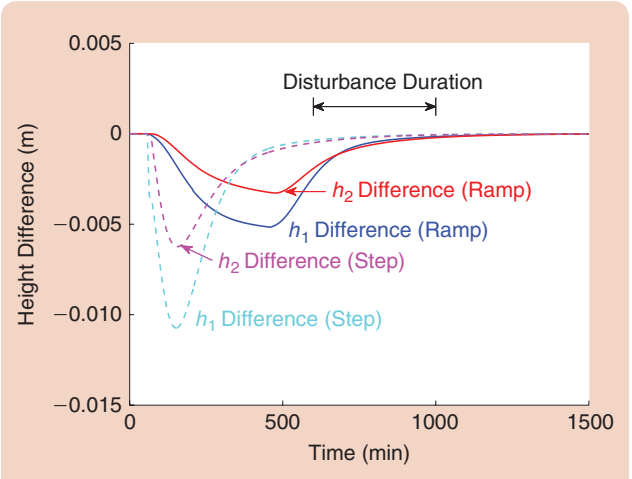


FIGURE 6 Reference tracking error differences. The difference in height reference tracking errors between the nominal and misappropriated cases is shown. Solid lines show the difference measurable by the nominal controller when the covert applies a 400 min ramp offset of -0.1 m. Dashed lines are the result of the covert agent applying a step offset of -0.1 m.

the augmented actuation command on the plant output. The difference between the two is

$$\gamma = \Pi_u(u_c + \mu) - \Pi_u(u_c), \tag{15}$$

and this is subtracted from the output measurements to be passed to nominal controller. The covert controller again calculates the covert actuation μ as a function of γ and γ_{ref}

$$\mu = \Theta(\gamma, \gamma_{\text{ref}}).$$

In the linear plant case, this covert agent structure is equivalent to the simpler structure illustrated in Figure 2. In the nonlinear case, several potential difficulties arise in the design of the covert agent. The first is that the covert action will move the plant to a different operating point, with presumably a different linearization. This may be detected by the nominal controller through probing signals or a careful analysis of the closed-loop disturbance response.

An additional problem arises from the fact that Π_u is a nonlinear model, and the accurate calculation of γ in (15) requires that both Π_u models are appropriately initialized. In practice this could be achieved by running an extended Kalman filter to provide a suitable initialization. Once the covert action is applied, the Kalman filter should be disconnected to avoid creating an additional feedback loop (by having γ depend on $y + n$), which will modify the noise and disturbance characteristics measured by the nominal controller.

The design and performance of the covert agent in the nonlinear case is problem dependent, although the approach taken for the linear case provides guidance on how this should be done. The linearization change caused by the covert agent driving the system to a different operating point is likely to be the factor that limits the degree to which the covert agent can remain undetected. The example in the next section illustrates that, even in the case of simple covert agent designs, detection will require detailed plant and disturbance knowledge within the nominal controller.

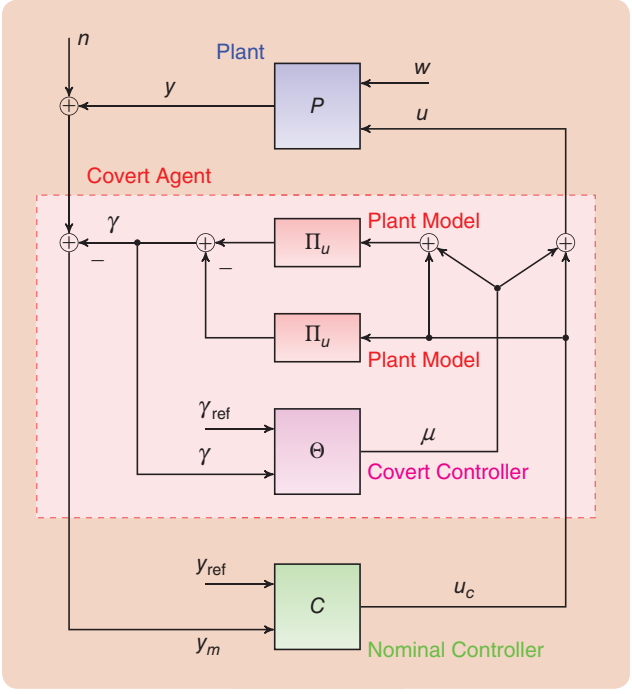


FIGURE 7 A covert controller structure for nonlinear plants. The covert controller calculates the difference in plant output measurements that are due to its manipulation of the plant input. The plant output difference is subtracted from the measured signals before they are passed to the nominal controller.

A NONLINEAR DC MOTOR EXAMPLE

The networked control of a separately excited dc motor is used as an example of the covert misappropriation strategy shown in Figure 7. The dominant nonlinearity comes from a product term in the state-space representation and results in an inverse relationship in the steady-state relationship between one of the inputs and one of the outputs. For simplicity, other nonlinear effects will be neglected.

DC Motor Model

The dc motor has two actuation inputs: the field voltage V_f and the armature voltage V_a. The measured outputs are the field and armature currents, I_f and I_a, respectively, and the motor speed ω. The field voltage V_f determines the field current I_f and the pole flux (scaled with respect to the number of turns) ϕ, via the differential equation

$$V_f = R_f I_f + \frac{d\phi}{dt}. \tag{16}$$

In general, the relationship between the field current and the pole flux has a hysteretic nonlinearity, but for simplicity operation is assumed to be in the linear region giving

$$\phi = L_f I_f, \tag{17}$$

where L_f is the field winding inductance. This results in a linear transfer function between the field voltage actuation V_f and the pole flux ϕ.

The differential equation for the armature current I_a is similar to that for I_f

$$V_a = R_a I_a + L_a \frac{dI_a}{dt} + V_{\text{EMF}} \tag{18}$$

but also includes the electromotive force V_{EMF}, which is determined by both the rotor speed and the pole flux

$$V_{\text{EMF}} = K_m \phi \omega, \tag{19}$$

where K_m is the motor constant. The torque generated by the motor is

$$\tau = K_m \phi I_a. \tag{20}$$

To complete the system model, the motor is assumed to drive a load described by the dynamic torque equation

$$\tau = J_m \frac{d\omega}{dt} + B_m \omega + \tau_L, \tag{21}$$

where τ_L is an unmeasured load disturbance torque. The parameters J_m and B_m are the motor inertia and viscous damping, respectively.

Using (16)–(21), a nonlinear state-space model of the dc motor can be derived

$$\frac{d}{dt} I_f = -\frac{R_f}{L_f} I_f + \frac{1}{L_f} V_f, \tag{22}$$

$$\frac{d}{dt} I_a = -\frac{R_a}{L_a} I_a - \frac{K_m L_f}{L_a} \omega I_a + \frac{1}{L_a} V_a, \tag{23}$$

$$\frac{d}{dt} \omega = -\frac{B_m}{J_m} \omega + \frac{K_m L_a L_f}{J_m} I_f I_a - \frac{1}{J_m} \tau_L. \tag{24}$$

Product nonlinearities occur in both (23) and (24). The effect of these nonlinearities is most easily seen in the system equilibria. The steady-state relationship between the armature voltage V_a, the load torque τ_L, the flux ϕ, and the motor speed ω is

$$\omega = \frac{-R_a}{K_m^2 \phi^2 + R_a B_m} \tau_L + \frac{K_m \phi}{K_m^2 \phi^2 + R_a B_m} V_a.$$

For moderately sized or larger motors, and under almost all practical operating conditions, $R_a B_m \ll K_m^2 \phi^2$, giving the steady-state rotor speed as

$$\omega \approx \frac{-R_a R_f^2}{K_m^2 L_f^2} \frac{\tau_L}{V_f^2} + \frac{L_f}{K_m R_f} \frac{V_a}{V_f}. \tag{25}$$

The inverse relationship between the field voltage V_f and the motor speed ω is evident. The effect of the field voltage on the load torque response is an inverse-squared relationship and, for the design given here, this will limit the covert controller's ability to remain hidden.

The motor and load parameters for this example are based on those in [14] and are given in Table 1. The model also includes input saturations of $\pm V_{\max}$ on both voltage inputs.

Design of the Nominal Controller

There are a variety of approaches for the design of separately excited dc motor controllers, and the techniques often involve exploiting the flux-weakening effect to allow operation at higher speeds—albeit with lower maximum load torque capabilities. See [15] and [14] for examples of such designs. For this example, a simpler two-loop strategy is used; reference inputs are used for both motor speed ω and the field current I_f. The motor would typically be operated by specifying a field current reference close to the rated maximum and then ramping up the speed reference to the desired operating point.

The field current loop is decoupled from the rest of the plant, and a simple feedback controller is used

$$V_f = \frac{50}{(s/25 + 1)} (I_{f\text{ref}} - I_f),$$

where $I_{f\text{ref}}$ is the reference field current. The design of the speed tracking control is formulated as a relatively standard $\mathcal{H}_\infty$ control problem with the measurements being the motor speed ω, the armature current I_a, and a speed reference ω_{ref}. The design was checked for robustness with respect to variations in the flux ϕ by a factor of two, which covers a wide range of typical operation conditions for this motor. Integral control was specified for the motor speed tracking.

Design of the Covert Controller

To illustrate that the design approach of the covert controller is independent of the design of the nominal controller, the covert controller uses a flux-weakening strategy to take control of the motor speed. The covert reference input γ_{ref} in Figure 7 is the relative motor speed offset. The covert controller's measurement is the difference between the plant measurement predicted from the covertly augmented actuation signal u and the plant measurement predicted from the commanded actuation signal u_c,

$$\gamma = \Pi_u u - \Pi_u u_c = \Pi_u (u_c + \mu) - \Pi_u u_c.$$

A cascade structure is used for Θ, with the relative speed error providing a field-current reference to a faster field-current inner loop. The covert actuation augmentation signal μ to be added to the commanded field voltage is

$$\mu = \frac{R_f}{(s/25 + 1)} \Theta_f (\Theta_\omega (\gamma_{\text{ref}} - \gamma_\omega) - \gamma_{I_f}),$$

where γ_ω and γ_{I_f} are the estimated motor speed and field current offsets, respectively. The covert controller gains used for the simulation below are

$$\Theta_f = 20 \text{ and } \Theta_\omega = -0.005.$$

TABLE 1 DC motor parameters.

Parameter	Value	Parameter	Value
Rated power	3730 W	Armature resistance, R_a	1.2 Ω
Rated speed	1750 r/min	Armature inductance, L_a	0.01 H
Rated torque	18 Nm	Field resistance, R_f	60 Ω
Rated armature current	16.74 A	Field inductance, L_f	60 H
Rated field current	4 A	Motor inertia, J_m	0.20 kgm^2
Maximum voltage, $V_{\max}$	240 V	Motor damping, B_m	0.011 kgm^2/s
Motor torque constant, K_m	30 Nm/A^2		

The choice of a flux-weakening strategy is not the best for a covert agent but it illustrates the extent to which linearization changes may reduce the covert agent's ability to remain undetected.

In practice, this attack could be implemented in a similar method to the Stuxnet attack [1], which would involve rewriting the code in the field-level PLC controllers. A similar approach could effectively interpose the covert agent between the low-level control algorithm and the interface to the dc drives.

Simulation Example

A simulation assuming exact plant models ($\Pi_u = P$) is used to illustrate the detectability of the covert agent's actions with respect to operating point changes. Sensor noise is modeled with a normal distribution that has a standard deviation that approximates using 14-b A/D converters on full-scale current and speed measurements of 50 A and 2500 r/min, respectively. The standard deviations are 0.003 A and 0.122 r/min.

For the nominal control scenario, the motor field current reference is set to its maximum value and one second later the speed reference is ramped up to 1312 r/min (75% of its rated value) over 1.5 s. The ramped speed reference serves to reduce the peak start-up current. The load torque is 1.0 Nm from the time of the motor starting until 12 s later when it ramps up (over 1 s) to 10 Nm. At 15 s it ramps back down (again over 1 s) to 1 Nm.

In the misappropriated case, the covert agent applies a reference offset beginning at 5 s and ramping up from 1312 r/min to 1850 r/min over 5 s. This offset is held for the duration of the scenario. Figure 8 compares closed-loop speed responses for the nominal and misappropriated cases. Because the covert controller's speed loop uses the field current, it is slower and has poorer tracking performance than the nominal speed control loop. However the covert agent has the ability to mask a large part of this effect from the nominal controller, as can been seen by the fact that the difference in speed measured by the nominal controller under the nominal and misappropriated scenarios is small and similar in character to that caused by a larger load torque.

The operation of the covert agent is more clearly seen in Figure 9, which illustrates the actuation voltages in both cases. Because the field-winding dynamics are linear and decoupled from the armature dynamics, the covert agent is able to completely mask its effect on this control loop. The field voltage commanded by the nominal controller is identical for the nominal and misappropriated cases. However, the actual field voltage applied to the motor is driven by the covert agent and drops to 165 V from its nominal value of 235 V.

The most prominent difference between the nominal and misappropriated scenarios can be seen in the motor armature currents, shown in Figure 10. As noted above, the linear field-current characteristics enable the covert agent to completely mask its actions with respect to field current. The field current is weakened from 3.92 A to 3.11 A without any change in the nominal controller's field current measurement. This holds even during the load torque disturbance.

The armature current shows potentially detectable response differences. During the covert speed-up of the motor (between 5 and 10 s) the armature current rises from 2.3 to 7.3 A. The value measured by the nominal controller rises to only 2.6 A, significantly less than its actual value. However, during the load torque disturbance, the covert agent is less successful in masking its actions.

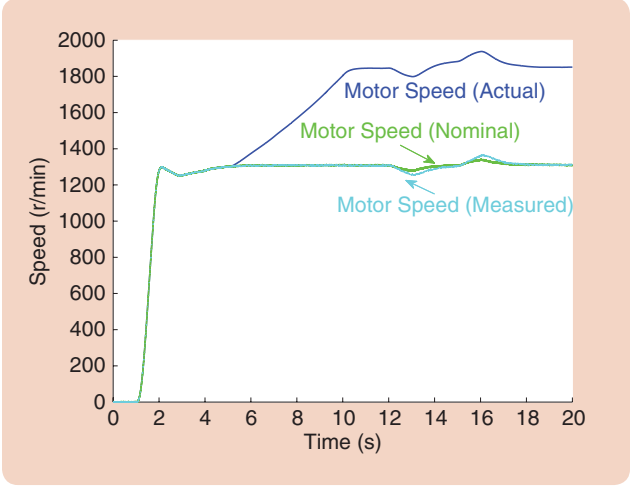


FIGURE 8 Motor speed comparison. From 5 to 10 s, the covert controller ramps up the motor speed. During the load disturbance the nominal motor speed deviation has a peak deviation of 30 r/min. Under the covert action, the nominal controller's speed measurement appears to have a deviation of 55 r/min. The actual deviation is 620 r/min.

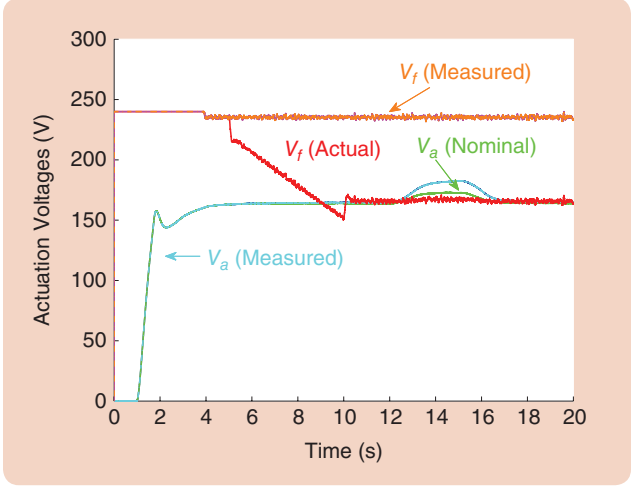


FIGURE 9 An actuation signal comparison. The covert controller action begins at 5 s when it ramps down the field voltage. From 10 s onward, the covert controller uses the field voltage to regulate the motor speed. The actual and measured armature voltages are the same since these are not manipulated by the covert controller.

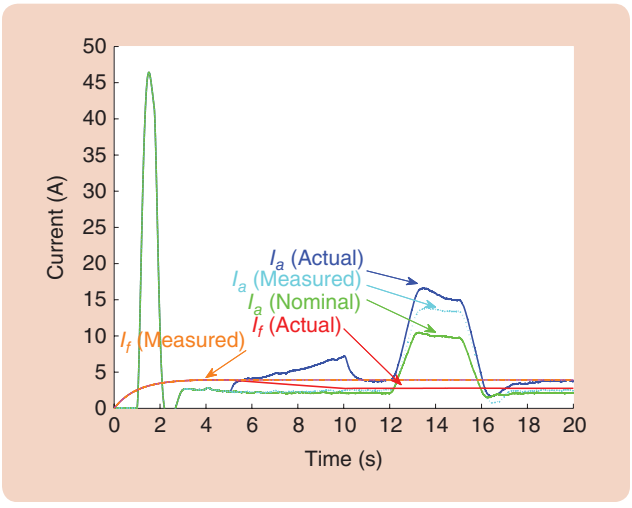


FIGURE 10 Motor current comparison. The armature current increases results from the nominal controller regulating the speed drop that would otherwise occur when the covert controller decreases the field current or the load torque slows the motor. Detecting the covert action relies on being able to distinguish these responses from those caused by normal disturbance rejection actions.

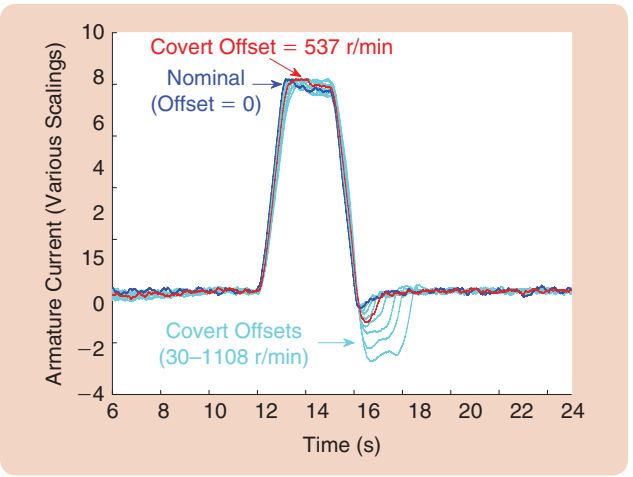


FIGURE 11 A scaled armature current load torque response comparison. The nominal I_a response is shown in blue. The I_a responses under covert action are shown in cyan. The covert misappropriation example shown in Figures 8–10 is given in red. All of the covert responses are shifted and scaled to the nominal response baseline and peak values. By comparing the norm of the difference, the nominal controller may be able to detect the presence of covert action.

The load torque disturbance does raise the possibility of discovery of the covert agent. An extensive simulation study is used to examine the ability of the nominal controller to distinguish between typical and abnormal load torque disturbance responses. For nonlinear plants, a covert controller changes the plant operating point and will likely also change the linearized dynamics. If the nominal controller has a good characterization of the typical disturbance responses at each operating point, then variations in the typical response can indicate potential covert action.

The detection approach considered is illustrated in Figure 11. The nominal controller operates the plant at a speed of 1312 r/min. The armature current load torque disturbance responses are examined for a series of covert speed offsets ranging up to 1108 r/min (2420 r/min in total). The nominal controller is assumed not to know the size of the load disturbance but has previously measured nominal load disturbances to use for characterization purposes. The detection method first shifts and then scales the observed I_a response so that it has the same base value and peak value as the nominal case. The shifted responses are shown in Figure 11 and show potentially detectable differences, particularly in the transient after I_a drops to its baseline level.

Figure 12 shows the norm of the difference between the scaled covert and nominal I_a response (as illustrated in Figure 11), normalized with respect to the norm of the nominal I_a response. The higher the nominal motor speed, the greater the scope of the covert agent for further increasing the motor speed with a low detection risk. At 1700 r/min, the covert controller can increase the speed by an additional 700 r/min with a less than 15% distortion to the load response. A detection approach like this assumes that the nominal controller has a good characterization of the time profile of the disturbances but may not know their size. This may be a strong assumption for practical systems, but in this example it is still difficult to detect the covert action.

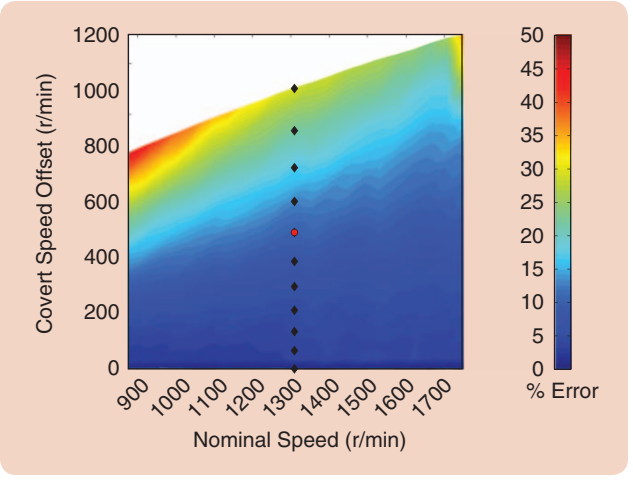


FIGURE 12 Detectable covert action as a function of operating point. The relative size of the scaled armature current load response (in Figure 11) is shown as a function of nominal speed and covert speed offset. Black diamond markers denote the operating points illustrated in Figure 11. The red circle denotes the operating point for Figures 8–10. The covert agent has a relatively large operating region in which it can significantly increase the motor speed with only a small relative discrepancy in the armature current load torque response.

DISCUSSION AND CONCLUSIONS

For linear plants, attempting to discover a covert agent by applying probing signals and checking the response, or by characterizing the noise will not work. The disturbance

characterization may appear to change, but the extent of this is largely determined by factors under the control of the covert agent. In particular, covert actions within the frequency range where the nominal control system has low sensitivity will be hard to detect. The better the covert agent's model of the plant, the easier it is for the covert agent to remain undetected.

In the nonlinear case, the covert agent has changed the plant's operating point, and this will potentially change the linearized dynamics. The degree to which this can be detected by probing signals depends on the extent of the linearization differences between the nominal and modified operating points. As illustrated in the dc motor simulation example, detection may require detailed knowledge of the disturbance characteristics. Even in this case, the covert agent may have significant scope for misappropriating the system.

The main point of these examples is to illustrate that a resourceful covert agent can easily hide its actions from a nominal controller. The more knowledge that the covert agent has about the plant and the more linear the plant, the harder it will be to detect the misappropriation of the control system. This makes it clear that the security of networked control systems depends on secure communication. Secure encryption of both the actuation and sensing signals is essential in this case. The physical security of the actuators and sensors is also critical. In some applications, for example, irrigation canal systems, covert misappropriation may be achieved by adding or modifying actuators and sensors in the field.

Covert attacks of the form given here rely on the covert agent having access to all of the actuation and sensing signals. For a small-scale covert misappropriation, this may be feasible, but for a large-scale problem, the resources required grow with the number of actuators and sensors. In grid control problems, for example, measuring and modifying every signal is unlikely to be feasible. For a covert agent with limited resources, the choice of which actuator and sensor signals to modify is an interesting topic and is initially addressed in [7] and [8]. From the point of view of the networked control system operator, these are the signals that should have the highest priority for being secured.

ACKNOWLEDGMENTS

The author would like to thank Bruno Sinópoli (CMU) and Henrik Sandberg (KTH, Stockholm) for helpful discussions. Thanks are also due to Ricardo Sánchez-Peña (Inst. Tecnológico, Buenos Aires) for providing the simulation code for the canal example.

AUTHOR INFORMATION

Roy S. Smith (rsmith@control.ee.ethz.ch) is a professor of electrical engineering at the Swiss Federal Institute of Technology (ETH), Zürich. Prior to joining ETH in 2011, he was on the faculty of the University of California, Santa Barbara, from 1990 to 2010. His Ph.D. is from the California Institute of Technology (1990) and his undergraduate degree is from the University of Canterbury (1980) in his native New Zealand. He has been a long-time consultant to the NASA Jet Propulsion Laboratory and has industrial experience in automotive control and power system design. His research interests are mostly focused on the modeling, identification, and control of uncertain systems. Particular control application domains of interest include chemical processes, flexible structure vibration, spacecraft and vehicle formations, semiconductor fabrication facilities, automotive engines, Mars aeromaneuvering entry design, energy management in buildings, and thermoacoustic machines. He is a Fellow of the IEEE, an associate fellow of the AIAA, and a member of SIAM, AACZ, and NZAC. He can be contacted at the Automatic Control Laboratory, ETH, Physikstrasse 3, 8092 Zürich, Switzerland.

REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien. (2010, Feb.). W32.Stuxnet dossier. Symantec Security Response, Tech. Rep. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[2] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Contr.*, vol. 58, no. 11, pp. 2715–2729, 2013.

[3] V. Igure, S. Laughter, and R. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, 2006.

[4] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, 2013.

[5] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1679–1693, 2013.

[6] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, 2013.

[7] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. IEEE Conf. Decision Control*, 2010, pp. 5991–5998.

[8] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Systems, Cyberphysical Systems*, Mar. 2010, pp. 1–6.

[9] K. C. Sou, H. Sandberg, and K. H. Johansson, "Data attack isolation in power networks using secure voltage magnitude measurements," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 14–28, 2014.

[10] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," arXiv: 1212.0226, Dec. 2012.

[11] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," in *Proc. Int. Federation Automatic Control World Congr.*, Aug. 2011, pp. 90–95.

[12] R. Sánchez-Peña, Y. Bolea, and V. Puig, "MIMO Smith predictor: Global and structured robust performance analysis," *J. Process Control*, vol. 19, no. 1, pp. 163–177, 2009.

[13] M. Morari and E. Zafiriou, *Robust Process Control*. Englewood Cliffs, NJ: Prentice-Hall, 1989.

[14] J. Zhou, Y. Wang, and R. Zhou, "Global speed control of separately excited DC motor," in *Proc. IEEE Power Engineering Society Winter Meeting*, 2001, vol. 3, pp. 1425–1430.

[15] S. Bolognani, A. Faggion, and L. Sgarbossa, "Design of a flux weakening control scheme for DC motor drives featuring full voltage operation," in *Proc. 43rd Int. Universities Power Engineering Conf.*, 2008, pp. 1–5.