Stealthy Deception Attacks on Water SCADA Systems

Saurabh Amin
Department of CEE
UC Berkeley, CA, USA
amins@berkeley.edu

Xavier Litrico
Cemagref, UMR G-EAU
Montpellier, France
xavier.litrico@cemagref.fr

S. Shankar Sastry
Department of EECS
UC Berkeley, CA, USA
sastry@coe.berkeley.edu

Alexandre M. Bayen
Department of CEE
UC Berkeley, CA, USA
bayen@berkeley.edu

ABSTRACT

This article investigates the vulnerabilities of Supervisory Control and Data Acquisition (SCADA) systems which monitor and control the modern day irrigation canal systems. This type of monitoring and control infrastructure is also common for many other water distribution systems. We present a linearized shallow water partial differential equation (PDE) system that can model water flow in a network of canal pools which are equipped with lateral offtakes for water withdrawal and are connected by automated gates. The knowledge of the system dynamics enables us to develop a deception attack scheme based on switching the PDE parameters and proportional (P) boundary control actions, to withdraw water from the pools through offtakes. We briefly discuss the limits on detectability of such attacks. We use a known formulation based on low frequency approximation of the PDE model and an associated proportional integral (PI) controller, to create a stealthy deception scheme capable of compromising the performance of the closed-loop system. We test the proposed attack scheme in simulation, using a shallow water solver; and show that the attack is indeed realizable in practice by implementing it on a physical canal in Southern France: the Gignac canal. A successful field experiment shows that the attack scheme enables us to steal water stealthily from the canal until the end of the attack.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*physical security, unauthorized access*; J.2 [**Physical Sciences and Engineering**]: Earth and atmospheric sciences

General Terms

Security

HSCC'10, April 12–15, 2010, Stockholm, Sweden.

1. INTRODUCTION

Numerous parts of the world are now using automation methods for management of their water distribution systems. For example, modern day irrigation systems are monitored and controlled by Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems enable the management agencies to remotely *monitor* water levels and velocities at desired locations as well as *control* the water flow through automated hydraulic structures. Based on the information gathered by level and velocity sensors, the control actions are generated by the SCADA system. Operators can also respond to *faults* by taking the necessary maintenance actions. The architecture of SCADA systems for irrigation canal networks is similar to that of many physical infrastructure systems such as waste-water treatment plants, oil and gas distribution, and process control systems.

SCADA systems are often commercially sold and deployed by information technology (IT) companies which use commodity solutions such as off-the-shelf operating systems, embedded devices and networking technology. Increasingly, these systems are being made accessible to remote users via corporate networks and the Internet. Even if these systems were designed to be closed, connectivity through uncontrolled connections can occur (e.g., via mobile devices). Wireless sensor and actuator networks are now allowing the managing agencies to monitor a larger number of events and operations. Thus, it can be concluded that SCADA systems inherit many of known IT vulnerabilities and threats. Many of these vulnerabilities now form a part of public-domain knowledge. Indeed, with the increasing complexity of monitoring and control systems, cyber-attacks are now becoming an attractive choice for the attacker; they are cheaper, less risky for the attacker, and are easier to execute.

1.1 The Gignac SCADA system

The Gignac irrigation canal network is located in South France and irrigates about 2800 hectares of agricultural land. The canal network can be used as an experimental testbed for research in hydrodynamic modeling and automatic control for canal network management. The canal network is equipped with level and velocity sensors at different sites to collect measurement data, and motorized gates with local slave controllers to control the flow of water. The canal is monitored and controlled by the SCADA system which comprises of a centralized base station communicating with the field devices through radio and telephone communication [1].

The functionalities of the Gignac SCADA system include: 1) monitoring of the hydraulic state of the canal as well as providing alarm status indicating malfunctioning resulting from faults, 2) changing parameters of local slave controllers that are programmed in the remote terminal units (RTUs), 3) Activating local slave controllers, sending manual gate movements, 4) Modifying operational objectives in terms of discharges or water levels. The full set of functionalities is available to the canal manager who can authorize one or more functionalities to other users. In order to develop and implement automatic control methods ranging from simple *proportional (P)* and *proportional integral (PI)* controllers to more advanced controllers on the canal, the canal management team has developed a software interface between the SCADA system and the SIC software [14]. SIC is a hydrodynamic simulation software that can test the controllers in simulation before implementing them on the real canal.

Recently, several attacks have been reported on the Gignac canal. For example, the solar panels that power radio communication systems used for data transmission from sensors to the base station were stolen. This resulted in loss of critical control functionalities. In a second attack, miscreants damaged the monitoring bridge on which a local gate controller was supported. This resulted in malfunctioning of gate controller. Finally, farmers who use the canal water for irrigation have made repeated attempts to steal water from the canal by tampering water offtakes and installing additional pumps to withdraw water. This threat remains a challenge for the management agency. Although these attacks were primarily physical, they directly affected the functioning of the SCADA system. In addition, several cyber-attacks on other water SCADA systems have been reported, for e.g., the Tehama colusa canal incident, Maroochy water breach incident, and Harrisburg water filtering plant incident.

1.2 Stealthy deception attacks

An adversary's motivation to attack a water SCADA system may be financial, malicious or even anti-social. An adversarial user wanting financial gains may want to steal the water without having to pay the charge for its use. Also, the adversary may steal the field devices and the communication system equipment to sell them for profit. An insider who is disgruntled with the water SCADA managing agency or a user who wants to gain advantage over other users are examples of adversaries with malicious intent. Finally, the adversary may be a miscreant who is just interested in causing any harm to the water distribution system.

In this article, we will consider deception attacks on sensors and controllers. During a deception attack, the adversary sends false information from (one or more) sensors or controllers. The false information can include: an incorrect measurement, the incorrect time when the measurement was observed, or the incorrect sender id. The adversary can launch these attacks by obtaining the secret keys used by the devices, or by compromising some sensors or controllers.

1.3 Focus of the article

During the past decade, several automatic control methods were developed and implemented into SCADA systems for regulatory control of canal networks [13]. These SCADA systems use sensor measurements to compute control actions based on a given hydrodynamic model and set-points provided by the canal supervisor (who decides the supervisory control actions). The hydrodynamic models range from simple algebraic equations to more complex *one-dimensional shallow water equations*. Canal control methods range from frequency-domain based (robust) PI controllers to more sophisticated methods such as $\mathcal{H}_\infty$, ℓ_1, linear quadratic regulator (LQG), and model predictive control (MPC).

Despite significant developments in the automatic control methods for canal systems with desired performance guarantees and robustness margins, we have at best little understanding of the resilience or defenses of SCADA systems under malicious attacks [11]. The methods for detection and diagnosis of random component failures are often not sufficient to deal with actions of an active adversary. Unfortunately, management agencies often *assume that insiders are trustworthy*, and only worry about outsider attacks.

In contrast, IT security solutions traditionally deal with prevention mechanisms such as authentication, access control, software security; detection mechanisms such as intrusion detection and malware filtering as well as resilient architectures such as separation of duty [9]. However, the computer security community has not analyzed adversarial actions that can compromise sensor and control data to affect the intended goal of automatic control methods.

In view of the aforementioned discussion, the aim of the present article is to characterize the effect of adversarial actions on the sensor and control data on the performance of the canal system. In particular, we aim to

a) Investigate the *stealthy deception attacks* on sensor and control data that can disrupt the intended purpose of commonly used P and PI controllers by increasing water loss and decreasing operational efficiency.

b) Characterize the difficulty in the *detection of attacks* due to slow and distributed nature of the system.

c) Illustrate the effect of deception attacks on SCADA performance by conducting a *field operational test* on a physical canal controlled by PI controllers.

This article is organized as follows: Section 2 discusses PDE models for a cascade of canal pools that is typical for a canal network. The adversary's actions are modeled by switching hyperbolic systems and an analysis on stability and performance of resulting a proportional control scheme is presented in Section 3. Section 4 discusses PI control design for a low frequency approximation of the PDE model and forms the basis of our experiments. Results from deception attacks conducted in simulation and in field operational experiment are presented in Section 5. Finally, we discuss the salient point of our analysis in Section 6.

2. SCADA REGULATORY CONTROL

2.1 Model of cascade canal system

We consider an irrigation canal system represented as a cascade of m individual canal pools as shown in Figure 1. Each canal pool is represented by a portion of canal in between two automated sluice gates. We will assume that each pool is prismatic, with a rectangular cross-section of constant width T in (m), length X in (m) and bed slope S_b in (m/m). For pool i, we denote $U_{i-1}(t)$ and $U_i(t)$ the opening of the upstream and downstream sluice gates in (m) respectively at time t.

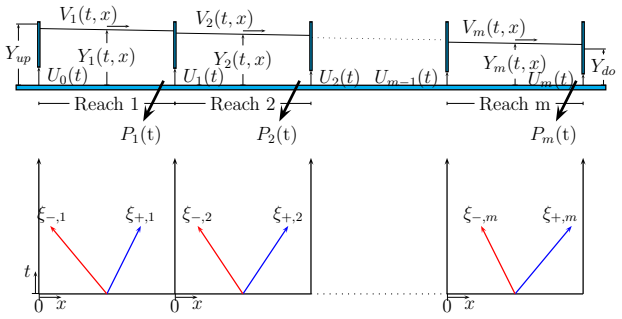

Figure 1: (a) Cascade of canals operated by underflow sluice gates. (b) Characteristic variables for each reach.

2.1.1 Networked Shallow Water Equations

The unsteady flow dynamics of each canal pool are classically modeled with the one-dimensional shallow water equations (SWE) [3]. The SWE are nonlinear hyperbolic partial differential equations describing evolution of the average cross-sectional velocity $V_i(x,t)$ in (m/s) and the water depth $Y_i(x,t)$ in (m) as a function of space variable $x \in (0,X)$ and time variable $t \in \mathbb{R}_+$. The SWE for pool i is stated as

$$\frac{\partial}{\partial t}\begin{pmatrix} Y_i \\ V_i \end{pmatrix} + F(Y_i,V_i)\frac{\partial}{\partial x}\begin{pmatrix} Y_i \\ V_i \end{pmatrix} = H(Y_i,V_i,P_i) \qquad (1)$$

for $(x,t) \in (0,X)\times\mathbb{R}_+$ with

$$F(Y_i,V_i) = \begin{pmatrix} V_i & Y_i \\ g & V_i \end{pmatrix}, \quad H(Y_i,V_i,P_i) = \begin{pmatrix} -P_i/T \\ g(S_b - S_{fi}) \end{pmatrix}$$

where g is the gravitational acceleration (m/s^2), $P_i(x,t)$ is the distributed lateral outflow per unit length of pool i in (m^2/s) ($P_i(x,t) < 0$ for inflow at (x,t)), and S_{fi} the friction slope for pool i in (m/m). The friction slope is given by

$$S_{fi} = \frac{V_i^2\eta^2(T+2Y_i)^{\frac{4}{3}}}{(TY_i)^{\frac{4}{3}}},$$

where η is the Manning's roughness coefficient (sm$^{-1/3}$). We will henceforth assume that flow in the canal pools is subcritical, that is, $V_i^2 < gY_i$. For notational convenience, we will denote $F(Y_i,V_i)$ as F_i and $H(Y_i,V_i,P_i)$ as H_i.

We have measurements of water levels Y at the upstream and downstream of each canal pool, i.e. $Y_i(0,t)$ and $Y_i(X,t)$. The control actions are imposed by actuators that can change the gate openings $U_{i-1}(t)$ and $U_i(t)$. The discharge relationships for the upstream and downstream sluice gates are given by

$$V_1(0,t)Y_1(0,t) = U_0(t)\sqrt{Y_{\text{up}} - Y_1(0,t)}, \qquad (2)$$

$$V_m(X,t)Y_m(X,t) = U_m(t)\sqrt{Y_m(X,t) - Y_{\text{do}}}, \qquad (3)$$

where the water levels Y_{up} and Y_{do} are assumed to be constant. For the intermediate gates $i = 1,\ldots,m-1$,

$$V_i(X,t)Y_i(X,t) = U_i(t)\sqrt{Y_i(X,t) - Y_{i+1}(0,t)}, \qquad (4)$$

$$V_i(X,t)Y_i(X,t) = V_{i+1}(0,t)Y_{i+1}(0,t), \qquad (5)$$

where the second equation results from flow conservation at each gate. Equations (2)–(5) specify the $2m$ boundary conditions for (1). The flow in (m^3/s) at any cross-section is defined as $Q_i = T\cdot Y_i\cdot V_i$; thus, equations (2)–(5) imply that we can impose flows $Q_i(0,t)$ and $Q_i(X,t)$ at the upstream and downstream of each pool i. The initial conditions are given by

$$Y_i(x,0) = Y_{0,i}(x) \text{ and } V_i(x,0) = V_{0,i}(x). \qquad (6)$$

2.1.2 Riemann Coordinates

System (1) is strictly hyperbolic if the matrix F_i has real and distinct eigenvalues given by $\lambda_{\pm,i} = V_i \pm \sqrt{gY_i}$. These eigenvalues are called *characteristic velocities* and for subcritical flow, they satisfy $\lambda_{-,i} < 0 < \lambda_{+,i}$. We now diagonalize the system (1) in the *Riemann coordinates*. Consider the following change of coordinates

$$\xi_i = \begin{pmatrix} \xi_{-,i} \\ \xi_{+,i} \end{pmatrix} := \begin{pmatrix} V_i - 2\sqrt{gY_i} \\ V_i + 2\sqrt{gY_i} \end{pmatrix} \qquad (7)$$

whose Jacobian matrix

$$D_i = \begin{pmatrix} -\sqrt{\frac{g}{Y_i}} & 1 \\ +\sqrt{\frac{g}{Y_i}} & 1 \end{pmatrix}$$

diagonalizes the matrix F_i in (1) such that

$$D_iF_iD_i^{-1} = \Lambda_i \quad \text{where} \quad \Lambda_i = \begin{pmatrix} \lambda_{-,i} & 0 \\ 0 & \lambda_{+,i} \end{pmatrix}. \qquad (8)$$

When necessary, we will use the notation $\Phi_i = 2\sqrt{gY_i}$. Thus, we can write $\xi_i = (V_i - \Phi_i, V_i + \Phi_i)^\top$. The change of coordinates can be inverted as

$$\begin{pmatrix} Y_i \\ V_i \end{pmatrix} = \begin{pmatrix} \frac{(\xi_{+,i}-\xi_{-,i})^2}{16g} \\ \frac{\xi_{-,i}+\xi_{+,i}}{2} \end{pmatrix}. \qquad (9)$$

Pre-multiplying equation (1) with D, noting (8), and using the definition (7) we obtain

$$\frac{\partial}{\partial t}\xi_i = D_i\frac{\partial}{\partial t}\begin{pmatrix} Y_i \\ V_i \end{pmatrix}, \quad \frac{\partial}{\partial x}\xi_i = D_i\frac{\partial}{\partial x}\begin{pmatrix} Y_i \\ V_i \end{pmatrix}$$

we obtain the SWE model in Riemann coordinates

$$\frac{\partial}{\partial t}\xi_i + \Lambda(\xi_i)\frac{\partial}{\partial x}\xi_i = E(\xi_i,P_i), \qquad (10)$$

where

$$\Lambda(\xi_i) = \begin{pmatrix} \frac{3\xi_{-,i}+\xi_{+,i}}{4} & 0 \\ 0 & \frac{\xi_{-,i}+3\xi_{+,i}}{4} \end{pmatrix},$$

and

$$E(\xi_i,P_i) = \frac{4gP_i}{T(\xi_{+,i}-\xi_{-,i})}\begin{pmatrix} +1 \\ -1 \end{pmatrix} + g(S_b - S_f(\xi_i))\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Here $\Lambda(\xi_i)$ and $S_f(\xi_i)$ respectively denote Λ_i and S_{fi} expressed in ξ_i coordinates.

2.1.3 Linearized Shallow Water Equations

Under constant gate openings $U_0(t) = \bar{U}_0$, $U_1(t) = \bar{U}_1$, $\ldots$, $U_m(t) = \bar{U}_m$ and constant withdrawal rates $P(t,x) = \bar{P}_i(x)$, the SWE (1) achieves a steady state. The discharge, water level, velocity, and friction slope of pool i corresponding to steady state are denoted by $\bar{Q}_i(x)$, $\bar{Y}_i(x)$, $\bar{V}_i(x)$ and $\bar{S}_{fi}(x)$. We will omit henceforth the dependence on x for the sake of conciseness. The steady state solution $(\bar{Y}_i,\bar{V}_i)$ satisfies

$$\frac{\partial}{\partial t}\begin{pmatrix} \bar{Y}_i \\ \bar{V}_i \end{pmatrix} = 0, \quad \frac{\partial}{\partial x}\begin{pmatrix} \bar{Y}_i \\ \bar{V}_i \end{pmatrix} = F^{-1}(\bar{Y}_i,\bar{V}_i)H(\bar{Y}_i,\bar{V}_i,\bar{P}_i),$$

and can be easily obtained by solving the ODEs

$$\frac{d\bar{Q}_i}{dx} = -\bar{P}_i$$
$$T\frac{d\bar{Y}_i}{dx} = \left(g\bar{Y}_i - \frac{\bar{Q}_i^2}{(T\bar{Y}_i)^2}\right)^{-1}\left(gT\bar{Y}_i(S_b - \bar{S}_{fi}) + \frac{\bar{Q}_i\bar{P}_i}{T\bar{Y}_i}\right),$$

and noting that $\bar{V}_i = (T\bar{Y}_i)^{-1}\bar{Q}_i$. The steady state solution in the Riemann coordinates $(\bar{\xi}_{-,i}, \bar{\xi}_{+,i})$ can now be obtained as $\bar{\xi}_{-,i} = (\bar{V}_i - 2\sqrt{g\bar{Y}_i})$ and $\bar{\xi}_{+,i} = (\bar{V}_i + 2\sqrt{g\bar{Y}_i})$. Indeed, following (10), $\bar{\xi}_i = (\bar{\xi}_{-,i}, \bar{\xi}_{+,i})^\top$ satisfies

$$\frac{\partial}{\partial t}\bar{\xi}_i = 0, \quad \frac{\partial}{\partial x}\bar{\xi}_i = \Lambda(\bar{\xi}_i)^{-1}E(\bar{\xi}_i, \bar{P}_i).$$

We now linearize (10) around the steady state $(\bar{\xi}_i, \bar{P}_i)$. For a given term $f(\xi_i, P)$ of (10), we use the approximation of Taylor's expansion:

$$f(\xi_i, P_i) \approx f(\bar{\xi}_i, \bar{P}_i) + \overline{\left(\frac{\partial f}{\partial \xi_{-,i}}\right)}\zeta_{-,i} + \overline{\left(\frac{\partial f}{\partial \xi_{+,i}}\right)}\zeta_{+,i} + \overline{\left(\frac{\partial f}{\partial P_i}\right)}p_i$$

where we define $\zeta_{-,i} = (\xi_{-,i} - \bar{\xi}_{-,i})$, $\zeta_{+,i} = (\xi_{+,i} - \bar{\xi}_{+,i})$ and $p_i = (P_i - \bar{P}_i)$; and $\overline{(\cdot)}$ indicates that all quantities are evaluated at steady state conditions. Let $\zeta_i := (\zeta_{-,i}, \zeta_{+,i})^\top$. Using (7), we can express ζ_i in terms of physical variables

$$\zeta_i = \begin{pmatrix} V_i - \bar{V}_i - 2(\sqrt{gY_i} - \sqrt{g\bar{Y}_i}) \\ V_i - \bar{V}_i + 2(\sqrt{gY_i} - \sqrt{g\bar{Y}_i}) \end{pmatrix} =: \begin{pmatrix} v_i - \varphi_i \\ v_i + \varphi_i \end{pmatrix},$$

with $v_i = V_i - \bar{V}_i$ and $\varphi_i = \Phi_i - \bar{\Phi}_i$.

Referring to equation (32) in the Appendix A, the linearized SWE around the steady state $(\bar{\xi}_i, \bar{P}_i)$

$$\frac{\partial}{\partial t}\zeta_i + \bar{\Lambda}_i(x)\frac{\partial}{\partial x}\zeta_i + \bar{B}_i(x)\zeta_i = \bar{C}_i(x)p_i, \tag{11}$$

where $\bar{\Lambda}_i(x)$, $\bar{B}_i(x)$, and $\bar{C}_i(x)$ are used to denote $\Lambda(\bar{\xi}_i)$, $B(\bar{\xi}_i, \bar{P}_i)$, and $C(\bar{\xi}_i)$ respectively.

For each canal pool, we impose the boundary control actions of the form

$$\zeta_{+,i}(0,t) = -g_{0,i}\zeta_{-,i}(0,t),\ \zeta_{-,i}(X,t) = -g_{X,i}\zeta_{+,i}(X,t), \tag{12}$$

or equivalently

$$\begin{aligned} V_i(0,t) &= \bar{V}_i(0) - \left(\frac{1-g_{0,i}}{1+g_{0,i}}\right)(\Phi_i(0,t) - \bar{\Phi}_i(0)) \\ V_i(X,t) &= \bar{V}_i(X) + \left(\frac{1-g_{X,i}}{1+g_{X,i}}\right)(\Phi_i(X,t) - \bar{\Phi}_i(X)), \end{aligned} \tag{13}$$

where $0 < g_{0,i}$ and $0 < g_{X,i}$.

The *change* in gate openings $u_i(t) := (U_i(t) - \bar{U}_i)$ can now be expressed as feedback boundary control actions in terms of the local gate openings using (13) and linearized gate equations; see the system of equations (36) in Appendix B. Note that the boundary control actions are of *proportional* (P) type and are *decentralized* in nature, i.e. they are locally computed using water level sensor measurements.

The initial data is specified as

$$\bar{\zeta}_i(x) = \begin{pmatrix} V_i(x,0) - \bar{V}_i(x) - (\Phi_i(x,0) - \bar{\Phi}_i(x)) \\ V_i(x,0) - \bar{V}_i(x) + (\Phi_i(x,0) - \bar{\Phi}_i(x)) \end{pmatrix}. \tag{14}$$

By defining

$$\zeta_- = (\zeta_{-,1}, \ldots, \zeta_{-,m})^\top, \quad \zeta_+ = (\zeta_{+,1}, \ldots, \zeta_{+,m})^\top,$$
$$\bar{\Lambda}_- = \mathrm{diag}(\bar{\lambda}_{-,1}, \ldots, \bar{\lambda}_{-,m}), \quad \bar{\Lambda}_+ = \mathrm{diag}(\bar{\lambda}_{+,1}, \ldots, \bar{\lambda}_{+,m}),$$
$$\zeta = \begin{pmatrix} \zeta_- \\ \zeta_+ \end{pmatrix}, \quad \bar{\Lambda}(x) = \begin{pmatrix} \bar{\Lambda}_- & 0 \\ 0 & \bar{\Lambda}_+ \end{pmatrix},$$

we can assemble the individual equations (11) for all canal pools to obtain the linearized SWE for the cascade of canals

$$\frac{\partial}{\partial t}\zeta + \bar{\Lambda}(x)\frac{\partial}{\partial x}\zeta + \bar{B}(x)\zeta = \bar{C}(x)p, \tag{15}$$

where $p = (p_1, \ldots, p_m)^\top$, and the matrices $\bar{B}(x)$ and $\bar{C}(x)$ are $2m \times 2m$ and $2m \times m$ dimensional matrices obtained by assembling $\bar{B}_i(x)$ and $\bar{C}_i(x)$ respectively.

Assembling (12) we obtain the boundary conditions

$$\zeta_+(0,t) = \Gamma_L\zeta_-(0,t), \quad \zeta_-(X,t) = \Gamma_R\zeta_+(X,t), \tag{16}$$

where we define

$$\Gamma_L = -\mathrm{diag}(g_{0,1}, \ldots, g_{0,m}), \quad \Gamma_R = -\mathrm{diag}(g_{X,1}, \ldots, g_{X,m}),$$

and assembling (14), we obtain the initial condition

$$\zeta(x,0) = \bar{\zeta}(x) \tag{17}$$

where $\bar{\zeta}(x) = (\bar{\zeta}_{-,1}(x), \ldots, \bar{\zeta}_{-,m}(x), \bar{\zeta}_{+,1}(x), \ldots, \bar{\zeta}_{+,m}(x))^\top$.

Equations (15)–(17) specify the hyperbolic initial boundary value problem (IBVP) and models the cascade of canals pools with offtakes.

3. ANALYSIS OF DECEPTION ATTACKS

3.1 Modeling attacks as switching PDE

We now extend the model (15)–(17) to include the actions of an adversary that influences the lateral water outflow through offtakes and also manipulates sensor data.

3.1.1 *Modeling water withdrawal of the attacker*

We assume that the canal pool i has J_i offtakes and that the $j-$th offtake of the $i-$th canal pool is present along length x, where $0 < \underline{x}_{i,j} \le x \le \overline{x}_{i,j} < X$. The lateral outflow along the length of the $i-$th canal pool can be expressed as

$$p_i(x,t) = \begin{cases} p_{i,j}(t) & x \in [\overline{x}_{i,j}, \underline{x}_{i,j}], \quad j = 1\ldots, J_i \\ 0 & \text{otherwise} \end{cases} \tag{18}$$

where $p_{i,j}(t)$ is the outflow per unit length of the $j-$th offtake of the $i-$th canal pool. We define the indicator $\mathcal{X}_{i,j}(x)$ for the $j-$th offtake of the $i-$th canal pool by

$$\mathcal{X}_{i,j}(x) = \begin{cases} 1 & \text{if } x \in [\overline{x}_{i,j}, \underline{x}_{i,j}] \\ 0 & \text{otherwise .} \end{cases} \tag{19}$$

Using this notation, we can express the total lateral withdrawal from all the J_i offtakes for $i-$th canal pool as

$$p_i(x,t) = \sum_{j=1}^{J_i} p_{i,j}(t)\mathcal{X}_{i,j}(x). \tag{20}$$

Defining the $\sum_{i=1}^m J_i-$dimensional vector as

$$\rho(t) = (p_{1,1}, \ldots, p_{1,J_1}, \ldots, p_{m,1}, \ldots, p_{m,J_m})^\top,$$

and assembling the offtakes for all canal pools we obtain

$$p(x,t) = \Xi(x)\rho(t)$$

where $\Xi(x)$ is a $m \times \sum_{i=1}^{m} J_i$ matrix function defined using (19). Plugging the expression of p in equation (15), we obtain

$$\frac{\partial}{\partial t}\zeta + \bar{\Lambda}(x)\frac{\partial}{\partial x}\zeta + \bar{B}(x)\zeta = \bar{C}(x)\Xi(x)\rho(t).$$

We now assume that the adversary can influence withdrawal of water through one or more of the J_i offtakes located along the length of each canal pool i. A reasonable model of water withdrawal through offtakes is to assume a piecewise-constant switching signal because water is withdrawn by discretely opening/closing the offtake gates. Thus, we assume that under the influence of the adversary, the offtake withdrawal vector $\rho(t)$ switches discretely among a set of modes $\mathcal{Q} = \{1, \ldots, \mathcal{N}\}$ according to a piecewise-constant switching signal $\sigma(\cdot) : \mathbb{R}_+ \to \mathcal{Q}$. Thus, following switching PDE models the offtake withdrawal under discrete open/close actions of the adversary

$$\frac{\partial}{\partial t}\zeta + \bar{\Lambda}(x)\frac{\partial}{\partial x}\zeta + \bar{B}(x)\zeta = \bar{\Xi}(x)\rho^{\sigma(t)}. \tag{21}$$

where $\bar{\Xi} := \bar{C}\Xi$.

3.1.2 Modeling sensor deception attacks

We now illustrate the model of a deception attack on sensor measurements which are water level measurements for upstream $Y_i(0,t)$ and downstream $Y_i(X,t)$ of each canal pool and the gate openings $U_i(t)$. Since we operate in linearized domain, this is equivalent to the deception attacks on $\varphi_i = 2\sqrt{g}(\sqrt{Y_i} - \sqrt{\bar{Y}_i})$ and $u_i = U_i - \bar{U}_i$. We simply refer to φ_i as the transformed water level and u_i as the gate opening.

For the ease of presentation, we will only explain the case of deception attacks on the transformed upstream water level $\varphi_1(0,t)$ and the gate opening $u_1(t)$ of the first canal pool and generalize to the case of attacks on other sensor measurements later. Using (12) and (33) in Appendix B, we can write

$$\begin{aligned}\zeta_{+,1}(0,t) &= -g_{0,1}(v_1(0,t) - \varphi_1(0,t)) \\ &= -g_{0,1}\left((k_{1,0}-1)\varphi_1(0,t) + k_{u_0}u_0(t)\right)\end{aligned}$$

Now suppose that the adversary conducts deception attacks on $\varphi_1(0,t)$ and $u_0(t)$; the values manipulated by the adversary are denoted $\tilde{\varphi}_1(0,t)$ and $\tilde{u}_0(t)$ respectively. Under attack, $\zeta_{+,1}$ becomes

$$\zeta_{+,1}(0,t) = -g_{0,1}\left((k_{1,0}-1)\tilde{\varphi}_1(0,t) + k_{u_0}\tilde{u}_0(t)\right).$$

We can now conclude that the effect of deception attack on sensor measurements is equivalent to changing boundary control parameter $g_{0,1}$ to $\tilde{g}_{0,1}$ where

$$\tilde{g}_{0,1} = g_{0,1}\frac{(k_{1,0}-1)\tilde{\varphi}_1(0,t) + k_{u_0}\tilde{u}_0(t)}{(k_{1,0}-1)\varphi_1(0,t) + k_{u_0}u_0(t)}.$$

The same argument can be extended to capture the effect of deception attacks on other sensor measurements; that is, the deception attacks of water level $\varphi_i(0,t)$ and $\varphi_i(X,t)$ and gate sensors $u_i(t)$ can be equivalently characterized by changing the boundary control parameters $g_{0,i}$ and $g_{X,i}$.

As for the case of water withdrawal through offtakes, we can now assume the adversary conducts deception attacks on sensor measurements according to a piecewise-constant signal $\sigma(t)$. We can now model the effect of deception attack on sensor measurements as boundary control actions that *switch* among a set of modes $\mathcal{Q} = \{1, \ldots, \mathcal{N}\}$ according to a piece

$$\zeta_+(0,t) = \Gamma_L^{\sigma(t)}\zeta_-(0,t), \quad \zeta_-(X,t) = \Gamma_R^{\sigma(t)}\zeta_+(X,t), \tag{22}$$

We conclude that the switching hyperbolic system (21), (17), (22) models the adversary's action on water withdrawal from offtakes and deception attack on sensor measurements. Thus, under the adversary's action, the water withdrawal rates ρ and the proportional control parameters Γ_L and Γ_R switching system are known to satisfy

$$(\rho, \Gamma_L, \Gamma_R) \in \{(\rho^j, \Gamma_L^j, \Gamma_R^j) : j \in \mathcal{Q}\}$$

at any time $t > 0$, where $\mathcal{Q} = \{1, \ldots, \mathcal{N}\}$ is a finite set of modes and, for all $j \in \mathcal{Q}$, $\rho^j, \Gamma_L^j, \Gamma_R^j$ are chosen by the adversary.

3.1.3 Stability under switching caused by adversary

We now characterize stability of the cascade canal pool under switching cause by adversary. Referring to [7], we note that given a non-zeno switching signal $\sigma(\cdot)$, the solution of the switching system (21), (17), (22) exists and is unique. In particular, under certain regularity assumptions on the matrix functions $\bar{\Lambda}(x)$, $\bar{B}(x)$, and $\bar{\Xi}(x)$, there exists a unique solution

$$\zeta(\cdot,t) \in L^\infty(\mathbb{R}_+; L^\infty((0,X); \mathbb{R}^{2m})).$$

The switching system is said to be *exponentially stable* (with respect to a norm $\|\cdot\|_\infty$) if there exist constants $c \geq 1$ and $\beta > 0$ such that the solution $\zeta(t,\cdot)$ satisfies

$$\|\zeta(t,\cdot)\|_\infty \leq c\exp(-\beta t)\|\zeta(0,\cdot)\|_\infty, \ t \geq 0. \tag{23}$$

We say that the switching system is *absolutely exponentially stable* (with respect to a norm $\|\cdot\|_\infty$) if (23) holds for all non-zeno $\sigma(\cdot)$ with constants $c \geq 1$ and $\beta > 0$ independently of $\sigma(\cdot)$.

Following the theory presented in [7], we can state the stability result under switching caused by adversary. In particular, if a spectral radius condition is jointly satisfied for the left and right boundary data and all pairs of modes $j, j' \in \mathcal{Q}$ then sufficiently small bounds on $\|\bar{B}(x)\|_\infty$ and $\|\bar{\Xi}(x)\rho^j\|_\infty$ exist such that the switching system is absolutely exponentially stable with respect to the norm $\|\cdot\|_\infty$. We define the spectral radius $\varrho(M)$ of a non-negative matrix $\mathcal{M}$ as the absolute value of the largest eigenvalue of $\mathcal{M}$.

THEOREM 1. *Suppose that for $j, j' \in \mathcal{Q}$ the following condition holds:*

$$\varrho\left(\begin{bmatrix} 0 & |\Gamma_R^{j'}| \\ |\Gamma_L^j| & 0 \end{bmatrix}\right) < 1. \tag{24}$$

Then there exists an $\epsilon_1 > 0$ and $\epsilon_2 > 0$ such that if $\|\bar{B}(s)\|_\infty < \epsilon_1$ and $\|\Xi(x)\rho^j\|_\infty < \epsilon_2$ for all $x \in [0,X]$ and $j \in \mathcal{Q}$, the switching system (21), (17), (22) is absolutely exponentially stable with respect to the norm $\|\cdot\|_\infty$.

PROOF. The result is obtained by deriving L_∞ bounds on the solution of the switching system based on method of characteristics and is a straightforward generalization of the result presented in [7]. □

Even though the conditions of Theorem 1 are only sufficient and not necessary, we note that the switching caused due to adversary's action can easily lead to instability. We refer the reader to a simple example in [8] of an unstable switching system resulting from switching between two exponentially stable subsystems. Next, we will qualitatively argue that even though the switching system resulting from the adversary's action is stable, detecting the attack just based on the boundary measurements may be an inherently difficult problem.

3.2 Limits on detectability of attacks

We now argue the difficulty in detection of attack by using the method of characteristics. For each mode $j \in \mathcal{Q}$, the PDE subsystems

$$\frac{\partial}{\partial t}\zeta^j + \bar{\Lambda}(x)\frac{\partial}{\partial x}\zeta^j + \bar{B}(x)\zeta^j = \bar{\Xi}(x)\rho^j \qquad (25)$$
$$\zeta_+^j(0,t) = \Gamma_L^j \zeta_-^j(0,t), \quad \zeta_-^j(X,t) = \Gamma_R^j \zeta_+^j(X,t)$$

can be transformed into an equivalent set of ODEs. In particular, for each i, where $i = 1, \ldots, 2m$, and each point (x^*, t^*), the ODE

$$\frac{d}{dt} z_i^j(t) = \lambda_i(z_i^j(t)), \quad z_i^j(t^*) = x^* \qquad (26)$$

has a unique solution, defined for all t. We say that $t \mapsto z_i^j(t; x^*, t^*)$ passing through (x^*, t^*) is the $i-$th *characteristic curve* for the j-th subsystem.

Equations (25) and (26) imply that ζ_i^j, $i = 1, \ldots, 2m$, satisfy

$$\frac{d}{dt}\zeta_i^j(t, z_i^j(t; x^*, t^*)) = \sum_{\vartheta=1}^{\Upsilon} \upsilon_{i\vartheta}(z_i^j(t; x^*, t^*))\rho_\vartheta^j$$
$$- \sum_{k=1}^{2m} b_{ik}(z_i^j(t; x^*, t^*))\zeta_k^j(t, z_i^j(t; x^*, t^*)) \qquad (27)$$

along almost every characteristic curve $z_i^j(t; x^*, t^*)$. Here $b_{ik}(\cdot)$ corresponds to the i-th row and k-th column of $\bar{B}(\cdot)$, $\upsilon_{i\vartheta}(\cdot)$ corresponds to the $i-$th row and $\vartheta-$th column of $\bar{\Xi}(\cdot)$, and $\Upsilon = \sum_{l=1}^{m} J_l$.

It is clear from (26) and (27) that at any change in the water withdrawal strategy via offtakes (switching from ρ^j to $\rho^{j'}$) will affect the solution ζ of the switching PDE; however, the slope of the characteristic paths do not change under offtake switching. As observed by [10], the change in transformed water level φ_i at the gate locations could be very small under the effect of changing offtake withdrawals. Secondly, the withdrawals from different offtakes may have very similar effect on the downstream water level and it might be necessary to measure water level at multiple points along the canal pools to distinguish between different offtake withdrawal strategies of the adversary. Lastly, even if the effect of offtake withdrawal is observed by water level sensors, the adversary can conduct deception attacks on these sensors. These qualitative arguments suggest that detecting change in offtake withdrawal strategy can be very difficult, especially under the influence of an adversary that can manipulate water level sensor readings.

4. CONTROL USING APPROX. MODEL

We now discuss the proportional integral (PI) controller based on a frequency domain approximation of the PDE system (15)–(17). For a link between characteristic curve approach introduced in the last section and the frequency domain approach, the reader is referred to [12]. The PI controllers are well-suited for *field implementation* and can be easily tuned by standard tuning methods such as the auto-tuned variation method [15]. We will use PI controller, so tuned, for the actual implementation of deception attack scenario on a physical canal pool of the Gignac canal system in the next section. The PI controller also achieves desired robustness margins based on a standard frequency domain approach [13]. From the adversary's point-of-view, this theory points toward synthesis of attack vectors based on only an approximate knowledge of canal hydrodynamics instead of full PDE models.

4.1 Integrator-delay model for canal cascade

For the case in which the effect of water withdrawals is lumped at the downstream end of each canal pool, the system (15)–(17), can also be analyzed in the frequency domain using the Laplace transform. Using the upstream and downstream discharges as control input variables, and the downstream water level as controlled variable, the input-output relationship for each canal pool i is given by:

$$y_i(s) = G_i(s)\mu_i(s) + \tilde{G}_i(s)[\mu_{i+1}(s) + p_i(s)] \qquad (28)$$

where $G_i(s)$ and $\tilde{G}_i(s)$ are infinite dimensional transfer functions and where s is the complex Laplace variable [1]. Here, y_i denotes the downstream water level, and upstream, p_i denotes the perturbation, and downstream discharge variables are denoted as μ_i and μ_{i+1} respectively. The regulatory control aim is to regulate y_i to a set-point r_i. This representation assumes that the problem of converting the discharge at the boundary of each pool μ_i into actual gate openings u_i can be handled locally by a slave controller on each gate, and the effect of all the offtakes along the canal pool can be lumped into a single perturbation p_i acting near the downstream end of the pool. For low frequencies, these transfer functions can be approximated by an Integrator Delay (ID) model (see [13], Chap. 4, Sec. 4.1 and 4.2, and also [4]). The ID model is classically used to design PI controllers [6]. The transfer functions for the ID model are given by

$$G_i(s) = \frac{\exp(-\tau_i s)}{A_i s}, \quad \tilde{G}_i(s) = -\frac{1}{A_i s} \qquad (29)$$

where τ_i is the propagation delay of the $i-$th canal pool (in s) and A_i is the backwater area (in m^2). By assembling (28) for individual pools, the multi-pool representation of canal can be obtained as

$$y = G\mu + \tilde{G}p.$$

4.2 Local upstream PI control of single pool

Frequency domain PI controllers based on ID model perform satisfactorily in most practical settings [13]. Two classical canal control policies are commonly used: local upstream control and distant downstream control. Local upstream control of a canal pool consists of controlling the downstream water level y_i using the downstream discharge μ_2

[1]For the case when $\bar{\Lambda}(x)$ and $\bar{B}(x)$ do not vary with x and when $\bar{C}(x) = 0$, these transfer functions belong to the Callier-Desoer algebra [5].

as control action variable. Distant downstream control consists of controlling y_1 using the upstream discharge μ_1 as control action variable.

Let the tracking error be defined as $\epsilon_1 = r_1 - y_1$, and let the transfer functions of the distant downstream controller and the local upstream controller be defined as $K_1(s)$ and $K_2(s)$ respectively. We have $\mu_1(s) = K_1(s)\epsilon_1$ and $\mu_2(s) = 0$ for the distant downstream control, $\mu_1(s) = 0$ and $\mu_2(s) = K_2(s)\epsilon_1$ for the local upstream control. Then, the tracking error e_1 can be expressed as

$$\epsilon_1 = \begin{cases} (1 + G_1(s)K_1(s))^{-1}[r_1 - \tilde{G}_1(s)p_1(s)] & \text{distant d.s.} \\ (1 + \tilde{G}_1(s)K_2(s))^{-1}[r_1 - \tilde{G}_1(s)p_1(s)] & \text{for local u.s.} \end{cases}$$

Thus we note that disturbance rejection is characterized by the modulus of the transfer function $\tilde{G}_1(s)(1+G_1(s)K_1(s))^{-1}$ for the case of distant downstream control and by the modulus of $\tilde{G}_1(s)(1 + \tilde{G}_1(s)K_2(s))^{-1}$ for the case of local upstream control. The control objective is to choose the respective linear controllers K_1 and K_2 such that the moduli of $|\tilde{G}_1(s)(1+G_1(s)K_1(s))^{-1}|$ and $|\tilde{G}_1(s)(1+\tilde{G}_1(s)K_2(s))^{-1}|$ are close to 0 over largest frequency bandwidth. In comparison to distant downstream control, the local upstream control has higher performance because there is no time-delay in $\tilde{G}_1(s)$ and the achievable bandwidth is only limited by actuator's limitation. On the other hand, the local upstream control has low water efficiency because it propagates all perturbations downstream of the canal pool without managing the upstream discharge.

We now briefly describe the PI controller tuning for local upstream control; the design of distant downstream controller follows similar principles [13]. Writing (29) for a single canal pool

$$y_1(s) = G_1(s)\mu_1(s) + \tilde{G}_1(s)[\mu_2(s) + p_1(s)]$$

with $G_1(s) = \exp(-\tau_1 s)/A_1 s$ and $\tilde{G}_1(s) = -1/A_1 s$. For local upstream control, $K_1(s) = 0$ and

$$K_2(s) = k_p\left(1 + \frac{1}{T_i s}\right),$$

with k_p the proportional gain and T_i the integral time. Referring to [6], we state the following tuning rules for local PI controller based a relay experiment in order to obtain a gain margin ΔG dB and a phase margin of $\Delta\Theta^\circ$:

$$k_p = \frac{\pi A_1}{2\tau_1} 10^{-\Delta G/20} \sin\left(\frac{\pi}{180}\Delta\Theta + \frac{\pi}{2}10^{-\Delta G/20}\right) \quad (30)$$

$$T_i = \frac{2\tau_1}{\pi} 10^{\Delta G/20} \tan\left(\frac{\pi}{180}\Delta\Theta + \frac{\pi}{2}10^{-\Delta G/20}\right) \quad (31)$$

where the phase margin[2] satisfies $\Delta\Theta < 90(1 - 10^{-\Delta G/20})$.

5. EXPERIMENTAL RESULTS

In order to demonstrate the feasibility of stealthy deception attacks, we implement deception attacks to compromise the local upstream controller for the Avencq cross-regulator, located at 4.5 km from the head gate on the right back of the Gignac canal (see [1] for a geographical map and Figure 2 for a picture of the site). The cross-regulator is equipped with a 1 m wide sluice gate which regulates the upstream water level to reject the perturbations caused by an offtake located just upstream. The set-point for the upstream water level is set to $r_1 = 79$ cm. The upstream water level is measured every 120 s. The parameters of the ID model were obtained by the relay-feedback auto-tuning method proposed by Åström and Hägglund [15]. The method uses a single relay experiment to determine the frequency response of the canal pool at phase lag of 180°, which in turn determines the parameters τ_1 and A_1 of the ID model. Using the tuning rules (30) and (31), for classical values of gain margin 10 dB and phase margin 43°, we obtain the proportional gain $k_p = -2.9$ and the integral time $T_i = 360$ s.

Figure 2: Upstream of the Avencq station with level sensor, offtake, and sluice gate with local controller.

We test our approach for stealthy deception attacks first in simulation and then in a field test performed directly on the Gignac canal facility. The stealthy deception attack compromises the water level sensor measurements y_1 to send false information to the PI controller implemented on the SCADA system. The goal of the adversary is to withdraw water from the offtake such that the SCADA system does not respond to counter adversarial action. In order to achieve this goal, the adversary injects false data a_1 into water level measurement y_1 such that the resulting deviation from set-point is very close to zero (in fact, during the attack duration attacked level measurement at each time is effectively set to a zero mean random noise sample). Upon receiving incorrect sensor data, the PI controller does not react to the error which is negligible. This results in degraded performance with respect to the actual control requirement of perturbation rejection due to offtake opening. We show next that it is indeed possible to design an attack vector such that the adversary is able to affect controller performance without getting detected even after the attack ends.

5.1 Simulation of Attack Scenarios

The SIC software developed at Cemagref implements an efficient numerical scheme to fully solve nonlinear shallow water equations and allows us to choose from a set of preprogrammed controllers or to test performance of any new controller implemented in Matlab or FORTRAN [2]. The second use of the SIC software is that it provides an interface capability for SCADA real-time control of a physical canal network, in particular, the Gignac canal. Thus, a controller tested in simulation can be directly implemented to control a physical canal without the need to re-code the control al-

[2]We recall that the gain margin (resp. phase margin) is the maximum multiplicative (resp. additive) increase in the gain (resp. phase) of the system such that the system remains closed-loop stable. These robustness margins in frequency domain are directly related to the time domain performance of the system.

gorithm. This method of testing controller in simulation first and then implementing on physical canals greatly limits the possibility of errors due to programming and logical mistakes.

We now describe two stealthy deception attack scenarios on water level sensor for the Avencq pool of the Gignac canal using SIC software as a simulator. In the first attack scenario, shown in Figure 3, the offtake is opened to about 3 cm at time $t = 15$ min after the beginning of the test. The PI controller reacts rapidly by opening closing the sluice-gate and rejects the perturbation in about 40 min. At $t = 75$ min, the offtake is closed. The controller achieves good closed-loop performance and rejects the perturbation in about 45 min by opening the sluice gate as shown in Figure 4. The offtake is again opened and closed at $t = 255$ min

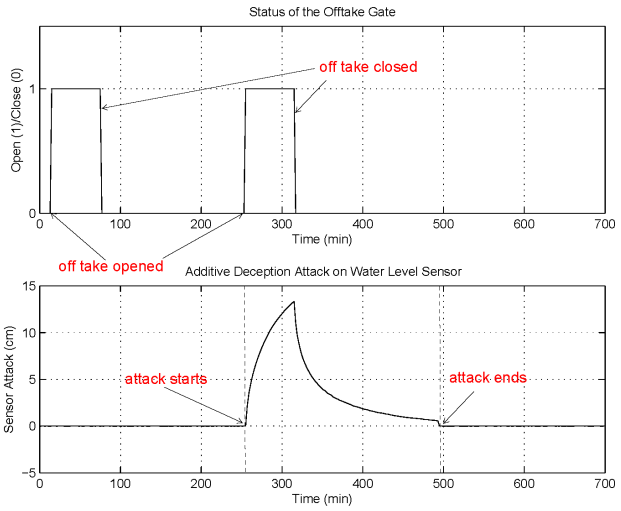

Figure 3: Offtake opening and additive attack with no recovery on upstream water level in SIC.

and $t = 315$ min, – this time under the influence of adversary's action. The adversary injects an additive deception attack on water level sensor measurements such that the difference of resulting sensor measurement with the set point is effectively zero (see figure 3). Therefore, the PI control does not react to the opening of the offtake[3]. The effect of additive attack on the performance of local upstream controller is shown in Figure 4. Even after the closing of the offtake at $t = 315$ min, the adversary continues the deception attack until $t = 495$ min when the water level – evolving in open-loop – comes close to the set point $r_1 = 79$ cm. At $t = 495$ min the adversary stops the deception attack and PI controller reacts to the residual error. The SCADA *may be* able detect the occurrence of attack a posteriori because the residual error at the end of attack is not negligible. We note, however, that for the canal manager monitoring SCADA supervisory interface it may be still difficult to distinguish between the residual error resulting from an attack or an error resulting from a small perturbation in the offtake. The amount of water the adversary manages to withdraw from the offtake during $t = 255$ min and $t = 315$ min can be

[3]This is also equivalent to saying that the control actions are subject to denial-of-service attacks.

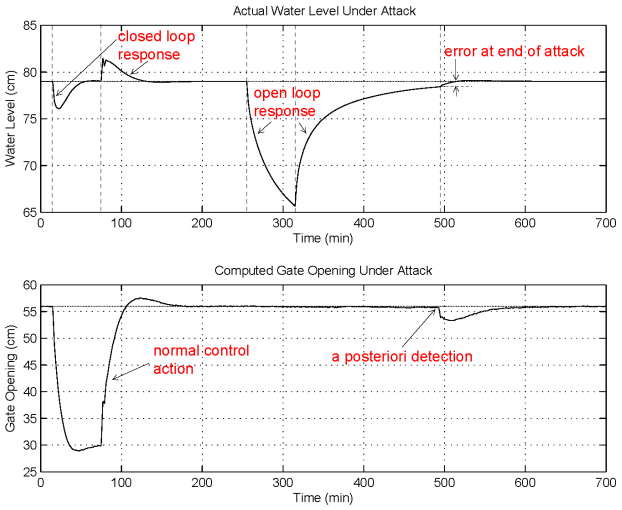

Figure 4: Performance of local upstream PI controller at Avencq cross-regulator under attack with no recovery (SIC simulation).

computed by integrating the gate discharge equation

$$Q_p = U_g\sqrt{Y(X,t)},$$

where $Y(X,t)$ is the actual water level and U_g is the actual gate opening scaled by $C_d L_g \sqrt{2g}$, with C_d the discharge coefficient, L_g the width, and U_g the opening of the offtake gate. Note that under our assumptions, the adversary has the knowledge of actual water level and the opening of offtake gate.

Our second attack scenario consists of increasing the duration of the deception attack so as to bring the residual error at the end of attack negligibly close to zero. The adversary achieves this by continuing to manipulate the water level measurements from $t = 495$ min until $t = 675$ min such that the residual error gradually becomes negligible by the end of attack. We call this period the *recovery period*. As shown in Figure 5, the PI controller is unable to detect any deviation from set-point even after the attack ends. This illustrates that an deception attacks on sensors can indeed be made stealthy in that they remain undetected well after the end of attack.

5.2 Field test on the Gignac canal

We now illustrate the feasibility of carrying out deception attacks on canal SCADA systems in real-life with an experiment conducted on the Avencq cross-regulator on October 12^{th}, 2009 with the help of real-time SCADA interface of the SIC software. This experiment was intended to be a proof-of-concept experiment and so we carried out the adversarial actions directly by modifying the sensor measurements sent from real-time SCADA interface of SIC to the Matlab code that implements PI controller for computing the control action for the sluice-gate. Thus for the purpose of this experiment, we played the adversarial role. This will have the same effect as a hypothesized deception attack on the radio communication link between the level sensor and the SCADA system.

At the start of experiment, we allowed the PI controller to react by changing set-points every few minutes and then

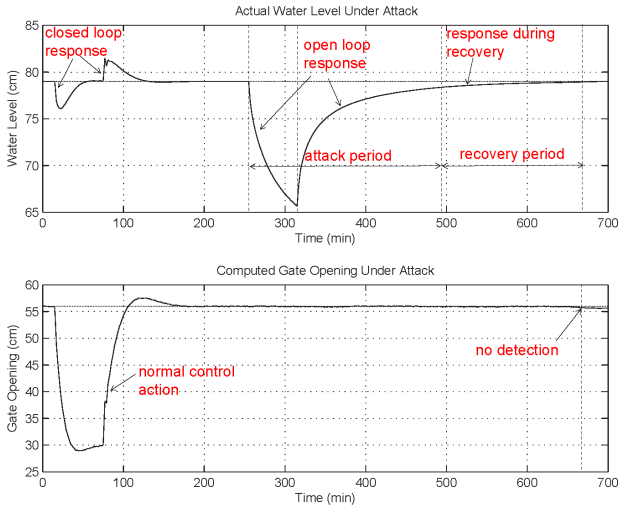

Figure 5: Performance of local upstream PI controller at Avencq cross-regulator under attack with recovery (SIC simulation).

letting the water level stabilize close to set-point in closed-loop. As shown in Figure 6, at $t = 90$ min, the offtake is opened and the adversary injects additive attack to water level measurement such that the PI controller fails to react to perturbation. At around $t = 184$ min the offtake was

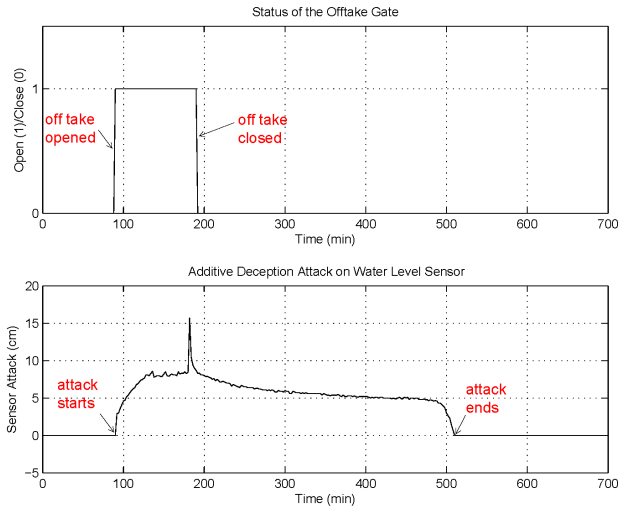

Figure 6: Offtake opening and additive attack upstream water level during the field operational test.

fully opened and then fully closed at around $t = 190$ min by a physical intervention at the Avencq cross-regulator. This effect is captured in the sudden drop in the actual water level as shown in Figure 7. From $t = 190$ min until $t = 360$ min, we (the adversary in this case) continue the deception attack resulting in open-loop response of actual water level, The recovery period lasts from $t = 360$ min to $t = 510$ min using the same recovery action as in the case of simulation experiment described above. However, a residual error still remains after the end of recovery period (which is also the end of attack) and the PI controller reacts to this error. As seen in Figure 7, it is difficult to distinguish between the response of PI control after the attack ends from a normal reaction to perturbation in the case of no attack.

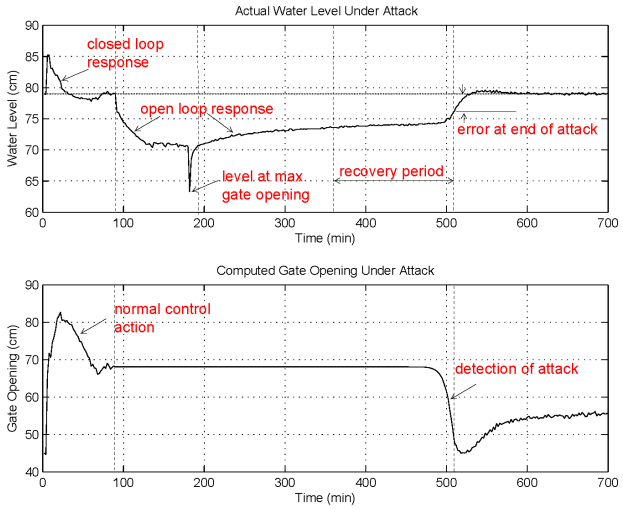

Figure 7: Performance of local upstream PI controller at Avencq cross-regulator under attack (field operational test).

6. CONCLUDING REMARKS

In this article, we used the theory of switching boundary control of PDEs to model deception attacks on SCADA systems managing a cascade of canal pools. We presented an extension of a well known stability mechanism for hyperbolic PDE systems as a sufficient condition to guarantee exponential stability under proportional control, and noted that synthesis of adversarial actions leading to instability can be worked out easily. We qualitatively argued that an adversary can evade detection by stealthily manipulating certain sensor measurements. In order to demonstrate the effect of deception attacks on an actual SCADA system, we presented results from a field operational test on the Gignac canal system in France and also analyzed the performance degradation of PI controller designed for a low-frequency approximation of the more general PDE model. Our results indicate that it is possible for an adversary to withdraw water from the canal while evading detection.

Our synthesis of deception attacks to stealthily withdraw water for a single canal pool can be extended to the case of multiple canal pools. This could be done by approximating the effect of water withdrawal at the downstream canal pool and subsequently manipulating the sensor readings of the downstream pool to deceive the local controller such that it does not react to the actual perturbation. Although we only implement attacks for a local upstream controller, similar analysis could be done for a distant downstream controller as well as for decentralized multi-variable controllers [13]. An interesting research question is then to characterize the trade-off between the effort of adversary versus the impact of resulting deception attack. Such control theoretic characterization can help in evaluating the robustness of practical control methods under attacks and point toward the design of better attack detection methods.

7. ACKNOWLEDGMENTS

This work was supported in part by Cemagref, the France-Berkeley Fund, and the TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (#CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, DoCoMo USA Labs, EADS, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec,TCS, Telecom Italia, and United Technologies. The authors are grateful to Celine Hugodot, David Dorchies, Alvaro A. Cárdenas, and Falk M. Hante for their help.

8. REFERENCES

[1] Experiment Station Research for the modernization of irrigation canals. http://gis-rci.montpellier.cemagref.fr/.

[2] SIC 3.0, a simulation of irrigation canals. http://www.canari.free.fr/sic/sicgb.htm.

[3] J. de Halleux, C. Prieur, B. Andrea-Novel, and G. Bastin. Boundary feedback control in networks of open channels. *Automatica*, 39(8):1365–1376, 2003.

[4] X. Litrico and V. Fromion. Analytical approximation of open-channel flow for controller design. *Applied Mathematical Modeling*, 28(7):677–695, 2004.

[5] X. Litrico and V. Fromion. Boundary control of hyperbolic conservation laws using a frequency domain approach. *Automatica*, 45(3), 2009.

[6] X. Litrico, P.-O. Malaterre, J.-P. Baume, P.-Y. Vion, and J. Ribot-Bruno. Automatic tuning of PI controllers for an irrigation canal pool. *Journal of irrigation and drainage engineering*, 133(1):27–37, 2007.

[7] S. Amin, F. Hante, and A. Bayen. Exponential stability of switched hyperbolic systems in a bounded domain. Technical report, UC Berkeley, 2008.

[8] S. Amin, F. M. Hante, and A. M. Bayen. On stability of switched linear hyperbolic conservation laws with reflecting boundaries. In *HSCC*, pages 602–605, 2008.

[9] R. Anderson. *Security Engineering*. Wiley, 2001.

[10] N. Bedjaoui, E. Weyer, and G. Bastin. Methods for the localization of a leak in open water channels. *Networks and Heterogeneous Media*, 4(2):189–210, 2009.

[11] A. Cardenas, S. Amin, and S. Sastry. Research challenges for the security of control systems. In *3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium*, July 2008.

[12] X. Litrico and V. Fromion. A link between riemann invariants and frequency domain approaches for boundary control of open channel flow. In *47th IEEE Conference on Decision and Control*, December 2008.

[13] X. Litrico and V. Fromion. *Modeling and Control of Hydrosystems*. Springer, 2009.

[14] P. Malaterre and C. Chateau. SCADA interface of the sic software for easy real time application of advanced regulation algorithms. In *Second Conference on SCADA and Related Technologies for Irrigation System Modernization*, Denver, Colorado, 2007.

[15] Åström and Hägglund. *PID controllers: Theory, design, and tuning*. Instrument society of America, 1995.

APPENDIX

A. LINEARIZATION OF SWE

Linearizing (10) around the steady state $(\bar{\xi}_i, \bar{P}_i)$ we obtain

$$\partial_t(\xi_i - \bar{\xi}_i) = \partial_t \zeta_i$$
$$\Lambda(\xi_i)\partial_x \xi_i - \Lambda(\bar{\xi}_i)\partial_x \bar{\xi}_i = \Lambda(\bar{\xi}_i)\partial_x \zeta_i + B_1(\bar{\xi}_i)\zeta_i$$
$$E(\xi_i, P_i) - E(\bar{\xi}_i, \bar{P}_i) = B_2(\bar{\xi}_i, \bar{P}_i)\zeta_i + B_3(\bar{\xi}_i)\zeta_i + C(\bar{\xi}_i)p_i,$$

where

$$B_1(\bar{\xi}_i) = \frac{1}{4}\begin{pmatrix} 3\partial_x \bar{\xi}_{-,i} & \partial_x \bar{\xi}_{-,i} \\ 3\partial_x \bar{\xi}_{+,i} & \partial_x \bar{\xi}_{+,i} \end{pmatrix},$$
$$B_2(\bar{\xi}_i, \bar{P}_i) = \frac{4g\bar{P}_i}{T(\bar{\xi}_{+,i} - \bar{\xi}_{-,i})^2}\begin{pmatrix} -1 & +1 \\ +1 & -1 \end{pmatrix},$$
$$B_3(\bar{\xi}_i) = -g\begin{pmatrix} \overline{(\partial_{\xi_{-,i}} S_{fi})} & \overline{(\partial_{\xi_{+,i}} S_{fi})} \\ (\partial_{\xi_{-,i}} S_{fi}) & (\partial_{\xi_{+,i}} S_{fi}) \end{pmatrix},$$
$$C(\bar{\xi}_i) = \frac{4g}{T(\bar{\xi}_{+,i} - \bar{\xi}_{-,i})}\begin{pmatrix} +1 \\ -1 \end{pmatrix}.$$

We now obtain the linearized SWE in ζ_i coordinates as

$$\partial_t \zeta_i + \Lambda(\bar{\xi}_i)\partial_x \zeta_i + B(\bar{\xi}_i, \bar{P}_i)\zeta_i = C(\bar{\xi}_i)p_i. \quad (32)$$

where $B(\bar{\xi}_i, \bar{P}_i) = (B_1(\bar{\xi}_i) - B_2(\bar{\xi}_i, \bar{P}_i) - B_3(\bar{\xi}_i))$.

B. GATE CONTROL EQUATIONS

Linearizing (2)–(5) expressed in V and Φ variables around the steady state $(\bar{V}_i, \bar{\Phi}_i, \bar{U}_i)$, we obtain

$$\begin{aligned} v_1(0,t) &= k_{1,0}\varphi_1(0,t) + k_{u_0}u_0(t) \\ v_m(X,t) &= k_{m,X}\varphi_m(X,t) + k_{u_m}u_m(t) \\ v_i(X,t) &= k_{i,X}\varphi_i(X,t) + k_{i+1,0}\varphi_{i+1}(0,t) + k_{u_i}u_i(t) \end{aligned} \quad (33)$$

and

$$\begin{aligned} &\alpha_{i,X}v_i(X,t) + \beta_{i,X}\varphi_i(X,t) \\ &\qquad = \alpha_{i+1,0}v_{i+1}(0,t) + \beta_{i+1,0}\varphi_{i+1}(0,t) \end{aligned} \quad (34)$$

where the index i varies as $i = 1, \ldots, m-1$. The coefficients in (33) and (34) depend on the steady state. Using (13), (34), and noting $v_i = V_i - \bar{V}_i$, $\varphi_i = \Phi_i - \bar{\Phi}_i$, we obtain

$$\Phi_{i+1}(0,t) = \bar{\Phi}_{i+1}(0) + \frac{\gamma_{i,X}}{\gamma_{i+1,0}}(\Phi_i(X,t) - \bar{\Phi}_i(X)) \quad (35)$$

where

$$\gamma_{i,X} = \left[\beta_{i,X} + \alpha_{i,X}\left(\frac{1-g_{X,i}}{1+g_{X,i}}\right)\right]$$
$$\gamma_{i+1,0} = \left[\beta_{i+1,0} - \alpha_{i+1,0}\left(\frac{1-g_{0,i}}{1+g_{0,i}}\right)\right].$$

Now using (13) and (35) in the linearized boundary conditions (33) gives us the gate control actions:

$$\begin{aligned} u_0(t) &= -\frac{1}{k_{u_0}}\left(\frac{1-g_{0,i}}{1+g_{0,i}} + k_{1,0}\right)(\Phi_1(0,t) - \bar{\Phi}_1(0)), \\ u_m(t) &= \frac{1}{k_{u_m}}\left(\frac{1-g_{X,m}}{1+g_{X,m}} - k_{m,X}\right)(\Phi_m(X,t) - \bar{\Phi}_m(X)), \\ u_i(t) &= K_{u_i}(\Phi_i(X,t) - \bar{\Phi}_i(X)), \end{aligned} \quad (36)$$

where the coefficient $K_{u_i} = \frac{1}{k_{u_i}}\left(\frac{1-g_{X,i}}{1+g_{X,i}} - k_{i,X} - k_{i+1,0}\frac{\gamma_{i,X}}{\gamma_{i+1,0}}\right)$.