Attack Detection in Water Supply Systems using Kalman Filter Estimator

Kebina Manandhar
Dept. of Computer Science
Georgia State University
Atlanta, Georgia 30303
Email: kmanandhar1@cs.gsu.edu

Xiaojun Cao
Dept. of Computer Science
Georgia State University
Atlanta, Georgia 30303
Email: cao@cs.gsu.edu

Fei Hu
Dept. of Electrical and Computer Engineering
University of Alabama
Tuscaloosa, Alabama 35487
Email: fei@eng.ua.edu

***Abstract*—In this paper we present a framework for the attack and fault detection in a Water Supply System consisting of wireless sensors and drifters. The framework is derived using the Saint-Venant equations for shallow water system. These equations are used to obtain the state space model for Kalman Filter which works as a central estimator. The estimator estimates the sensor readings for the next time cycle based on the readings of the past and neighbor sensors. The estimates from the Kalman filter and the actual observations are then fed to a χ^2 detector. The detector computes the difference between the two readings and compares it with a given threshold to detect if the system has been compromised. Our discussion shows that the proposed framework can detect various attacks and faults in the system.**

I. Introduction

A Cyber Physical System (CPS) tightly combines and co-ordinates its computational/cyber elements together with physical elements. Various CPS systems have been studied, for example, [1], [2]. In many CPS, sensors are deployed to enable the communication between cyber and physical elements by converting the information gathered from the physical world to cyber data. For example, the authors of [3] designed the CPS employing sensor techniques to monitor the algae growth in *Lake Tai, China*. Their design comprises of sensors and actuators to monitor the order of severity of the algae bloom and to dispatch salvaging boats. Similarly, the authors of [4] proposed a CPS approach that navigates users in locations with potential danger, which takes advantage of the interaction between users and sensors to ensure timely safety of the users.

Along with the growth of interest in CPS, the security aspects of the system also attracts significant attention. Recent attacks on cyber systems, such as STUXNET [5] and the attack on Illinoi's water *Supervisory Control and Data Acquisition* (SCADA) system [6], further highlights the vulnerability of such a system and emphasizes the need to study as well as understand the security viewpoint of a CPS. Besides pure cyber attacks as in the case of STUXNET, sensors being one of the indispensable elements of CPS, are equally prone to attacks and manipulations. In this work we focus on the security of sensors in Water Supply System (WSS).

Water Supply System is one of the sensitive areas which can have dramatic public health and economical impacts when attacked. In the literature some attack and detection models were studied: [7]-[12]. The attacks studied in these papers can be categorized into two groups. The first group deals with the deployment of different types of sensors to detect water quality. A taste sensor called *Electronic Tongue* is discussed in [7]. As stated in the paper, the sensor is based on voltametric technique and is able to detect small changes in the chemical and bacterial compound in the water. An advanced nanomaterial based sensor is presented in [8] for continuous and in-situ monitoring of various organic along with non-organic pollutants in water. The second group deals with attack detection schemes primarily focusing on the sensor placement problem. The paper [9] focuses on minimizing the number of sensors as well as minimizing the effect of attacks on general public by efficiently positioning sensors in the WSS. Data mining techniques are applied in [10] to find the optimal location for the sensor placement to determine drinking water quality. The authors of [11] proposed a technique to optimally choose online monitoring points to monitor municipal water supply system for prediction and early detection of contaminants. In both these groups, sensors are considered accurate/reliable and attacks on sensors to manipulate actual sensor readings are not considered. The authors of [12] used theory of switching boundary control of partial differential equations to model deception attacks on water SCADA system. The paper presented a stealthy deception attack that can evade detection by manipulating sensor measurements. However, it does not provide any specific mechanism to detect such an attack on SCADA system.

Attacks on sensor readings allow attackers to mask the actual attack performed on the WSS, causing the attack to remain undetected. How to detect attacks in such scenarios, in fact motivates this study. In this work, we propose a framework for attacks and faults detection in a Water Supply System by applying the Saint-Venant equations and Kalman Filter techniques. Our contributions include: *(i)* we propose a comprehensive mathematical framework to detect possible attacks and faults on the sensors of the WSS; *(ii)* we present various types of possible attacks and discuss how these attacks can be detected by our system; and *(iii)* we investigate a sophisticated false data injection attack on sensors and elaborate corresponding defending approaches.

The rest of the paper is organized as follows. In Section II, we derive the mathematical model for the WSS. The model is

978-1-4673-1466-4/12/$31.00

applied to generate an estimator and detector based on Kalman Filter, which is discussed in Section III. In Section IV, we discuss attacks that can be detected using our framework. Section V presents data injection attack on the sensors and possible defenses along with a case study. Finally, we conclude the work in Section VI.

II. Modeling the Water Supply System

In this section, the Saint-Venant equations are introduced to model the WSS. For a steady state water flow, the hyperbolic and continuous Saint-Venant model are then linearized and discretized for its direct application in the Kalman Filter (to be discussed in next section).

A. The Saint-Venant Model

The Saint-Venant equations are derived from the conservation of mass and momentum [13]. These equations are first order hyperbolic nonlinear partial differential equations and for one dimensional flow with no lateral inflow, these equations can be written as:

$$T\frac{\delta H}{\delta t}+\frac{\delta Q}{\delta x}=0 \tag{1}$$

$$\frac{\delta Q}{\delta t}+\frac{\delta}{\delta x}\left(\frac{Q^2}{A}\right)+\frac{\delta}{\delta x}(gh_cA)=gA(S_b-S_f) \tag{2}$$

for $(x,t)\in(0,L)X\mathbf{R}^+$, where L is the length of the flow (m), $Q(x,t)=V(x,t)A(x,t)$ is the discharge or flow (m^3/s) across cross section, $A(x,t)=T(x)H(x,t).V(x,t)$ refers to velocity (m/s), $H(x,t)$ refers to water depth (m) and $T(x,t)$ refers to the free surface width (m), S_f(x,y) is the friction slope, S_b is the bed slope and g is the gravitational acceleration (m/s^2), These equations can be elaborated [14] in terms of water depth and velocity as:

$$T\frac{\delta H}{\delta t}+\frac{\delta(THV)}{\delta x}=0 \tag{3}$$

$$\frac{\delta V}{\delta t}+V\frac{\delta V}{\delta x}+g\frac{\delta H}{\delta x}=g(S_b-S_f) \tag{4}$$

The friction is empirically modeled by the Manning-Stickler's formula:

$$S_f=\frac{m^2V|V|(T+2H)^{\frac{4}{3}})}{(TH)^{\frac{4}{3}}} \tag{5}$$

where m is the Manning's roughness coefficient $(s/m^{\frac{1}{3}})$

B. Steady State Flow

There exists a steady state solution of the Saint-Venant equations under constant boundary conditions [13]. We denote the variables corresponding to the steady state condition by adding suffix 0. By excluding term containing δt and expanding equation (3), we obtain the following equation:

$$\frac{dV_0(x)}{dx}=-\frac{V_0(x)}{H_0(x)}\frac{dH_0(x)}{dx}-\frac{V_0(x)}{T(x)}\frac{dT(x)}{dx} \tag{6}$$

Solving (4) and (6), we get,

$$\frac{dH_0(x)}{dx}=\frac{S_b-S_f}{1-F_0(x)^2} \tag{7}$$

with $F_0=V_0/C_0$, $C_0=\sqrt{gH_0}$. Here C_0 is the gravity wave celerity, F_0 is the Froude number. We assume the flow to be subcritical i.e, $F_0<1$ [13].

C. Linearized Saint-Venant Model

The linearized Saint-Venant model can be obtained from the steady-state flow characterized by V_0 and H_0 [13]. Let, $v(x,y)$ and $h(x,y)$ denote the first-order perturbations in water velocity and water level. Then,

$$V(x,t)=V_0(x,t)+v(x,t) \tag{8}$$

$$H(x,t)=H_0(x,t)+h(x,t) \tag{9}$$

The values of H and V are substituted in equation (3) and (4) and expanded in Taylor Series. We use T_0 in place of T to emphasize that it is uniform. As described in [13] neglecting higher order terms, a given term $f(V,H)$ of Saint-Venant model can be written as: $f(V,H)=f(V_0,H_0)+(f_V)_0v+(f_H)_0h$ in which, $()_0$ indicates steady state conditions. The linearized Saint-Venant equations can be obtained as the following [14],[15].

$$h_t+H_0(x)v_x+V_0(x)h_x+\alpha(x)v+\beta(x)h=0 \tag{10}$$

$$v_t+V_0(x)v_x+gh_x+\gamma(x)v+\eta(x)h=0 \tag{11}$$

where $\alpha(x),\beta(x),\gamma(x)$ and $\eta(x)$ are given by,

$$\alpha(x)=\frac{dH_0}{dx}+\frac{H_0}{T}\frac{dT_0}{dx} \tag{12}$$

$$\beta(x)=-\frac{V_0}{H_0}\frac{dH_0(x)}{dx}-\frac{V_0(x)}{T(x)}\frac{dT(x)}{dx} \tag{13}$$

$$\gamma(x)=2gm^2\frac{|V_0|}{H_0^{\frac{4}{3}}}-\frac{V_0}{H_0}\frac{dH_0(x)}{dx}-\frac{V_0(x)}{T(x)}\frac{dT(x)}{dx} \tag{14}$$

$$\eta(x)=-\frac{4}{3}gm^2\frac{V_0|V_0|}{H_0^{\frac{7}{3}}} \tag{15}$$

D. Discretization

In order to discretize the linear equations generated in previous section, we use the Lax Diffusive Scheme [14] as listed below. The channel is divided into smaller segments of length Δx and a suitable time interval Δt is selected.

$$\frac{\delta v}{\delta t}=\frac{v_i^{k+1}-\frac{1}{2}(v_{i+1}^k+v_{i-1}^k)}{\Delta t} \tag{16}$$

$$\frac{\delta v}{\delta x}=\frac{(v_{i+1}^k+v_{i-1}^k)}{2\Delta x} \tag{17}$$

$$\frac{\delta h}{\delta t}=\frac{h_i^{k+1}-\frac{1}{2}(h_{i+1}^k+h_{i-1}^k)}{\Delta t} \tag{18}$$

$$\frac{\delta h}{\delta x}=\frac{(h_{i+1}^k+h_{i-1}^k)}{2\Delta x} \tag{19}$$

Given $(h_i^k, v_i^k)_{i=0}^I$, we want to compute $(h_i^{k+1}, v_i^{k+1})_{i=0}^I$. Here I is the total number of segments of length Δx. The updated equations for (h_i, v_i) are:

$$\begin{aligned} h_i^{k+1} &= \frac{1}{2}(h_{i+1}^k + h_{i-1}^k) \\ &\quad -\frac{\Delta t}{4\Delta x}(H_{0(i+1)} + H_{0(i-1)})(v_{i+1}^k - v_{i-1}^k) \\ &\quad -\frac{\Delta t}{4\Delta x}(V_{0(i+1)} + V_{0(i-1)})(h_{i+1}^k - h_{i-1}^k) \\ &\quad -\frac{\Delta t}{2}\alpha_{i+1}v_{i+1}^k + \alpha_{i-1}v_{i-1}^k \\ &\quad -\frac{\Delta t}{2}\beta_{i+1}h_{i+1}^k + \beta_{i-1}h_{i-1}^k \end{aligned} \tag{20}$$

$$\begin{aligned} v_i^{k+1} &= \frac{1}{2}(v_{i+1}^k + v_{i-1}^k) \\ &\quad -\frac{\Delta t}{4\Delta x}(V_{0(i+1)} + V_{0(i-1)})(v_{i+1}^k - v_{i-1}^k) \\ &\quad -\frac{g\Delta t}{2\Delta x}(h_{i+1}^k - h_{i-1}^k) \\ &\quad -\frac{\Delta t}{2}\gamma_{i+1}v_{i+1}^k + \gamma_{i-1}v_{i-1}^k \\ &\quad -\frac{\Delta t}{2}\eta_{i+1}h_{i+1}^k + \eta_{i-1}h_{i-1}^k \end{aligned} \tag{21}$$

We assume that Δx is very small then we can write that $h_{i-1} = h_i = h_{i+1}$ and $v_{i-1} = v_i = v_{i+1}$. The above equations will become:

$$\begin{aligned} h_i^{k+1} &= (1 - \frac{\Delta t}{2}\beta_i + \beta_i)h_i^k \\ &\quad +(\alpha_i - \frac{\Delta t}{2}\alpha_i)v_i^k \end{aligned} \tag{22}$$

$$\begin{aligned} v_i^{k+1} &= (\eta_i - \frac{\Delta t}{2}\eta_i)h_i^k \\ &\quad +(1 - \frac{\Delta t}{2}\gamma_i + \gamma_i)v_i^k \end{aligned} \tag{23}$$

E. Discrete Linear State-Space Model

From the discretized equations in previous section, state-space model can be formed as follows:

$$x(k+1) = Ax(k) + Bu(k) + w(k) \tag{24}$$

where, $x(k) = (v_0^k, ..., v_I^k, h_0^k, ..., h_I^k)^T$, with the applied control $u(k)$ in the form of discharge perturbation at the upstream end v_0^k and the discharge perturbation $w(k)$ at the downstream end v_I^k [13]. Here, w_k, x_0 are independent Gaussian random variables, and $x_0 \sim \mathcal{N}(0, \Sigma)$ and $w_k \sim \mathcal{N}(0, Q)$.

III. Detecting Attacks using Kalman Filter

In this section, we introduce the Kalman Filter [16] technique to obtain estimates for the state space vector $x(k)$ described in Section II-E. Figure 1 shows the control system of the Kalman Filter with the sensor readings or observations from the Water Supply System namely, y_i. And x_i denotes the output of the control system that is fed to the controller. The observations (y_i) are forwarded to the central system containing estimator and detector at a regular time interval

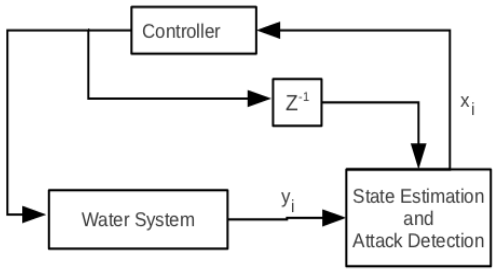

Fig. 1. Kalman Filter

denoted by Δt. At each time step Δt, the estimator of the system generates estimated readings based on the reading of previous time step. These readings are used by the detector to detect the difference between the newly observed sensor readings and estimated readings.

A. The Kalman Filter

To apply the Kalman Filter technique, the observation equation for the above system can be written as:

$$y_k = Cx_k + \nu_k \tag{25}$$

Here, $y_k = [y_1^k, ..., y_m^k]^T \in \mathbf{R^m}$ is measurement vector collected from the sensors and y_i^k is the measurement generated by sensor i at time k. v_k is the measurement noise and assumed to be white Gaussian noise, which is independent of initial conditions and process noise.

Kalman filter can then be applied to compute state estimations $\hat{x}_k$ using observations y_k. Let the mean and covariance of the estimates be defined as follows:

$$\begin{aligned} \hat{x}_{k|k} &= E[x_k, y_0, ..., y_k] \\ \hat{x}_{k|k-1} &= E[x_k, y_0, ..., y_{k-1}] \\ P_{k|k-1} &= \Sigma_{k|k-1} \\ P_{k|k} &= \Sigma_{k|k-1} \end{aligned} \tag{26}$$

The iterations of Kalman filter can be written as:

$$\begin{aligned} \hat{x}_{k+1|k} &= A\hat{x}_k + Bu_k \\ P_{k|k-1} &= AP_{k-1}A^T + Q \\ K_k &= P_{k|k-1}C_k^T(C_kP_{k|k-1}C_k^T + R)^{-1} \\ P_{k|k} &= P_{k|k-1} - K_kCP_{k|k-1} \\ \hat{x}_k &= \hat{x}_{k|k-1} + K_k(y_k - C_k\hat{x}_{k|k-1}) \end{aligned} \tag{27}$$

Initial conditions being $x_{0|-1} = 0, P_{0|-1} = \Sigma$ and K_k being Kalman gain. We assume that the kalman gain converges in a few steps and is already in a steady state, then,

$$P \triangleq \lim_{k\to\infty} P_{k|k-1}, K = PC^T(CPCT + R)^{-1} \tag{28}$$

The Kalman filter equation can be updated as

$$\hat{x}_{k+1} = A\hat{x}_k + Bu_k + K[y_{k+1} - C(A\hat{x}_k + Bu_k)] \tag{29}$$

The residue z_{k+1} at time $k+1$ is defined as:

$$z_{k+1} \triangleq y_{k+1} - \hat{y}_{k+1|k}$$

equivalently,

$$z_{k+1} \triangleq y_{k+1} - C(A\hat{x}_k + Bu_k) \tag{30}$$

The estimate error e_k is defined as:

$$e_k \triangleq x_k - \hat{x}_k \tag{31}$$

Substituting the values x_{k+1} and $\hat{x}_{k+1}$ from equations (24), (25) and (29), we obtain the following recursive formula for error calculation:

$$e_{k+1} = (A - KCA)e_k + (I - KC)w_k - K\nu_k \tag{32}$$

B. Attack/Failure Detection

Since it is assumed that the noises in the system is Gaussian, we use χ^2 detector to compute the difference between the observed value from the sensors and the estimated values from the Kalman Filter as the following [17]:

$$g_k = z_k^T \mathcal{P} z_k \tag{33}$$

where $\mathcal{P}$ is the covariance matrix of z_k, the residue. The χ^2 detector compares g_k with a certain threshold to detect a failure or attack and triggers the alarm for potential attack or failure.

$$g_k > threshold, \tag{34}$$

where g_k is defined as:

$$g_k = g(z_k, y_k, \hat{x}_k, ..., z_{k-\tau+1}, y_{k-\tau+1}, \hat{x}_{k-\tau+1}) \tag{35}$$

The function g is continuous and $\tau \in \mathbf{N}$ is the window size of the detector [17].

IV. Attacks and Defenses

Without loss of generality, we use level and velocity sensors in this work to design the framework. However, it must be noted that the framework is valid when any other types of sensors are used in the WSS. Without limiting ourselves to just level and velocity sensors, in this section, we list various attack/fault models that can be defended using the framework designed above.

1) WSS fault: Any system fault that can be detected by the sensors of the WSS, for example, water leakage, unintentional addition of contamination, will alert the detector and the alarm will be triggered.
2) Naive attack on the system: If the attacker simply adds contaminants to the water or steals water from the WSS, the sensors will report it to the central system. The detector will detect it immediately as the difference between estimated and actual observation will be large and will trigger the alarm.
3) Physical damage to the sensors: When the sensors are damaged physically, no measurements are obtained causing the system to detect it immediately. As in case of naive attack, the estimated reading will be different from the actual reading and will cause the alarm to trigger.
4) Random data injection: Let us assume that the attacker has control over some sensors and feeds some random values to mislead the system. As these randomly generated sequences will not correspond to the estimates generated by the Kalman Filter, the detector will detect the difference and report the attack.

V. Injection of False Data into the System

The attacks discussed above do not take statistical attack into account. The authors of [17] proposed false data injection attack that uses statistical analysis and has proved that a system with the Kalman Filter estimator can be attacked by generating an attack sequence y_k^a. It is assumed that the attacker knows the matrices A, B, C, Q, R of the system along with observation gain K. The attack sequence changes the measurements obtained from the sensors to:

$$y'_k = Cx'_k + v_k + \Gamma y_k^a \tag{36}$$

where $\Gamma = diag(\gamma_1, ...\gamma_m)$ is the sensor selection matrix. γ_i is a binary variable whose value is 1 if the sensor i has been compromised, 0 otherwise. y_k^a is the input from the attacker. y'_k and x'_k denote the partially compromised system and are different from the original non-tampered values. Then the system dynamics changes as following:

$$\begin{aligned} x'(k+1) &= Ax'(k) + Bu'(k) + w(k) \\ y'_k &= Cx'_k + \nu_k + \Gamma y_k^a \\ \hat{x}'_{k+1} &= \hat{x}'_k + Bu'_k + K_k[y'_{k+1} - C(A\hat{x}'_k + Bu'_k)] \end{aligned} \tag{37}$$

The new residue and estimation error can be defined as

$$\begin{aligned} z'_{k+1} &= y'_{K+1} - C(A\hat{x}'_k + Bu'_k) \\ e'_k &= x'_k - \hat{x}'_k \end{aligned} \tag{38}$$

Also, the new error detection function can be defined as

$$g'_k = g(z'_k, y'_k, \hat{x}'_k, ..., z'_{k-\tau+1}, y'_{k-\tau+1}, \hat{x}'_{k-\tau+1}) \tag{39}$$

The alarm will be triggered when

$$g'_k > threshold \tag{40}$$

As stated in [17], if the attacker simply injects a large y_k^a, the residue z'_k will be large as well resulting in attack detection by the detector. However, if the vector $\hat{x}'_k, y'_k, z'_k$, has the same statistical properties in the partially compromised system as those of the healthy system, then the attack can be successful.

The algebraic condition to identify perfectly attackable systems is presented in [17]. As stated in the paper, the system described above is perfectly attackable iff A has an unstable eigenvalue and the corresponding eigenvector v satisfies the following conditions:

1) $Cv \in span(\Gamma)$, where $span(\Gamma)$ is the column span of Γ

2) v is the reachable state of dynamic system $e_{k+1} = (A - KCA)e_k - K\Gamma y^a_{k+1}$

Using the results from [17], the attack sequence can be generate using the following equation:

$$y^a_{n+i} = y^a_i - \frac{\lambda^{i+1}}{M} y^*, i = 0, 1, 2, ... \quad (41)$$

where, $|\lambda| \geq 1$ and $Cv \in$ span(Γ). There exists y^* such that $\Gamma y^* = Cv$ and M = max $||\Delta z_k||$. Following equation (41), the attacker can generate an attack sequence based on eigen decomposition of matrix A and matrix Γ.

A. Defense Against Data Injection Attack

As proposed in [17], the eigen decomposition could also be performed at the defender side on matrix A to find all the unstable eigenvector v to compute Cv. For each Cv, the 1's will indicate the compromised sensors needed by the attacker to perform a successful attack along direction v. Therefore, the defender can defend the system by deploying more redundant sensors along the direction of attack.

Another powerful defense mechanism is to implement the data encryption algorithms. The data from sensors to the estimator can be encrypted using either symmetric key or asymmetric key. The key can be periodically exchanged between the sensors and the central system which will make data injection more difficult.

B. Case Study

Using the Water Supply model and attack model described in sections above, a more comprehensive illustration is provided here. For the sake of simplicity, one water level sensor and one drifter is considered. Let the dimension of the state space be $n = 2$. Then, from equation (25) and (26) and assuming $\Delta t = 1$, we get:

$$X_{k+1} = \begin{bmatrix} 1 + \frac{\beta_i}{2} & \frac{\alpha_i}{2} \\ \frac{\eta_i}{2} & 1 + \frac{\gamma_i}{2} \end{bmatrix} X_k + w_k$$

where, $X_k = \begin{bmatrix} h_k \\ v_k \end{bmatrix}$

Also,

$$y_k = X_k + \nu_k \quad (42)$$

Considering the above system and substituting Manning's Coefficient $m = 0.025$, the matrix A will be: $A = \begin{bmatrix} 1 & 0 \\ 0 & 1.006 \end{bmatrix}$ and value of K will be: $K = \begin{bmatrix} 0.618 & 0 \\ 0 & 0.6193 \end{bmatrix}$

The eigenvector for the system with level sensor compromised will be $[0, 1]^T$ and with $n = 2$ the attack sequence can be designed to be:

$$y^a_{2+i} = y^a_i - \frac{\lambda^{i+1}}{M} y^*, \quad (43)$$

where i = 1,2,3,... and $\lambda <= 1$ and $M <= 1$

VI. Conclusion

In this paper, we have presented a framework for attack/fault detection in a Water Supply System (WSS). The framework is derived mathematically using the Saint-Venant equations for the shallow water systems. The Kalman Filter is then applied to these equations to obtain the state estimations for the WSS. The estimations obtained from the Kalman filter along with the actual observations are fed to a χ^2 detector and the difference between the two readings is compared with a given threshold. The detector is designed to trigger an alarm when the difference is greater than the threshold, hence detecting attacks or faults in the WSS. We have demonstrated various attacks can be detected by the framework. Furthermore, we have addressed a statistical attack model that could bypass the detection scheme and discussed possible defenses against such an intelligent attack.

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference (DAC), 2010 47th ACM/IEEE*, pp. 731 –736, June 2010.

[2] E. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*, pp. 363 –369, May 2008.

[3] D. Li, Z. Zhao, L. Cui, H. Zhu, L. Zhang, Z. Zhang, and Y. Wang, "A cyber physical networking system for monitoring and cleaning up blue-green algae blooms with agile sensor and actuator control mechanism on lake tai," in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 732 –737, April 2011.

[4] M. Li, Y. Liu, J. Wang, and Z. Yang, "Sensor network navigation without locations," in *INFOCOM 2009, IEEE*, pp. 2419 –2427, April 2009.

[5] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, (New York, NY, USA), pp. 355–366, 2011.

[6] "U.S. probes cyber attack on water system," November 2011. http://www.reuters.com/article/2011/11/21/us-cybersecurity-attack-idUSTRE7AH2C320111121.

[7] M. Lindquist and P. Wide, "New sensor system for drinking water quality," in *Proceedings of Sensors for Industry Conference*, pp. 30 – 34, 2004.

[8] A. Vaseashta, E. Braman, P. Susmann, Y. Dekhtyar, and K. Perovicha, "Sensors for water safety and security," in *Sensors Applications Symposium (SAS), 2011 IEEE*, pp. 302 –307, February 2011.

[9] X. Ma, Y. Song, J. Huang, and J. Wu, "Robust sensor placement problem in municipal water networks," in *2010 Third International Joint Conference on Computational Science and Optimization (CSO)*, vol. 1, pp. 291 –294, May 2010.

[10] A. Ailamaki, C. Faloutos, P. S. Fischbeck, M. J. Small, and J. VanBriesen, "An environmental sensor network to determine drinking water quality and security," *SIGMOD Rec.*, vol. 32, pp. 47–52, December 2003.

[11] W. Wu, J. Gao, M. Zhao, Z. qian, X. Hou, and Y. Han, "Assessing and optimizing online monitoring for securing the water distribution system," in *2007 IEEE International Conference on Networking, Sensing and Control*, pp. 350 –355, April 2007.

[12] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Stealthy deception attacks on water scada systems," in *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*, HSCC '10, (New York, NY, USA), pp. 161–170, 2010.

[13] M. Rafiee, A. Tinka, J. Thai, and A. Bayen, "Combined state-parameter estimation for shallow water equations," in *American Control Conference (ACC), 2011*, pp. 1333 –1339, July 2011.

[14] M. Rafiee, Q. Wu, and A. Bayen, "Kalman filter based estimation of flow states in open channels using lagrangian sensing," in *Proceedings of the 48th IEEE Conference on Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009.*, pp. 8266 –8271, December 2009.

[15] X. Litrico and V. Fromion, "Infinite dimensional modelling of open-channel hydraulic systems for control purposes," in *Proceedings of the 41st IEEE Conference on Decision and Control*, vol. 2, pp. 1681 – 1686 vol.2, December 2002.

[16] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal Of Basic Engineering*, vol. 82, pp. 35–45, 1960.

[17] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *2010 49th IEEE Conference on Decision and Control (CDC)*, pp. 5967 –5972, December 2010.