ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 1, Issue 1, November 2012 | A Monthly Peer Reviewed & Referred Journal |

Evaluation of the Quality and Process Control System of Domestic Water Supply

Lalit Pal Singh

Assistant Professor, Dept. of Chemistry, R.B.S. College, Agra, India

ABSTRACT: This paper introduces the role of a PCS in a critical infrastructure, and especially addresses the processing flow and control of a water system. By leveraging advanced IT technologies, a modern process control system (PCS) can help monitor and control physical processes in a water system. Conventionally, a water system is composed of a water treatment subsystem and a water distribution subsystem. To provide better water quality and steady water flow, PCSs should be adopted in these subsystems to more precisely control the concentration of chemicals in water and the outlet valve of water tanks. We investigate the security issues and possible attacks in a water system adopting a close- loop control mechanism. Taking the concentration control of chlorine in water as an example, we formally explain how an integrity attack leads a water system into a harmful state by adding improper amount of chlorine into water. In the future, we will further develop a formal model describing a *n*-tank water system, evaluate the impact of simultaneous more attacks and discuss the potential impacts. We will also try to design a detection and defence system to resist against known attacks.

KEYWORDS: evaluation, quality, control, domestic, water supply, IT technologies, security, tank water

I. INTRODUCTION

PROCESS CONTROL SYSTEM

Control systems are computer-based systems that mon- itor and control physical processes. Depending on the applications, a control system may also be referred to Process Control System (PCS), Supervisory Control and Data Acquisition (SCADA) system, or Cyber-Physical System (CPS).

Traditionally, a PCS, running one or more physical pro- cesses, is usually composed of several sensors, actuators, and one controller, as shown in Fig. 1. Sensors monitor the status of the physical processes.[1] The controller receives the process status from sensors, computes, makes decisions, and commands the actuators to control the operations of a physical process. These components (sensors, actuators and controller) are connected in a network such that they can communicate with each other and deliver information via the network.

Advanced of modern networking technologies, a PCS can provide a more powerful and flexible domination of the distributed collaborative works. In between these collaborative works, information can be updated to the controller via the network. Hence, the physical processes can be fully controlled by the controller.[2] With such a PCS, administrators can remotely and efficiently manage and regulate the physical processes in the system.

In this way, a PCS can be further applied to a variety of critical information infrastructures, such as electric power grid, factories and refineries, water systems, etc. By adopt- ing a PCS in an electrical power grid, the power company

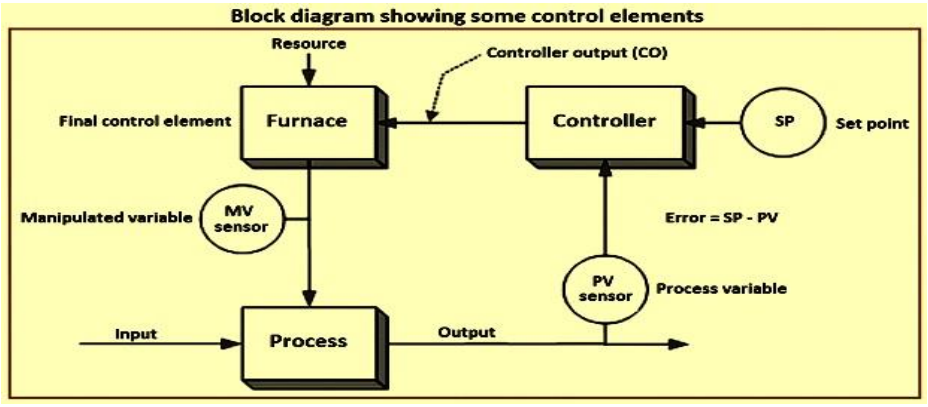

Fig. 1. General Architecture of a Process Control System: the system consists of several sensors and actuators

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 1, Issue 1, November 2012 | A Monthly Peer Reviewed & Referred Journal |

Normally one controller can maintain reliable operations and service to provide a stable power flow over the delivery network. Similarly, a PCS helps an industrial plant control the manufacturing process and maintain the production rates. Again, a water system utilizes a PCS to govern the water purification process, and distributes clean and stable livelihood water to end users.[3]

Since these systems are mostly safety-critical, any dam- age to the system or any instability of the system can cause great impacts on the industry, or even worse, on the public. In short, protecting a PCS from being attacked then recently gets much attention from public [1] [2].

In this paper, we overview a generic water system in Section II. Then, we dive into the design of a PCS adopted in a water system, which is composed of water treatment and distribution subsystems in Section III. Subsequently, we analyze the control mechanism of a water system and discuss its security in Section IV. Finally, Section V concludes the paper.

WATER SYSTEM

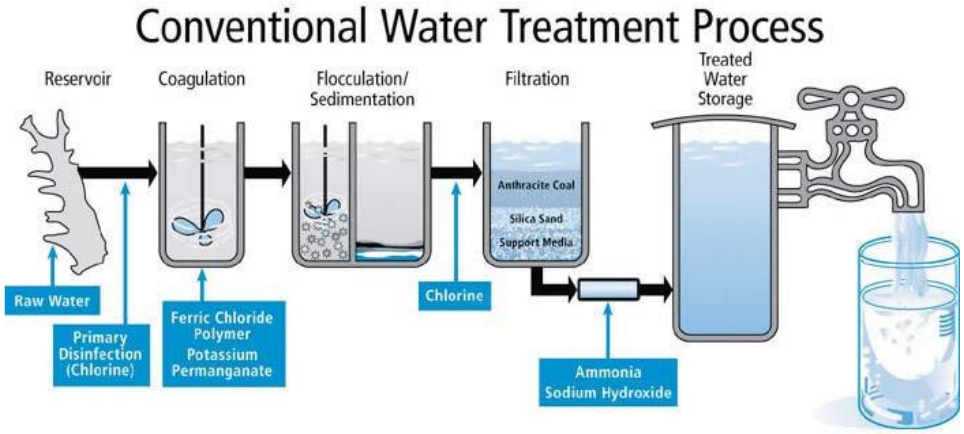

Fig.2:Generally, a water system can be divided into two subsystems: treatment and distribution.

Water treatment removes the undesired substances in raw water and main- tains the expected water quality at outlet of the water system. Water distribution guarantees the steady supply of water.[4]

A. *Treatment*

To obtain clean and drinkable water, several procedures should be considered and executed in a water system to purify raw water. The main purifying process includes flocculation, precipitation, filtration and disinfection, as shown in Fig. 2.

- **Flocculation** removes turbidity or color of water. The suspended solids in raw water are gathered to form bigger particles. Most of the time, some chemicals will be injected to hasten this subprocess.
- **Precipitation** settles the particles generated in **floc- culation**. Tanks used in **precipitation** are bigger, but with a slower water flow (to make the particles settled more easily).[5]
- **Filtration** filters and removes the remaining sus- pended particles.
- **Disinfection** disinfects the water to decrease the risk of pathogen exposure to a human user. Again, chemicals are required to disinfect water [3].

By means of these subprocesses, the undesired chemicals, materials, and biological contaminants can be filtered and removed from raw water.

II. DISCUSSION

One of the major goals of water treatment is to provide high water quality. When evaluating the water quality, numerous factors are considered, including turbidity, con- centration of residual chlorine, pH, temperature, etc. These factors can be evaluated with three basic assessments: physical assessment, chemical assessment and biological assessment [5]. Physical assessment is the standard for the appearance and the taste of water; chemical assessment is the standard for the dissolved chemicals in water; and biological assessment is the standard for the biological contaminants in water, such as bacteria. In the following paragraphs, we explain the three assessments in detail.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 1, Issue 1, November 2012 | A Monthly Peer Reviewed & Referred Journal |

Physical assessment includes the limitation of turbid- ity, temperature, and odor etc. Turbidity is the mea- surement of the scattering degree of the suspended materials toward light in water. Since there are several kinds of suspended materials (clay, organic or inor- ganic colloid, and plankton etc.) existed in water [6], the turbidity (apperance) of raw water is influenced. If the turbidity is higher than the standard threshold, it indicates the raw water is not drinkable. Although the turbidity is affected by the suspended solids, these solids may not be harmful. Instead, they may protect pathogens from being disinfected[6].

Chemical assessment includes the residual chlorine, heavy metals, orthophosphates etc. The concentra- tion of chemicals in water has a great impact on the palatability of water. For example, chlorine, the most common disinfectant in water industry, forms hypochlorous acid and hypochlorite ions (aka effec- tive residual chlorine) when mixing up with water. However, highly concentrated chlorine may not effec- tively reduce pathogen exposure and even overreacts with the organic compounds to produce harmful by- products. Hence, proper concentration control for chemicals in water is important in treating water.

Biological assessment is the limitation of the con- centration of different organisms in water. High con- centration of organisms (such as bacteria, escherichia coli, cryptosporidium etc.) is risky to human health. A water company usually adopts some chemicals to reduce the concentration of organisms in water.

The concentration of the chemicals in water is consid- ered a major factor in treating water. To better control water quality, PCSs are generally introduced in a water system to maintain the concentration of the chemicals in water in a proper range. Section III-A lists the existing PCS simulators of water treatment.[7]

B. *Distribution*

The water distribution subsystem takes care of the treated water and distributes the water to the end users. In such a subsystem, two major goals should be reached:

1) the water quality should be maintained even after a long-distanced distribution, and 2) supply stability should be guaranteed.

Generally, a water distribution subsystem is composed of actuators, pipes, and tanks. These components construct a network for distributing water. The behaviours and operations of these components may vary by the topology of the distribution network. Fig. 3 shows some examples of the topology of water distribution network [7]. In Fig. 3(a) presents a tree-structured distribution network. In such a structure, a large reservoir is presented to supply water to internal reservoirs or end users. The flow directions should be further defined from source to destinations, such that the consuming nodes can obtain the demanded water. Fig. 3(b), a star network is presented, starting from the central source to the internal reservoirs and end users. Usually, the central source is the largest source node supplying water to other consuming nodes (i.e., internal reservoirs or end users).[8]

III. RESULTS

The control scenarios of water distribution may vary by different topologies. However, the objectives and goals are remained same, that is, delivering clean water and providing steady water supply.

I. PCSS USED IN A WATER SYSTEM

To provide clean and drinkable water, adequate control of water treatment and distribution is necessary. For water treatment, water companies should control the hydraulic stability and optimize the subprocesses of treatment. For water distribution, water companies need to control the system to supply steady water flow and qualified water. In the following sections, we explain the existing researches[9]

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 1, Issue 1, November 2012 | A Monthly Peer Reviewed & Referred Journal |

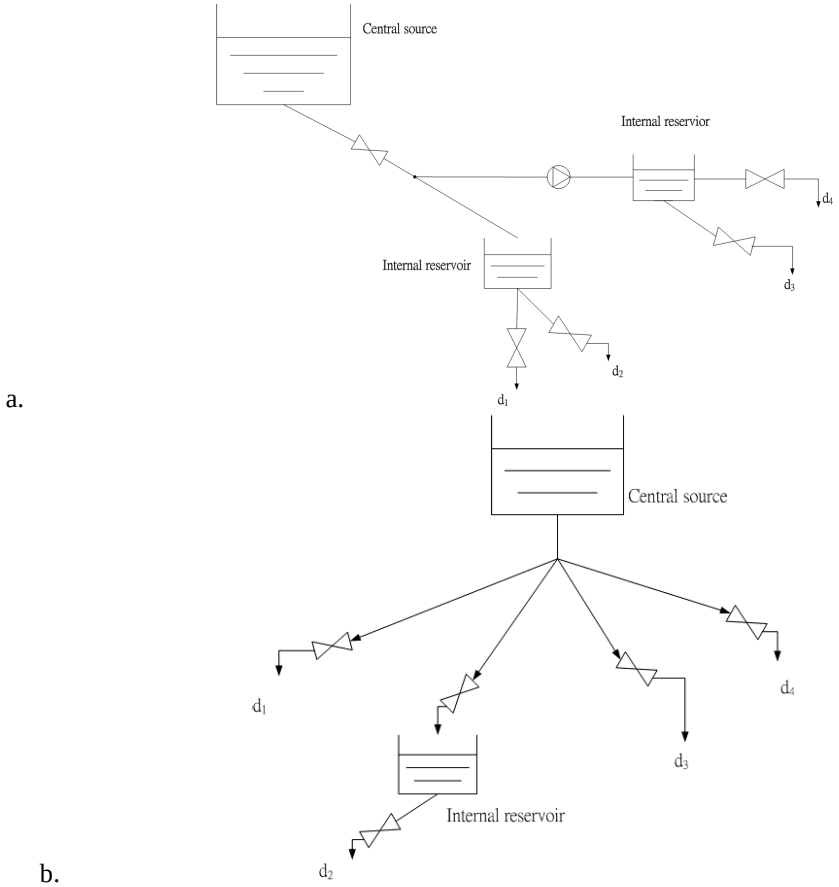

Fig. 3. Basic Topology Types of a Water Distribution Network: (a) Tree; (b) Star discussing the process control in water treatment and distribution subsystems.

A. *Water Treatment with PCS*

To maintain the water quality, PCSs are usually adopted in a water system to control the subprocesses of water treatment and provide variant consuming demands of water. Recent researches have developed a variety of sim- ulators to help a water company understand the reactions of a water system under different control strategies and parameters [8]:

- **OTTER** [9], a FORTRAN-based tool developed by WRc, simulates the dynamics in subprocesses of water treatment and the operating conditions. OTTER helps an operator analyze the changes of disinfectants under different strategies such that the operator can

1) study the effects of pH control on coagulation strategies, 2) predict the maximum throughput of a treatment works and 3) evaluate the monitoring strategies for water treatment.[14]

- **Stimela** [10], developed by DHV Water BV and the Delf University of Technology, models the water treatment environment. Stimela especially focuses on the analysis and simulation of water quality. In Stimela, the treatment process is able to calculate the changes of factors (pH, oxygen concentration etc.) which have impact on water quality. The simulator also allows the connection of different processes and models, and can be used to evaluate the interference and effects among the processes and models.
- **WatPro** [11] is a simulator of a water treatment subsystem for quality prediction. With specific treat- ment subprocesses and chemical addition, WatPro can analyze the conditions of steady water [8]. WatPro adopts the dynamics of chemicals in water to model the behavior of subprocesses of water treatment. WatPro also provides flexibility for a water company to design specific topologies for treating water.

Most of these simulators focus on different procedures of a water treatment subsystem. They simulate the behav- ior of subprocesses (flocculation, disinfection, sedimen- tation, etc.) of water treatment. However, few of them emphasizes on the security and control algorithm of water treatment.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 1, Issue 1, November 2012 | A Monthly Peer Reviewed & Referred Journal |

B. *Water Distribution with PCS*

In addition to the water treatment, water distribution also plays an important role in a water system. After treatment, clean water may still be polluted during the dis- tribution pipes. To keep the water drinkable after leaving the distribution pipes, chlorine is added to avoid the taint. As mentioned in the previous section, sufficient chlorine disinfects virus in water, but overdosed chlorine contrarily produces harmful by-products in water. Since chlorine in water decays with time, proper amount of chlorine should be added into the distribution subsystem.

For the past few years, many models were presented to discuss the control of chlorine concentration in water distribution subsystems. In 1994, Rossman et al. proposed a mass-transfer-based model [12] to predict the decay of chlorine in water during the distribution pipes. In 1998, Zierolf et al., developed an input-output model to discuss the chlorine transport in drinking water [13]. Several years after, O. Ozdemir and A. Ucak [14] proposed a time- driver approach to trace chlorine transport and evaluate chlorine decay in the distribution pipes. In the same year, Polycarpou et al. [15] applied a feedback control algorithm to the quality control model for evaluating the changes of chlorine. Then, an adaptive control algorithm [16] is utilized to control a water distribution subsystem so that the subsystem can meet the time-variant consuming demands and provides stable water quality.

Most of these models emphasize the importance of adopting PCSs into water distribution subsystems. Once the concentration of chemicals in water can be properly controlled, researchers should further consider the security of the PCSs to avoid the significant damages to the public.

IV. CONTROL MECHANISM AND ITS SECURITY

To better control the water quality, feedback control (close-loop) mechanisms [15] are used to monitor the water quality at the specified point (such as the output ports of distribution pipes), such that the water system can precisely adjust the parameters to control the treatment and

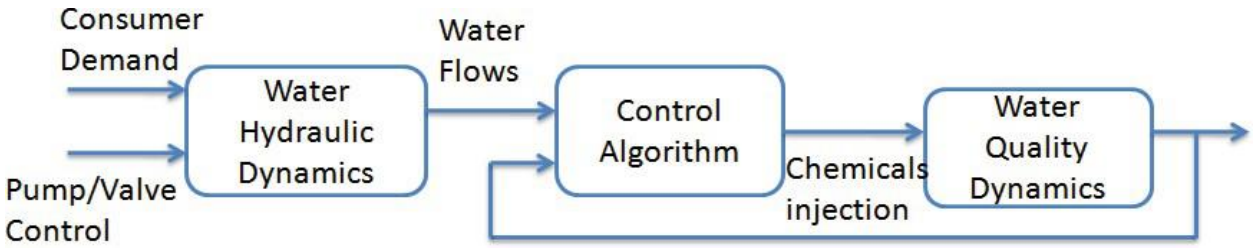

Fig. 4. Schema of a Close-loop Water System distribution subsystems. Fig. 4 shows the general schema of a close-loop control mechanism (feedback) of a water system.

Typically, when adopting a PCS into a water system, the whole controlling system can be represented with sensors, controllers, actuators. Sensors monitor the status of water subsystems (i.e. treatment and distribution) and send status information (s) to the controller. The controller sends control signals (u) to control the actuators. Upon receiving a control signal, an actuator performs a physical action (e.g., opening a valve, adding chlorine, etc.) in the physical system, as illustrated in Fig. 5.

To formally model attacks on such a control system, we define the following notations:

- Sensing data (y_i): denotes the value sensed by the ith sensor.
- Control signal (u_i): denotes the output of the ith controller.[13]

With those notations, we can identify and address attacks on the whole system, as illustrated in Fig. 6. In the figure, an adversary may attack the system at points A_i, where i = 1 11. In addition to the direct attacks (A_9, A_{10}, A_{11}) against controllers, sensors, actuators and the water system [16], each path may suffer from the integrity attacks (A_1, A_2, A_3, A_4) and DoS (denial-of- service) attacks (A_5, A_6, A_7, A_8) [18]. When encountering integrity attacks, the input signals are tampered (i.e., y becomes $y\hat{}$, u becomes $u\hat{}$). On the other hand, signals are dropped if DoS attacks are launched.

Taking the concentration of chlorine as an example, a proper amount of residual chlorine in water should be maintained to provide drinkable water quality. Fig. 7 shows the concentration of chlorine in a water tank. The dashed line stands for the amount added into the tank, while the solid line presents the concentration of residual chlorine in the tank. In such a system, the PCS periodically adds a fixed amount (0.2g/L) into the water tank.[15] Note that, the concentration is a little bit higher due to the smaller amount of water at the beginning of our simulation. Ideally, the concentration of chlorine can be maintained at a safe range. However, in addition to the nature decay of chlorine, the concentration changes with the amount of water in the tank. The controller needs to adjust the amount of chlorine to be injected into the tank. In general, the controller takes the 'current concentra- tion of residual chlorine in water' and the 'amount of water in tank' as parameters, and calculates the proper amount of chlorine to be injected. This is so called a close-loop control mechanism.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 1, Issue 1, November 2012 | A Monthly Peer Reviewed & Referred Journal |

In such a control mechanism, the sensors placed at the water tank are in charge of collecting the concentration of chlorine in water. The sensing data (*y*, concentration) is fed back to a controller in the PCS. The controller then controls the actuators by sending a control signal (*u*) to add a proper amount of chlorine to the tank after a specific period of time. (Note that, chlorine in water decays with time.)[16]

The following paragraphs describe the possible integrity and DoS attacks to the system controlling the concentra- tion of residual chlorine in water.

- Integrity attack

Once if the sensing data (the solid line) is altered (*y* *y*ˆ), the controller may give wrong commands (*u*ˆ) to the actuators and add improper amount of chlo- rine to water (much higher or much less than 0.2g/L). Then, the integrity of the sensing data is damaged and the attack results in either overdosed residual chlorine in water (¿ 0.6 g/L), or non-drinkable water.

- DoS attack

If the sensing data (the solid line) is dropped (*y* *φ*), the controller receives nothing and may enter a unknown state. If a default concentration of 0.2 g/L is configured to handle such a situation, the damage to the whole water system and the public may be limited, but the operational cost may increase (since more chlorine may be injected into the tank). If no default handler is configured for handling the missing signals, the water system may become unstable and produce unexpected results.The nature of decay of chlorine, the concentration changes with the amount of water in the tank. The controller needs to adjust the amount of chlorine to be injected into the tank. In general, the controller takes the 'current concentra- tion of residual chlorine in water' and the 'amount of water in tank' as parameters, and calculates the proper amount of chlorine to be injected. This is so called a close-loop control mechanism.

In such a control mechanism, the sensors placed at the water tank are in charge of collecting the concentration of chlorine in water. The sensing data (*y*, concentration) is fed back to a controller in the PCS. The controller then controls the actuators by sending a control signal (*u*) to add a proper amount of chlorine to the tank after a specific period of time. (Note that, chlorine in water decays with time.)

The following paragraphs describe the possible integrity and DoS attacks to the system controlling the concentra- tion of residual chlorine in water.

- Integrity attack

Once if the sensing data (the solid line) is altered (*y* *y*ˆ), the controller may give wrong commands (*u*ˆ) to the actuators and add improper amount of chlo- rine to water (much higher or much less than 0.2g/L). Then, the integrity of the sensing data is damaged and the attack results in either overdosed residual chlorine in water (¿ 0.6 g/L), or non-drinkable water.

- DoS attack

If the sensing data (the solid line) is dropped (*y* *φ*), the controller receives nothing and may enter a unknown state. If a default concentration of 0.2 g/L[15]

V. CONCLUSION AND FUTURE WORK

Advanced of the modern network and information technologies, control systems can be used to monitor and control critical infrastructure assets (power grid, water treatment, and transportation management). Most of these infrastructures are safety-critical, an attack can greatly impact the public, the environment, and may lead to the loss of human life. Since modern control systems leverage the contemporary information technologies, the existing computer attacks are also applied to the control systems and made the control systems vulnerable to cyber- attacks. The increased risk of these attacks thus has led to numerous investigations of control system security.

In this paper, we investigate the security of a water system, and explain how an attack on the control system may result in a harmful state in the water system. The factors influence water quality are numerous. Taking the concentration of the chemicals in water as an example, a water company aims to maintain the concentration of the chemicals at a certain range to guarantee the water quality. By adopting a automatic PCS in a water system, the water company can precisely control water quality. Moreover, the water company also needs to design and investigate protection mechanisms to secure the PCS, and detect the intrusion in real time, so that the company can keep the water system stable, safe and secure. When considering the possible cyber-attacks, formalizing a PCS seems a good way to provide a systematic analysis of the attacking behaviours and the consequences of these attacks. The paper overviews the security control of a physical system (taking water system as an example). We first present the importance of a PCS for a physical system, and then address the reason to adopt a protection mechanism to secure the PCS in the physical system. Our future research will attempt to develop a formal model describing a *n*-tank water system and evaluate the impact of simultaneous attacks by conducting a series of experiments. Furthermore, we will also try to design a detection and defence system to resist against the known attacks.[16]

ACKNOWLEDGEMENTS

This effort was partially supported by the department of Agriculture Chemistry RBS College Agra.

REFERENCES

1. "water treatment." [Online]. Available: http://en.wikipedia.org/ wiki/Water purification
2. "general schema of water treatment systems." [Online]. Available: http://www.sandiego.gov/water/quality/treatmentprocess.shtml
3. "Water quality." [Online]. Available: http://en.wikipedia.org/wiki/ Water quality
4. "Turbidity." [Online]. Available: http://en.wikipedia.org/wiki/ Turbidity
5. G. Cembrano, G. Wells, J. Quevedo, R. Pe´rez, and R. Argelaguet, "Optimal control of a water distribution network in a supervisory control system," Control Engineering Practice, vol. 8, no. 10, pp. 1177–1188, 2000.
6. J. Dudley, G. Dillon, and L. Rietveld, "Water treatment simulators," Aqua- Journal of Water Supply: Research and Technology, vol. 58, no. 1, pp. 13–21, 2008.
7. R. Head, D. Shepherd, G. Butt, and G. Buck, "OTTER mathemat- ical process simulation of potable water treatment," Water Supply, vol. 2, no. 1, pp. 95–101, 2002.
8. van der Helm and L. Rietveld, "Modelling of drinking water treatment processes within the Stimela environment," Innovations in Conventional and Advanced Water Treatment Processes, vol. 2, no. 1, pp. 87–93, 2002.
9. "Hydromantis." [Online]. Available: www.hydromantis.com/ WatPro.html
10. L. Rossman, R. Clark, and W. Grayman, "Modeling chlo- rine residuals in drinking-water distribution systems," Journal of environmental engineering, vol. 120, no. 4, pp. 803–820, 1994.
11. M. Zierolf, M. Polycarpou, and J. Uber, "Development and autocal- ibration of an input-output model of chlorine transport in drinking water distribution systems," Control Systems Technology, IEEE Transactions on, vol. 6, no. 4, pp. 543 –553, jul 1998.
12. O. Ozdemir and A. Ucak, "Simulation of chlorine decay in drinking-water distribution systems," Journal of environmental engineering, vol. 128, p. 31, 2002.
13. M. Polycarpou, J. Uber, Z. Wang, F. Shang, and M. Brdys, "Feedback control of water quality," Control Systems Magazine, IEEE, vol. 22, no. 3, pp. 68 –87, jun 2002.
14. Z. Wang, M. Polycarpou, J. Uber, and F. Shang, "Adaptive control of water quality in water distribution networks," Control Systems Technology, IEEE Transactions on, vol. 14, no. 1, pp. 149 – 156, jan. 2006.
15. Ca´rdenas, S. Amin, and S. Sastry, "Secure control: Towards sur- vivable cyber-physical systems," in 28th International Conference on Distributed Computing Systems Workshops, 2008. ICDCS'08, 2008, pp. 495–500.
16. Ca´rdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in Proceedings of the 3rd conference on Hot topics in security. USENIX Association, 2008, p. 6.