Assessing the Effect of Cyber-Physical Attacks on Water Distribution Systems

R. Taormina[1]; S. Galelli, M.ASCE[1]; N. O. Tippenhauer[1]; A. Ostfeld, F.ASCE[2]; and E. Salomons[3]

[1]Singapore Univ. of Technology and Design, Singapore. E-mail: riccardo_taormina@sutd.edu.sg; stefano_galelli@sutd.edu.sg; nils_tippenhauer@sutd.edu.sg
[2]Technion - Israel Institute of Technology, Haifa, Israel. E-mail: ostfeld@tx.technion.ac.il
[3]Optiwater, Haifa, Israel. E-mail: selad@optiwater.com

Abstract

Modern water distribution systems (WDSs) largely depend on computer networks and industrial control systems for monitoring and operational purposes. Although the adoption of these cyber-physical components has improved the reliability and quality of service, such progressive computerization may render WDSs vulnerable to cyber and cyber-physical attacks. The spectrum of potential threats is very broad, with several attacks able to cause the disclosure of critical information or service disruption at different levels—a water supply interruption, for instance. These attacks usually target the supervisory control and data acquisition (SCADA) system—i.e., the centralized computer system supervising the whole infrastructure—or the programmable logic controllers (PLCs) that locally operate pumps and valves. In this work, we introduce an EPANET-based toolbox that allows simulating the effects of cyber-physical attacks on a WDS. Plausible attack scenarios to network SCADA and PLCs are implemented in EPANET to simulate the response of a large WDS and assess how it diverges from normal operating conditions.

INTRODUCTION

Modern Water Distribution Systems (WDS) are being increasingly supervised by complex networked control systems that rely on internet-connected devices. Although these solutions provide higher reliability at lower costs, their deployment exposes WDSs to novel security vulnerabilities with respect to their traditional hard-wired counterparts (Gao, 2013). As for other critical infrastructures, the threat of cyber-attacks to WDSs represent a major concern. The US Department of Homeland Security reported that 15 percent of the responses to cyber-incidents were in the water sector for the fiscal year 2012 (ISC-CERT, 2012). Those attacks usually target the Supervisory Control and Data Acquisition (SCADA) system and the Programmable Logic Controllers (PLCs) that locally operate pumps and valves (Amin et al., 2013a; Liu et al., 2011; Xie et al., 2010; Kosut et al., 2010). Security against such attacks can be increased through additional measures on the sensors, network, and SCADA layers (Anderson, 2008). However, a fundamental problem remains: sensors readings rely on physical layer properties that can be manipulated, in addition the sensor readings are susceptible to manipulations on the cyber layer. Furthermore, these infrastructures are typically operated for extended periods of time, so there are higher chances that one or multiple components are attacked during their life cycle.

We consider Cyber-Physical Attacks (CPA), which include both physical and cyber-attacks that target the WDS. Although both hydraulic (e.g., water spillage, tank overflow, pipe

bursts, loss of pressure) and water quality processes (e.g., pollution with chemical or metals, biological matter) should be considered (Abrams and Weiss, 2008), this study is concerned only with the former typology. Complex process-based models are needed to understand the effects of cyber-physical attacks on a WDS, in order to assess its robustness, resilience and vulnerability under attack scenarios. This is a novel field of research, and only few studies have tackled the problem of understanding the effect of cyber-attacks on complex water systems. Notable examples are available for the detection and isolation of attacks on a water network comprised of cascaded, gravity-flow canal pools (Amin et al., 2013a,b).

In this work, we discuss the use of EPANET (version 2.0) for modeling the effects of malicious attacks on WDSs. In particular, we describe a novel MATLAB-based toolbox (EPANET-CPA), which enables the simulation of attack scenarios by overriding the control logic governing the EPANET simulations. In the remainder of the paper we first describe a set of possible cyber-physical attacks to WDS that can be modeled by the EPANET-CPA toolbox (Section 2). The toolbox itself is described in Section 3, while some examples of attacks to WDS hydraulics are presented in Section 4. Concluding remarks are given in Section 5.

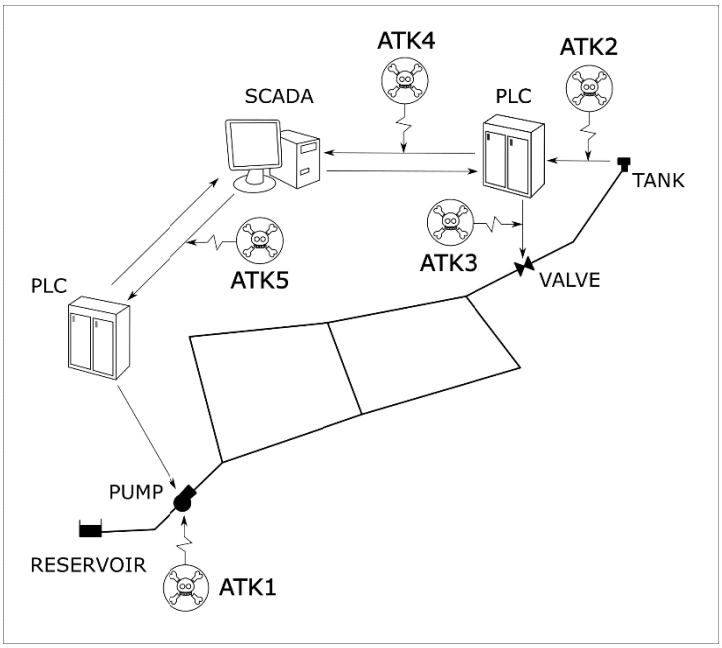

Figure 1. Examples of possible cyber-physical attacks to WDS.

CYBER-PHYSICAL ATTACKS ON WDS

The scheme in Fig. 1 shows a range of CPA that an adversary can perform against a WDS. The minimal network represented has a pump that feeds water from a reservoir to the demand nodes and a storage tank. The water level in the storage tank is used to control pump operations, as well as the opening/closing of the valve that links it to the network. The two actionable components are controlled by two separate PLCs that communicate with the SCADA system. The pumping schedule is decided at SCADA level based on nodal demands and water level in the tank. Five generic CPA scenarios are illustrated. ATK1 represents a physical attack to a WDS component (the pump in this case) that the adversary can perpetrate only by having physical access to the

system. ATK2-5 are instead representative of cyber-attacks aimed at the communication between sensors, controllers and actionable components in the WDS.

In general, we differentiate between *passive* and *active attacks* (Anderson, 2008). In passive attacks, the adversary is interested in *eavesdropping* the communication in order to gain knowledge on 1) a particular component, 2) process dynamics from sensor readings (ATK2), 3) the nature of the information exchanged between controller and actuators (ATK3), or 4) the nature of information exchanged between PLC and SCADAs (ATK4-ATK5). The possibility of direct exchange between remote PLCs is not considered in this example.

In the active setting the attacker interferes with communication and WDS components to different extents. Simple attacks are aimed at just disabling a component or disrupting the communication. Although easier to perpetrate, simple attacks are also easier to detect and bear lower impact on the attacked system. On the other hand, advanced attacks that change content or timing of the exchanged messages can be devised if the adversary has gained some insights on the system. Since these threats are more difficult to detect, they carry more disruptive potential.

Active attacks can have different effects, we differentiate between *denial-of-service* (DoS) attacks targeting system availability, and *deception attacks* targeting data authenticity (Amin et al., 2013a). In DoS attacks, the attacker effectively prevents communication between two victim devices (e.g. by injecting extraneous data, or jamming the communication channel). In deception attacks, the attacker manipulates exchanged data, or transmits own additional data with forged source (e.g., with altered sensor measurements, control inputs, or wrong time stamps). Using this nomenclature, some examples of active attacks can be illustrated on the WDS of Fig. 1:

- ATK1: the attacker manually deactivates the pump to disconnect the network from the reservoir.

- ATK2: the attacker perpetrates a deception attack by altering the readings transmitted by the water level sensor in the tank. This will affect both the PLC controller and SCADA pumping scheduling.

- ATK3: the attacker carries out a DoS attack by preventing communication between PLC and the valve actuator. The attack prevents the valve from opening/closing according to PLC requests.

- ATK4: the attacker deceives the SCADA system by manipulating the readings of tank water level as transmitted by PLC. This decouples pump scheduling from actual tank water level.

- ATK5: the attacker launches a DoS attack on the PLC, such that it cannot acknowledge SCADA rescheduling of pump operations.

THE EPANET-CPA TOOLBOX

Our toolbox allows the simulation of the threats described in the previous section. This MATLAB toolbox interfaces with the public-domain EPANET 2.0 developer toolkit (Rossman,

1999, 2000) to provide reliable representation of cyber-physical attacks. EPANET is the de facto industry standard for hydraulic and water quality behavior simulations within pressurized pipe networks. EPANET accurately reproduces WDS dynamics by employing a sophisticated network model and two engines for hydraulics and water-quality simulation. EPANET features *physical* components for designing the network topology and *non-physical* components to define its operations. The network is designed using *junctions*, *reservoirs*, *tanks*, *pipes*, *valves* and *pumps*, while operations are specified by means of *curves*, *time patterns* and *controls*.

EPANET controls are statements that determine the behavior of selected links — pumps and valves — as a function of time or the value of some nodal variables, i.e. pressure at junctions or water level in storage tanks. These statements represent the logic governing the WDS at both PLC and SCADA layer, thus the EPANET-CPA toolbox is able to simulate attack scenarios by overriding the controls operating the WDS under normal conditions. This procedure is carried out by running the simulation in a step-by-step fashion and interposing the attacker constructs between consecutive steps of the simulation.

Although EPANET cannot directly model tank overflows, the EPANET-CPA toolbox allows this by automatically modifying the original network. This is done by 1) duplicating the original pipe connecting the tank to the network, 2) connecting this additional pipe (NEWLINK) to a dummy storage tank, and 3) including controls that keep the link closed unless the level in the original tank reaches the maximum water level. The amount of overflow due to the attack is therefore equal to the amount of water stored in the dummy tank at the end of the attack, or to the volume of water that flows through NEWLINK during the attack.

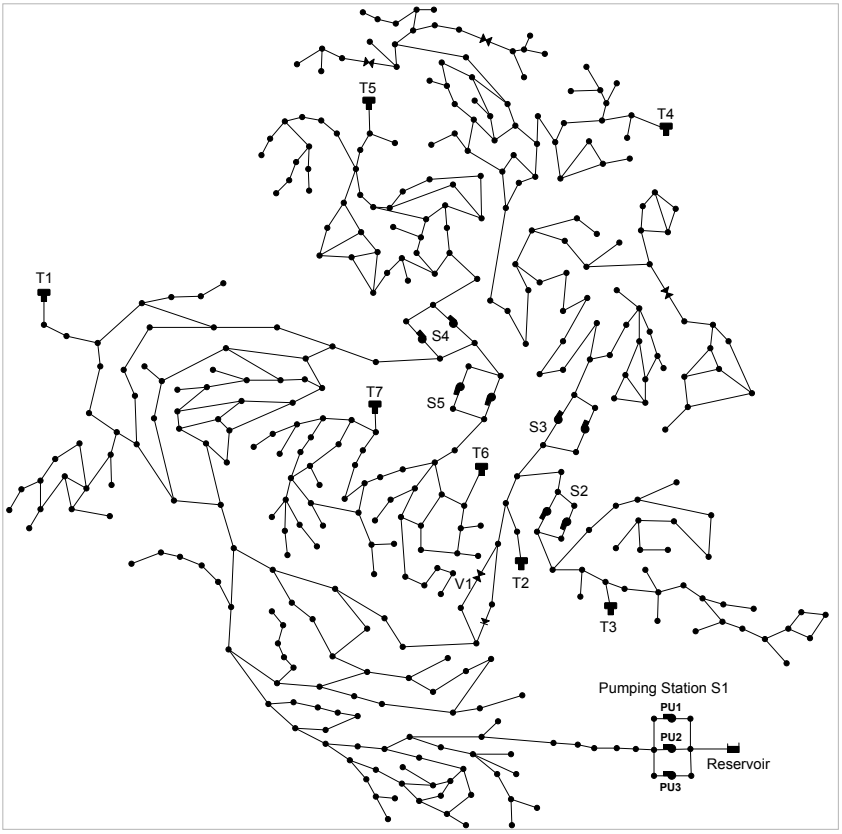

Figure 2. The C-TOWN network.

SIMULATION OF CPA SCENARIOS

The C-TOWN Network. The C-Town benchmark WDS (Giustolisi et al., 2015) depicted in Figure 2 is based on a real-world medium-sized network with a total of 388 nodes and 429 links. C-Town has two main storage tanks (T1 and T2), and a main pumping station S1. The operations of pumps PU1 and PU2 in S1 are regulated by the water levels in T1, while PU3 is a redundant pump that is kept off during standard operating conditions. The remaining five tanks are refilled by four secondary booster stations that pump water from T1 and T2. The secondary branch pertaining to T2 is connected to the reservoir through valve V1, which is controlled by the water level in T2.

Example 1: Overflow of T1 via deception attack on water level sensor. This first example shows the effect of a deception attack of type ATK2 (see Fig. 1) where the adversary causes T1 to overflow by manipulating the water level sensor readings received by the PLC commanding pumping station S1. This scenario assumes that there is no additional overflow sensor in the tank or that it has been deactivated by the attacker. In normal conditions, the pumps PU1 and PU2 are deactivated when the water level is below 6.3 meters and 4.5 meters, respectively. The attack consists in tampering with the readings of the water level in T1 so that the value transmitted to the PLC is always below 4.5 meters. In this way, PU1 and PU2 keep pumping water to the system causing T1 to overflow when the level rises above its maximum level of 6.5 meters. The results of the attack are illustrated in Figure 3. It can be seen (right side) that at some point during the simulation the real water levels measured by the sensor (red line) diverge from those received by the PLC (black line) following the attacker intervention. Due to the system inertia and prior state, it takes around 10 hours for the attack to drive the system outside its normal regime, while almost 2 days are needed to cause T1 to overflow.

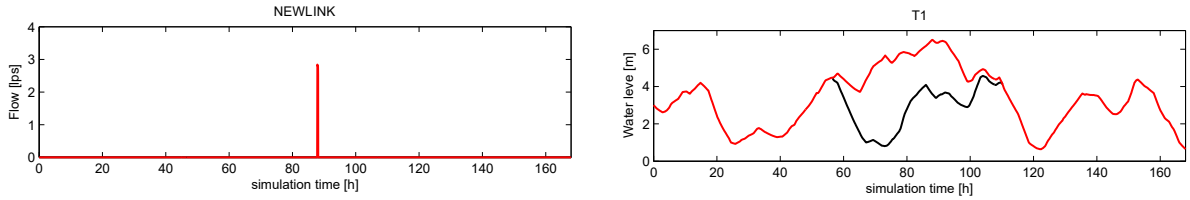

Figure 3. Example 1: Water overflow through NEWLINK (left). Water level in T1 (right). The red line shows the real readings of water level sensor in T1, while the black line shows the manipulated readings received by PLC during the attack.

Example 2: Overflow of T2 via DoS attack. Overflow in T2 occurs if the valve V1 connecting it to the main line of the network is forced to stay open for a sufficient amount of time. Under normal conditions, the controller operates V1 so that it shuts down when the water level in T2 rises above 5.3 meters, which is 0.6 meters below the maximum level of 5.9 meters for this tank. In this example, a DoS attack of type ATK3 (see Fig. 1) prevents the reception of the CLOSE signal from the PLC at V1, which as result remains open. The effects of this attack are shown in Figure 4. This time, the PLC (and the SCADA consequently) receives the correct reading from the water level sensor in T2 (red line), but it fails to operate the valve. Repeated overflows

therefore occur shortly after the attack occurs. The black line shows the water levels that would have been recorded for the "no attack" scenario under the same initial conditions.

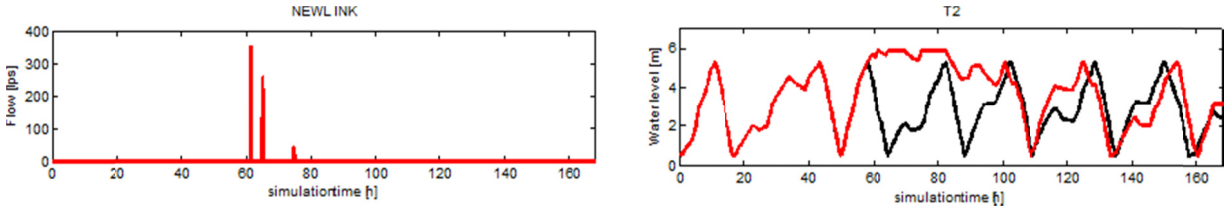

Figure 4. Example 2: Water overflow through NEWLINK (left). Water level in T2 (right) during normal operations (black line) and under attack (red line).

SUMMARY AND FURTHER DEVELOPMENTS

In this work, we discussed the use of our EPANET-based toolbox that allows us to simulate CPA attacks to WDS. Two examples of attacks were presented, in which storage tanks were forced to overflow by both a deception attack and a DoS attack. The analysis of the two cases shows that the EPANET-CPA toolbox can be a valuable tool to help researcher and practitioners assess the effects of CPA on WDS. Furthermore, the attack scenarios modeled by the toolbox can be employed to devise attack detection algorithms for real-time monitoring of the physical layer. Further research is needed to extend the toolbox capabilities as to model threats concerning water quality and the injection of hazardous substances in the WDS.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation (NRF), Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-40), by the Chief Scientist (OCS) Ministry of Science, Technology and Space (MOST), and by the Germany Federal Ministry of Education and Research (BMBF), under project no. 02WA1298.

REFERENCES

Abrams, M. and Weiss, J. (2008). “Malicious Control System Cyber Security Attack Case Study— Maroochy Water Services, Australia.” McLean, VA: The MITRE Corporation.

Anderson, R. (2008). Security engineering. John Wiley & Sons.

Amin, S., Litrico, X., Sastry, S., and Bayen, A. M. (2013a). “Cyber Security of Water SCADA Systems — Part I: Analysis and experimentation of Stealthy Deception Attacks." *IEEE T. Contr. Syst. T.,* 21(5), 1963-1970.

Amin, S., Litrico, X., Sastry, S., and Bayen, A. M. (2013b). “Cyber Security of Water SCADA Systems — Part II: Attack Detection Using Enhanced Hydrodynamic Models." *IEEE T. Contr. Syst. T.,* 21(5), 1679-1693.

Gao, W. (2013). “Cyberthreats, Attacks and Intrusion Detection in Supervisory Control and Data Acquisition Networks". PhD thesis, Mississippi State University.

Giustolisi, O., Berardi, L., Laucelli, D., Savic, D., and Kapelan, Z. (2015). "Operational and Tactical Management of Water and Energy Resources in Pressurized Systems: Competition at WDSA 2014." *J. Water Res. PL.-ASCE*, C4015002.

Kosut, O., Jia, L., Thomas, R. J., and Tong, L. (2010). "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures." Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, IEEE. 220-225.

Liu, Y., Ning, P., and Reiter, M. K. (2011). "False Data Injection Attacks Against State Estimation in Electric Power Grids." ACM Transactions on Information and System Security (TISSEC), 14(1), 13.

ISC-CERT (2012). "Malware Infections in the Control Environment." ICS-CERT Monitor, 1-15.

Rossman, L. A. (1999). "The EPANET Programmer's Toolkit for Analysis of Water Distribution Systems." *Proc., Conf. on Water Res. Plan. and Manag.*, 39-48.

Rossman, L. A. (2000). "EPANET 2: Users Manual."

Xie, L., Mo, Y., and Sinopoli, B. (2010). "False Data Injection Attacks in Electricity Markets." Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, IEEE. 226-231.