Characterizing Cyber-Physical Attacks on Water Distribution Systems

Riccardo Taormina[1]; Stefano Galelli, M.ASCE[2]; Nils Ole Tippenhauer[3]; Elad Salomons[4]; and Avi Ostfeld, F.ASCE[5]

Abstract: This work contributes a modeling framework to characterize the effect of cyber-physical attacks (CPAs) on the hydraulic behavior of water distribution systems. The framework consists of an attack model and a *MATLAB* toolbox named *epanetCPA*. The former identifies the components of the cyber infrastructure (e.g., sensors or programmable logic controllers) that are potentially vulnerable to attacks, whereas the latter allows determining the exact specifications of an attack (e.g., timing or duration) and simulating it with *EPANET*. The framework is applied to C-Town network for a broad range of illustrative attack scenarios. Results show that the hydraulic response of the network to a cyber-physical attack depends not only on the attack specifications, but also on the system initial conditions and demand at the junctions. It is also found that the same hydraulic response can be obtained by implementing completely different attacks. This has some important implications on the design of attack detection mechanisms, which should identify anomalous behaviors in a water network as well as the cyber components being hacked. Finally, the manuscript presents some ideas regarding the next steps needed to thoroughly assess the risk of cyber attacks on water distribution systems. **DOI: 10.1061/(ASCE)WR.1943-5452.0000749.**

Author keywords: Water distribution systems; Cyber-physical systems; Cyber-physical attacks; Cyber security; *EPANET*; Smart water networks.

Introduction

Cyber-physical systems (CPSs) are defined as the combination of physical processes with computation and networking. In a CPS, embedded networking devices monitor and control the physical processes, usually in a real-time fashion, with regular feedback interactions between the cyber and physical spaces of the system (Lee 2008). CPSs are steadily replacing existing infrastructures in different domains (e.g., energy, transportation, and manufacturing) due to their enhanced performance granted by advanced design and superior level of abstraction. The breakthrough represented by CPS and other new technologies such as the Internet of Things and the Internet of Service (Atzori et al. 2010) has induced experts to collectively term these new paradigms as the *fourth industrial revolution* (Schwab 2016).

Similar transformations are ongoing in the water supply sector, involving a broad range of critical infrastructures, such as reservoirs (Bobat et al. 2015), water and wastewater treatment plants (Spellman 2013), and water distribution systems—or *smart water networks*. The latter are CPS built on the interaction between physical water assets and networked devices designed to monitor, operate, and supervise all physical processes in the distribution system. These devices include sensor networks (Ostfeld et al. 2008; Hart and Murray 2010), mobile sensors (Gong et al. 2016), and smart meters (Cominola et al. 2015), for instance. Two additional key components of smart water networks are arguably the programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) system. Programmable logic controllers are embedded devices connected to sensors and actuators for data handling and process control purposes, wheras a SCADA is a centralized computer employed to supervise the operations of the entire infrastructure, as well as to store and analyze real-time process data.

While these networked devices grant modern water distribution systems superior reliability, autonomy, and efficiency, they expose both physical and cyber infrastructures to cyber-physical attacks (CPAs), as noted by a recent editorial (Rasekh et al. 2016). In particular, such attacks can range from the accessing of private consumer or operational information to intentional damage to the physical water assets (pumps, valves, tanks), decreases of water supply, and even impacts on water quality. The safety-critical role played by water distribution systems makes them attractive targets for terrorism and cyber warfare (Lewis 2002; Horta 2007; Dakin et al. 2009), thus raising concerns regarding their vulnerability and potential damages to economies and local communities. One of the first attacks in the water supply sector occurred in 2000 at Maroochy Water Services (Queensland, Australia), where a disgruntled contractor attacked the SCADA of a sewage system releasing almost 1 million liters of wastewater into waterways and parks (Slay and Miller 2008). Since then, cyber-physical attacks

[1]Postdoctoral Research Fellow, iTrust Centre for Research in Cyber Security, Singapore Univ. of Technology and Design, 8 Somapah Rd., Singapore 487372 (corresponding author). E-mail: riccardo_taormina@sutd.edu.sg

[2]Assistant Professor, Pillar of Engineering Systems and Design, Singapore Univ. of Technology and Design, 8 Somapah Rd., Singapore 487372. E-mail: stefano_galelli@sutd.edu.sg

[3]Assistant Professor, Pillar of Information Systems Technology and Design, Singapore Univ. of Technology and Design, 8 Somapah Rd., Singapore 487372. E-mail: nils_tippenhauer@sutd.edu.sg

[4]Consultant, OptiWater, 6 Amikam Israel St., Haifa 3438561, Israel. E-mail: selad@optiwater.com

[5]Professor, Faculty of Civil and Environmental Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel. E-mail: ostfeld@tx.technion.ac.il

Note. This manuscript was submitted on July 14, 2016; approved on October 19, 2016; published online on February 7, 2017. Discussion period open until July 7, 2017; separate discussions must be submitted for individual papers. This paper is part of the ***Journal of Water Resources Planning and Management***, © ASCE, ISSN 0733-9496.

have been steadily increasing. According to the United States' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT 2014), several cyber-physical attacks have already occurred against United States water utilities. Remedial actions are being taken at both national and international level; the United States EPA has been explicitly addressing cyber threats for a period of at least five years (EPA 2011), while international partnerships between water/environmental agencies have been recently launched (Ackerman 2015).

Research in the water supply sector focused mostly on water/wastewater treatment plants (Spellman 2013) and automated canal networks (Amin et al. 2013a, b), with almost no emphasis on water distribution systems. To the authors' knowledge, only Perelman and Amin (2014) presented an approach to assess the vulnerability of water networks. There is a lack of analytical and computational tools that merge models of the physical processes, control, and communication systems. Such tools are required to characterize the response of distribution systems to adversary attacks, and are thus needed to assess vulnerabilities and design adequate countermeasures. This work represents a first step toward a simulation-based approach for the assessment of the risks associated to cyber-physical attacks on water distribution systems. The authors start by considering the hydraulic response of water networks, and present a modeling framework consisting of two main components, namely an *attack model* that characterizes a broad range of attacks on cyber components (e.g., sensors, PLCs, and SCADA) and a *MATLAB* toolbox (named *epanetCPA*) that automatically implements in *EPANET* all attacks based on the attack model. The proposed framework can be seamlessly extended to model attacks aimed at disrupting the infrastructure, affecting water quality or thwarting emergency responses.

The remainder of the paper is organized as follows. The following section outlines the security goals of CPS, the attack model, and *epanetCPA* toolbox. Section "Experimental Setup" presents the experimental setup of this study. The setup includes a medium-sized water distribution network, the attacks specifications, and three indices to quantify the hydraulic response of the network under different cyber-physical attacks. Results are presented and discussed in the "Results" section. Extensions of this work to enable risk assessment and conclusions are given in the "Toward Simulation-Based Risk Assessment" and "Conclusions" sections, respectively.

Modeling Framework

Security Goals and Cyber-Physical Attacks

The purpose of a water distribution system is to fulfill customers demand while ensuring appropriate quality of the delivered water. When analyzing a water distribution system from a cyber-security perspective, one has to consider the security goals along with the traditional operational goals of the distribution network. In information security, classic security properties for systems are *integrity*, *availability*, and *confidentiality*. Those properties were translated to CPS by Cardenas et al. (2008) as follows. Operational integrity implies that system resources and the data shared between them are not manipulated by an attacker, while availability entails that the system is ready for use upon demand. Confidentiality relates to keeping the status of the physical system and other sensitive information secret from unauthorized users—access to sensitive information not only violates end-users' privacy, such as in the case of smart meters (Cominola et al. 2015), but is also a potential gateway to the design of complex attacks aimed at damaging the physical infrastructure. In synthesis, the security goals can be interpreted as the ability of the system to fulfill its operational goals by preventing, detecting, or surviving cyber attacks (Cardenas et al. 2008).

Each security goal can be targeted by a specific type of cyber-physical attack. An adversary may compromise integrity with *deception* attacks by manipulating the information sent or received by sensors, actuators, or controllers. Such attacks are commonly achieved by compromise of one of the involved devices, or a man-in-the-middle attack on the communications (Urbina et al. 2016). As result of such an attack, an actuator within a CPS may change its operations after receiving manipulated data believed true, thus allowing the adversary to lead the physical system to a desired state. Alternatively, the attacker can render the system unavailable with *denial of service* (DoS) attacks (Krotofil et al. 2014) by preventing sensors to send data, the controllers from receiving data and issuing commands, or the actuators from receiving commands and executing actions. DoS attacks can be achieved in various ways, e.g., by jamming wireless channels, flooding wired channels with additional traffic, or overloading PLC or SCADA systems with additional requests. Confidentiality is threatened by *eavesdropping* attacks, e.g., by an adversary who manages to tap the communication channels and sniff the transmitted packages to gain information on the system state and behavior.

Attack Model

The security goals and types of cyber-physical attacks previously described are used to devise an attack model for water distribution systems. The goal of the attack model is to define: (1) the elements of the cyber and physical space that can be attacked; and (2) the type of attacks they might be subject to. A graphical representation of the attack model is given in Fig. 1 for a simple distribution network consisting of one pump, one valve, one tank, and a few demand nodes. The attack model lists nine attacks—classified on the basis of the type of element being attacked—that target sensors, actuators, PLCs, and SCADA, as well as the communication links connecting them. Following the numbering of Fig. 1, the types of attacks are as follows:

- ATK1: Physical attack to a sensor. In order to perform this attack the attacker is supposed to have direct physical access to a sensor, such as the water level sensor in Fig. 1, which can be damaged, manipulated, or replaced. As a consequence of this attack, the PLC connected to the sensor (e.g., PLC1) may receive NULL or altered readings that compromise controlling operations (e.g., settings of the valve and/or pump), thereby causing a deception or denial of service;
- ATK2: Physical attack to an actuator. Similarly to ATK1, ATK2 is based on the physical access to a system component—an actuator, in this case. The adversary may damage, activate/deactivate the actuator, or change its operational settings, such as the pump speed in Fig. 1. Such attacks can cause a DoS, or compromise the operational integrity of the system. While ATK1 and ATK2 might be unlikely and not be perceived as cyber attacks, they are included in the model for the sake of completeness, for example to consider the case of an actuator in a remote (or poorly monitored) area that was physically accessible to an attacker;
- ATK3: Attack to the connection link between sensor and PLC. The link between these two components is represented by a wireless connection, or a hardwire. The type of connection link determines whether the attacker needs physical access to the sensor to perpetrate its actions. These actions include denial of service (to interrupt the connection), manipulation of the data packages being sent to the PLC, and eavesdropping (to get information on the system state);

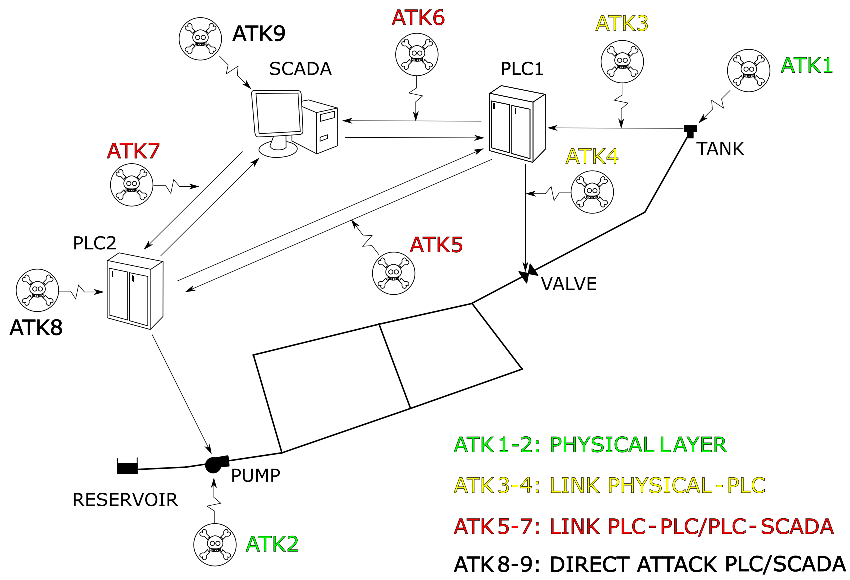

Fig. 1. Graphical representation of the attack model; the attacks are categorized depending on their target component/communication link

- ATK4: Attack to connection link between PLC and controlled actuator. The considerations made for ATK3 regarding the nature of the connection link still hold for this attack. In this case, the adversary physically or remotely interrupts the connection between the PLC and controlled component, such as the valve in Fig. 1, which fails to acknowledge new control signals (DoS). The attacker can also alter these control signals and directly control the actuator (deception). Such action may be anticipated by an eavesdropping attack aimed at gathering information about the signals transmitted by the PLC to the actuator;
- ATK5: Attack to the connection link between two PLCs. Programmable logic controllers are generally connected through a private network or internet to exchange information on the system state. For example, in Fig. 1 PLC1 gathers data from the tank water level sensor and transmits them to PLC2, which controls the pump on the basis of the tank water level. When this connection is intercepted and its content manipulated (deception), a disruption of normal pumping operations is caused. The adversary may also eavesdrop the communication or prevent PLC1 (PLC2) from sending (receiving) the updated sensor reading by flooding the communication channel with traffic (denial of service). As result of such attacks, different PLCs might have different readings from the same sensor. A model assumption is that the sensor reading sent to the SCADA originates from the PLC directly connected to the sensor itself. This applies unless one considers an interruption or manipulation of the communication between that PLC and SCADA, as described in the next attack scenario;
- ATK6: Attack to the connecting link between PLC and SCADA. The PLC-to-SCADA communication (usually established via a private network or the Internet) is manipulated, eavesdropped, or temporarily interrupted by flooding the communication channel. As a result, incomplete or wrong key information on the system state (e.g., the tank water level in Fig. 1) reaches the SCADA. The adversary might resort to this attack to conceal other actions from human operators or event detection algorithms implemented at SCADA level;
- ATK7: Attack on the connecting link between SCADA and PLC. This attack represents the dual of ATK6. In this attack, the signals sent by the SCADA to a PLC are blocked (DoS), manipulated (in a deception attack), or eavesdropped by the adversary. In Fig. 1, for instance, the attacker resorts to ATK7 to prevent PLC2 from receiving a new pumping schedule or to manipulate the reference tank water levels that determine the pump activation/deactivation;
- ATK8: Attack on the PLC. With this attack, the adversary has direct control of a PLC in the network. Depending on the level of control gained, the attacker may completely stop normal operations of the controlled process (DoS), manipulate the control logic in the PLC (deception), or deliberately report incorrect data to the SCADA. Although ATK8 is related to some of the attacks previously described (e.g., ATK6 and ATK7), this particular attack is generally more persistent. A compromised PLC must be assumed to be under control of the attacker until the attack is detected and restored. In contrast, the other attacks are usually characterized by an intermittent behavior that requires constant interaction by the attacker; and
- ATK9: Attack on SCADA. This attack represents a situation in which the attacker has compromised the SCADA system, either through a local or remote attack. This family of attacks is included in the model for the sake of completeness, but it is not considered in the remainder of this study because ultimately a compromised SCADA system cannot be detected (because the detection happens in the SCADA layer), and is able to arbitrarily change any system configuration, and obtain all data measured by sensors. As such, the attacker is assumed to be successful as soon as ATK9 is achieved.

While the attack model univocally categorizes the attacks a water distribution system may be subject to, a further modeling step is necessary to determine the exact specifications of an attack. For example, the start and end times, or the number of components being attacked need to be specified. An adversary may perform multiple attacks in sequence or target several components at the same time. For instance, the attacker might first eavesdrop a communication channel to later perform a more sophisticated deception on the same line, or conceal the outcomes of an attack to the physical system by simultaneously carrying out another one to the SCADA. All specifications are modeled and implemented in the toolbox described next.

EpanetCPA Toolbox

The *epanetCPA* toolbox extends the features of *EPANET* (version 2.0.12) to the realm of cyber-physical security, allowing users to design multiple attacks and reproduce their effects on the operations and dynamics of water distribution systems (Taormina et al. 2016). The toolbox operates by running *EPANET* hydraulics simulation engine in a step-by-step fashion while overriding the original control logic to enable potential adversary actions. In *epanetCPA* users are required to first specify the cyber layer related to the physical process network map. In particular, the following information is required: (1) number and locations of PLCs deployed in the network; (2) connections between PLCs and sensors/actuators; (3) distributed control statements among PLCs (based on the actuators they control); and (4) data flow between PLCs. A SCADA is also introduced on top of the PLC hierarchy, under the assumption that the status of a sensor at SCADA level matches the one of the PLC directly connected to the sensor, unless the corresponding PLC-SCADA connection is attacked. During the simulation, the software stores the simulation outputs that reflect the status of the physical layer. The toolbox also keeps track of altered readings at PLC and SCADA level in case attacks involving sensor and signals manipulation are simulated.

EpanetCPA is an object-oriented software where ATK1–ATK8 in Fig. 1 are implemented with specific classes. Specific attack instances are created from the class templates using customizing attributes. Such specifications include the identity of the component or connection link under attack and the statements defining attack initial and ending conditions, as well as details characterizing the particular action perpetrated by the adversary. The latter information defines whether the target is undergoing a physical, DoS, or deception attack. Eavesdropping attacks are not explicitly implemented because they do not affect the physical processes directly. However, *epanetCPA* implicitly accounts for eavesdropping by letting the user model DoS and deception attacks based on the amount of knowledge the attacker can infer by violating system confidentiality. For instance, the toolbox can equally reproduce the behavior of a naive adversary who jams a connection link randomly in time, and that of a more informed counterpart who can read the status of system components, and is able to time a DoS attack to maximize impact. In the same way, *epanetCPA* features deception attacks with increasing levels of sophistication based on the information previously gathered via eavesdropping.

EpanetCPA also implements some automatic workarounds that are necessary to reproduce the hydraulic response of a water distribution network to a cyber-physical attack. For instance tank overflows are not explicitly simulated by *EPANET*, so the toolbox preprocesses the original network map to amend for this shortcoming. This is done by (1) duplicating the original pipe connecting the tank to the network; (2) placing a dummy storage tank at the end of the duplicated pipe; (3) introducing a check-valve to prevent flow from the dummy tank to the network; and (4) including controls that keep the additional link closed unless the level in the original tank reaches the maximum capacity.

Experimental Setup

C-Town Network

The potential effects of cyber-physical attacks are demonstrated on the C-Town water distribution system, which is based on a real-world medium-sized network. This benchmark was introduced for the *Battle of the water calibration networks* (Ostfeld et al. 2012) and subsequently used for a variety of problems—e.g., leakage reduction (Saldarriaga et al. 2015) and optimal design and operation (Sousa et al. 2015; Creaco et al. 2015). Water storage and distribution across the demand nodes is guaranteed by seven tanks, whose water level triggers the operations of 11 pumps (see Table 1 for additional details on C-Town hydraulic components). As depicted in Fig. 2, pumps, valves, and tank water level sensors are connected to nine PLCs, which are located in the proximity of the hydraulic components they monitor/control. There is also a single SCADA system that collects the readings from all PLCs and coordinates the operations of the entire network. Table 2 reports the role played by each PLC, that is, the sensors they are connected to and the hydraulic actuators they control. Most of the PLCs controlling the pumps are not directly connected to the sensors employed in the control logic, but rather receive the necessary information via other PLCs. The hydraulic simulation is carried out with *EPANET*, with a simulation horizon and hydraulic time step of 7 days (168 h) and 1 h, respectively.

Table 1. Hydraulic Components of C-Town Water Distribution System

Hydraulic component	Number
Nodes	388
Pipes	429
Tanks	7
Pumps	11
Valves	4 (1 actionable)

Attack Specifications

Among the large numbers of attacks one could conceive, six *attack scenarios* have been designed to exemplify the potential effects of the attacks outlined by the attack model. All scenarios lead to a disruption of the system operations, such as overflow and low level conditions of the tanks. The level of disruption one can simulate is limited to a certain extent by *EPANET*'s demand-driven hydraulic engine; for instance, it is not possible to simulate pipe bursts or empty conditions of the tanks. The attack scenarios have the following specifications (see Table 3 for further details):

- Scenario 1: Tank overflow because of a direct attack to a booster station (unscheduled activation of pumps PU1 and PU2 leading to an overflow of tank T1). This action can be perpetrated if the attacker is physically at the pumping station (ATK2) or if the attacker alters the control signal sent by PLC1 (ATK4) by either switching the pumps on or preventing them from receiving a stop signal. Alternatively, the attacker may take control of PLC1 altogether and manipulate the activation signals at will (ATK8);
- Scenario 2: Low level in a tank because of manipulated water level readings. The water level readings in tank T2 are altered, thus preventing the tank from refilling. This can be obtained with a physical manipulation of the water level sensor (ATK1) or with an alteration of the communication link between the sensor and PLC3 (ATK3). A similar attack on tank T4 is also implemented (Scenario 2b). The difference between the two attacks is that in the former the low water level is a result of valve V1 closure, whereas in the latter it is a result of pumps PU6 and PU7 deactivation;
- Scenario 3: Tank overflow because of an alteration of PLC-to-PLC connection. This scenario exemplifies attack ATK5, where the attacker intercepts the PLC2-to-PLC1 connection and alters tank T1 water level readings, leading to the activation of pumps PU1 and PU2 with a consequent increase of tank T1 water level;
- Scenario 4: Concealment via replay attack on PLC-to-SCADA connection. Scenario 3 is complemented by an attack aimed

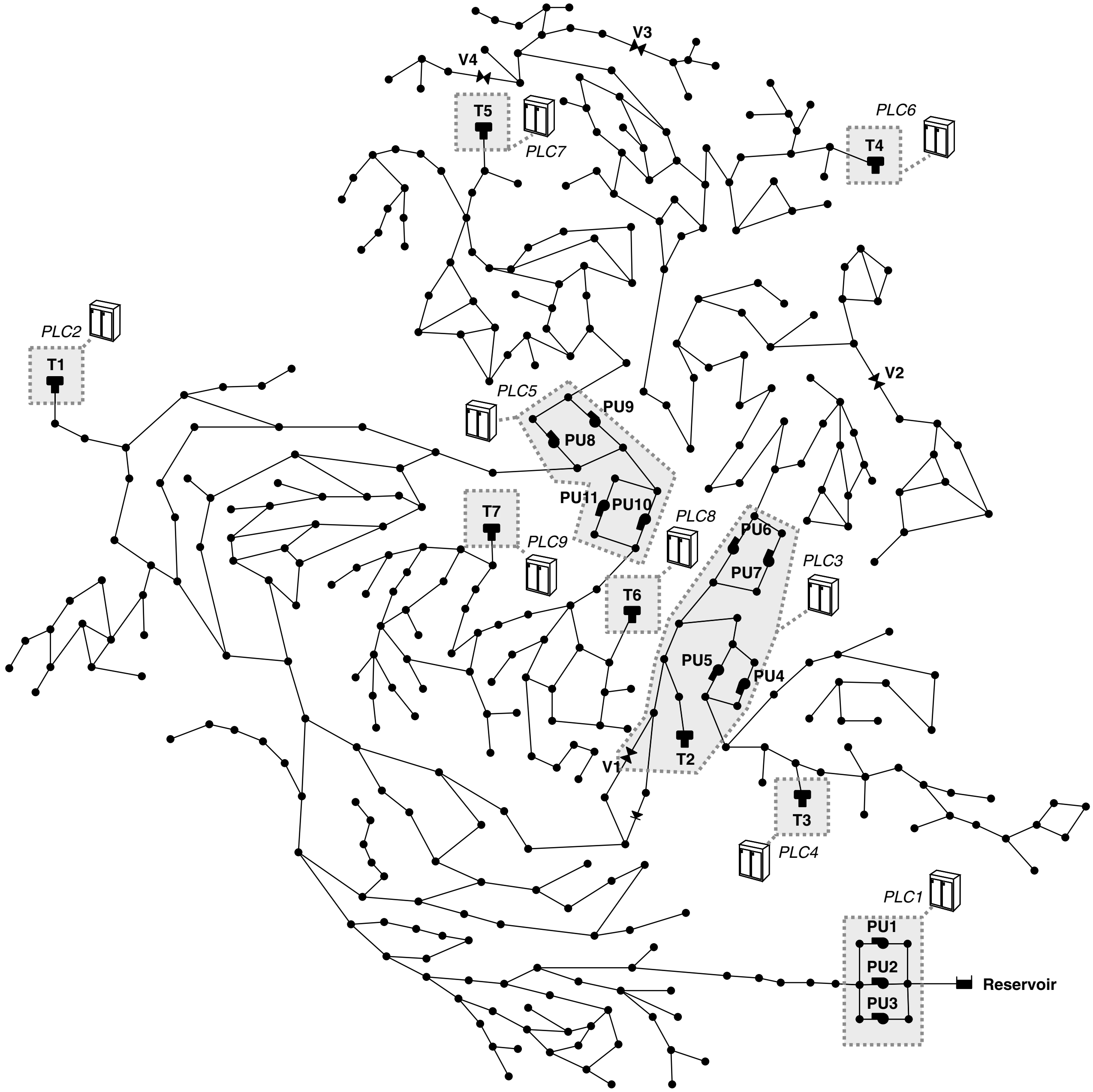

Fig. 2. Graphical representation of C-Town water distribution system

at concealing its effects from the SCADA. This is obtained by attacking the PLC2-to-SCADA communication link (ATK6);

- Scenario 5: Tank overflow due to wrong settings sent by SCADA. This attack scenario entails the alteration of the packages being sent by SCADA to change the operations of a PLC it supervises (ATK7). In particular, the communication link between SCADA and PLC5 is attacked, resulting in the activation of pump PU11 and overflow of tank T7; and
- Scenario 6: Random multiple attacks on PLC. This last experiment is aimed at causing an overflow of tanks T2, T3, and T4 by manipulating the water level readings arriving to PLC3, which controls all the actuators diverting water to these tanks. In particular, the manipulation is performed on the link between the T2 water level sensor and PLC3 (ATK3), as well as on two PLC-to-PLC communication links, i.e., PLC4-to-PLC3 and PLC6-to-PLC3 (ATK5), respectively.

Attack Scenarios 1–5 described previously are repeated 100 times by randomly varying the initial condition (e.g., tanks' water levels) and demands at the junctions of C-Town network. This combination of attack and hydraulic scenarios is used to quantify the impact of cyber-physical attacks using the indices described in the next section. Attack Scenario 6 is also repeated 100 times, although in this case the randomization is performed for the starting time and duration of each attack rather than the network initial condition and demands.

Impact Quantification Indices

Because the attack scenarios are primarily aimed at causing tanks overflow, low level conditions, and pumps malfunctioning, three indices are employed to quantify such effects across the different scenarios. These indices are not meant to exhaustively characterize

Table 2. Main Characteristics of C-Town PLCs

PLC[a]	Sensor	Actuators (controlling sensor)
PLC1	—	PU1(T1), PU2(T1), PU3(—)
PLC2	T1	—
PLC3	T2	V1(T2), PU4(T3), PU5(T3), PU6(T4), PU7(T4)
PLC4	T3	—
PLC5	—	PU8(T5), PU9(—), PU10(T7), PU11(T7)
PLC6	T4	—
PLC7	T5	—
PLC8	T6	—
PLC9	T7	—

[a]A PLC-to-PLC connection is established whenever an actuator and the relative controlling sensor are attached to two different PLCs.

the network hydraulic behavior, but simply to complement and support the analysis of the data produced by *epanetCPA*; see Todini (2000), Raad et al. (2010), and Creaco et al. (2016) for a detailed description of resilience and failure indices commonly used for water distribution systems.

The *total tank overflow* V_{TOT} is defined as the amount of water spilling over an attacked tank during the simulation period, that is

$$V_{\mathrm{TOT}} = \sum_{t=1}^{T} Q_t \cdot \Delta_t \tag{1}$$

where T = length of the simulation; Q_t = overflow from the attacked tank at time t; and Δ_t = simulation time step.

An equivalent index to quantify the effect due to empty tanks conditions is the amount of undelivered water (or unmet demand) caused by a cyber-physical attack. This index cannot be calculated because of the limitations of *EPANET*'s demand-driven hydraulic engine in modeling empty tanks and pressure-deficient scenarios, so a proxy index is used (*total time at low level*, T_{LOW}) defined as the total amount of time during which an attacked tank is in low level conditions, i.e.

$$T_{\mathrm{LOW}} = \sum_{t=1}^{T} g_t \cdot \Delta t \tag{2a}$$

with g_t being a step indicator defined as

$$g_t = \begin{cases} 0 & \text{if } h_t \geq l \\ 1 & \text{otherwise} \end{cases} \tag{2b}$$

where h_t = water level of the attacked tank at time t; and l = its low level threshold. The values of these thresholds are usually set by process managers to trigger some emergency actions when breached. In this study, these values are arbitrarily set equal to 50% of the lowest value recorded for each tank during normal operations; this corresponds to 0.25 m for both tank T1 and T2; 1 m for tanks T3, T4, and T7; 0.75 m for tank T5; and 2 m for tank T6.

To characterize the effect of cyber-physical attacks on pumping operations, the *relative variation in the pumps' total power consumption* $\Delta_p\%$, is computed, which is defined as

$$\Delta_p\% = \frac{\sum_{t=1}^{T}\sum_{i=1}^{N_p}(P_{it}^{*} - P_{it})}{\sum_{t=1}^{T}\sum_{i=1}^{N_p} P_{it}} \tag{3}$$

where N_p = number of pumps; and P_{it} and P_{it}^{*} = power consumption of the ith pump at time t under normal and attack conditions, respectively. In other words, this index expresses the relative variation in the pumps' power consumption between normal and attack conditions.

Results

Hydraulic Response to Cyber Threats

For each attack scenario (and a single hydraulic scenario), a visual inspection of the time series simulated by *epanetCPA* is performed and compared against the time series generated during normal operations. The analysis is complemented by the calculation of the indices across all hydraulic scenarios and attack conditions.

Attack Scenario 1: Tank Overflow due to a Direct Attack to a Booster Station

During normal operations pump PU1 is generally active, while pump PU2 is switched on only when a surge in demand causes tank T1 to empty faster. In this scenario, the attacker takes control of both pumps at time equal to 10 h, and forces both pumps to run simultaneously. Fig. 3 displays the effects of such attack on tank T1 water level and on PLC2 and SCADA readings. It is shown that the trajectories of the water level under normal and attack conditions diverge after the attack starts (gray versus black solid line). That happens because contrary to normal operations pump PU2 does not stop running when the water level in tank T1 is higher than 4.5 m, ultimately leading to an overflow at approximately 35 h into the simulation. Because there is no attack to the PLC monitoring the water level in tank T1 (i.e., PLC2) nor to the PLC2-to-SCADA communication link, the status of the tank water level is correctly monitored and registered. The implementation of the attack under different hydraulic scenarios leads to an overflow of the tank in all the cases, as depicted in Fig. 4. That is expected because this attack

Table 3. Specification of the Attack Scenarios

Scenario	Profile	Target	Action	Effect	Start condition	End condition
1	ATK4	PU1	Turn PU1 on	PU1 on	Time = 10 h	T1 overflow ≥ 50 m^3
		PU2	Turn PU2 on	PU2 on		
2	ATK3	T2 to PLC3 CL	Set T2 = 6 m (high level)	V1 closed	Time = 50 h	T2 < 0.125 m
2b	ATK3	T2 to PLC6 CL	Set T4 = 6 m (high level)	PU6 and PU7 off	Time = 50 h	T4 < 0.5 m
3	ATK5	PLC2 to PLC1 CL	Alter T1 level to PLC1	PU1 and PU2 on	Time ≥ 50 h and T1 < 1 m	T1 overflow ≥ 10 m^3
4	ATK5	PLC2 to PLC1 CL	Alter T1 level to PLC1	PU1 and PU2 on	Time ≥ 50 h and T1 < 1 m	T1 overflow ≥ 10 m^3
	ATK6	PLC2 to SCADA CL	Repeat T1 level to SCADA	SCADA deception	Time = 50 h	End of simulation
5	ATK7	SCADA to PLC5 CL	Alter PU11 activation level	PU11 on	Time = 50 h	Time = 100 h
6	ATK3	T2 to PLC3 CL	Alter T2 level to PLC3	V1 open	Random starting time	Random ending time
	ATK5	PLC4 to PLC3 CL	Alter T3 level to PLC3	PU4 and PU5 on	Random starting time	Random ending time
	ATK5	PLC6 to PLC3 CL	Alter T4 level to PLC3	PU6 and PU7 on	Random starting time	Random ending time

Note: CL = communication link.

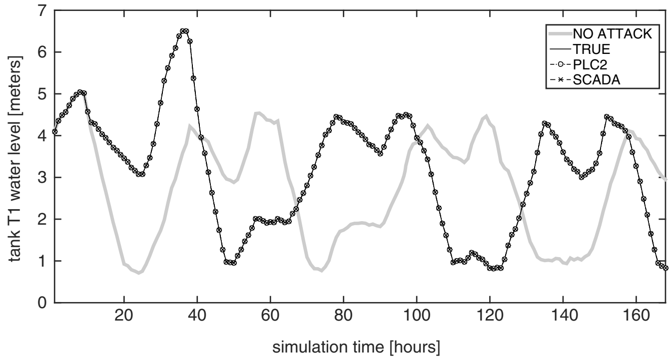

Fig. 3. Attack Scenario 1 with a comparison between tank T1 water level during normal and attack conditions (gray and black solid line, respectively), and a report of water level data monitored by PLC2 and transmitted to the SCADA

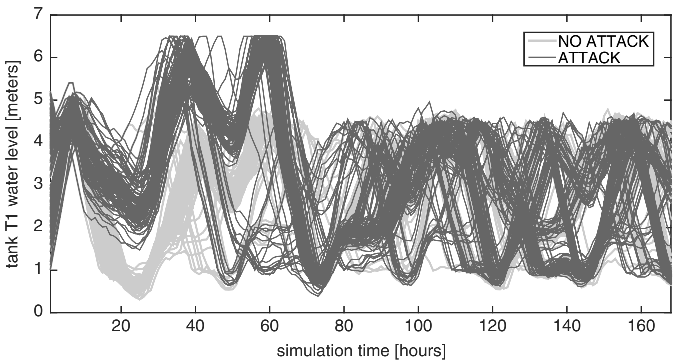

Fig. 4. Comparison between tank T1 water level during normal and attack conditions (Scenario 1) for all hydraulic scenarios considered in the study (gray and black solid line, respectively)

stops after causing at least 50 m^3 of *total tank overflow* V_{TOT} (Table 3). In particular, Table 4 reports an average value of V_{TOT} of approximately 68 m^3, with a standard deviation of over 9.5 m^3 denoting an appreciable sensitivity of the impact to different initial conditions. The attack also results in 1% increase in the *pumps' total power consumption* Δ_p%, which simply reflects the fact that one pump is switched on for several hours to cause a tank overflow. Conversely, the *total time at low level* T_{LOW} for T1 is equal to 0, as expected from an attack that is aimed at achieving the opposite outcome of increasing the water level in the tank.

Attack Scenario 2: Low Level in a Tank due to Manipulated Water Level Readings

Fig. 5(a) shows an instance of Scenario 2, where the water level readings in tank T2 are altered to prevent the tank from refilling. When T2 water level readings collected by PLC3 (dashed line with circles) are temporarily altered to a value triggering valve V1 closure, the tank is disconnected from the main line, resulting in a quick decrease of the water level; see the difference between normal and attack conditions (gray versus black line). Because the PLC3-to-SCADA communication link is not attacked, the anomalous PLC3 reading is communicated and stored in the SCADA. The implementation of the attack across all hydraulic scenarios leads to an average *total time at low level* T_{LOW} of 1.11 h, with a negligible variation in the pumps' energy consumption. As expected, the value of the *total tank overflow* is equal to zero (Table 4). Similar results are obtained for Scenario 2b, where tank T4 water level readings collected by PLC6 are altered. That wrong information is sent to PLC3, which controls pumps PU6 and PU7, resulting in the temporarily deactivation of the booster station and a decrease of the tank water level. Although the effects of the attack are more visible on tank T4, which normally operates further away from empty conditions [Fig. 5(b)], the average value of T_{LOW} for T4 is also 1.11 h.

Attack Scenario 3: Tank Overflow due to an Alteration of PLC-to-PLC Connection

In Scenario 3, the attacker modifies the information on tank T1 water level sent by PLC2 to PLC1, which controls pumps PU1 and PU2. As shown in Fig. 6, the water level time series associated to PLC2 and PLC1 differ (dashed line with circles versus dotted line with crosses). In particular, the value of tank T1 water level received by PLC1 triggers the activation of pumps PU1 and PU2, leading to a sharp increase of tank T1 water level. Similarly to the previous scenarios, the PLCs-to-SCADA communication links are not attacked; see in Fig. 6 the correct readings received by the SCADA system. That implies that the anomaly (with respect to standard operating conditions) might be discovered by an operator or an event detection mechanism. As reported in Table 4, that scenario is generally associated with an overflow from tank T1 (average value of the *total tank overflow* of approximately 38 m^3) and an obvious increase in pump usage. As for Scenario 1, tank T1 does not experience low level conditions during the attack simulation.

Attack Scenario 4: Concealment via Replay Attack on PLC-to-SCADA Connection

Scenario 3 is complemented by attacking the communication link between PLC2 and SCADA. The adversary first eavesdrops the PLC2-to-SCADA connection, deciphers the signals, and stores tank T1 readings for the first 48 h of simulation. Then, the attacker slightly modifies these readings by adding a random component, which are channeled through the PLC2-to-SCADA communication link. Hence, the SCADA receives plausible information on tank T1 water level (see the dashed line with crosses in Fig. 7) while the level is in fact rising sharply. The importance of the scenario goes beyond the hydraulic response of the water distribution system; the value of the impact quantification indices is comparable to that obtained for Scenario 3. It resides in the fact that the SCADA collects

Table 4. Average Value (μ) and Standard Deviation (σ) of the Impact Quantification Indices across All Hydraulic Scenarios

Attack scenario	V_{TOT} (m^3)	T_{LOW} (h)	$\Delta_P(\%)$
Scenario 1	$\mu = 68.247$, $\sigma = 9.507$	$\mu = 0.000$, $\sigma = 0.000$	$\mu = 1.061$, $\sigma = 0.953$
Scenario 2	$\mu = 0.000$, $\sigma = 0.000$	$\mu = 1.110$, $\sigma = 0.665$	$\mu = 0.025$, $\sigma = 0.708$
Scenario 2b	$\mu = 0.000$, $\sigma = 0.000$	$\mu = 1.110$, $\sigma = 0.373$	$\mu = 0.182$, $\sigma = 0.811$
Scenario 3	$\mu = 37.818$, $\sigma = 12.689$	$\mu = 0.000$, $\sigma = 0.000$	$\mu = 1.484$, $\sigma = 0.974$
Scenario 4	$\mu = 35.980$, $\sigma = 12.173$	$\mu = 0.000$, $\sigma = 0.000$	$\mu = 1.508$, $\sigma = 0.896$
Scenario 5	$\mu = 10.379$, $\sigma = 0.262$	$\mu = 0.000$, $\sigma = 0.000$	$\mu = 0.695$, $\sigma = 0.738$

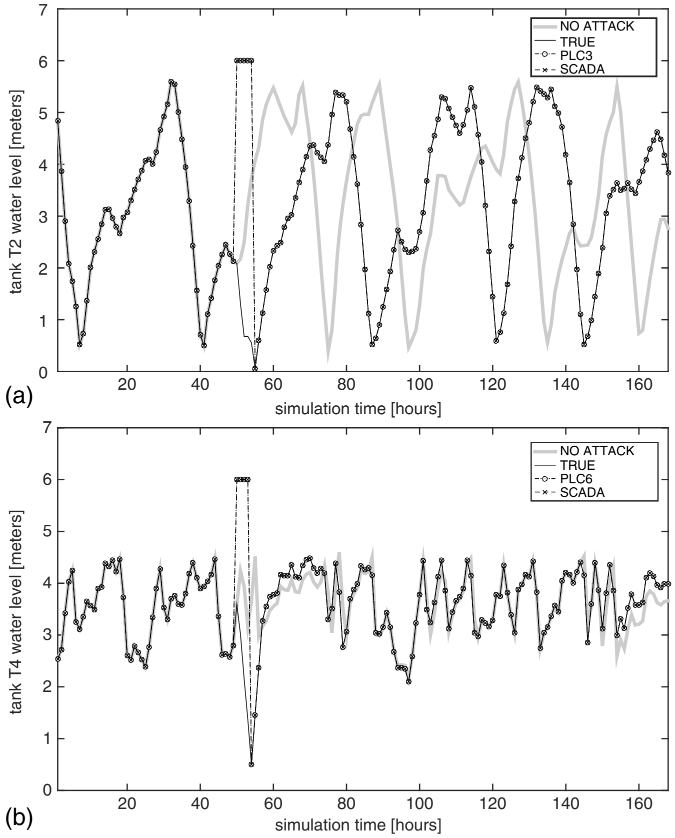

Fig. 5. Attack Scenario 2 and 2b: (a) comparison between tank T2 water level during normal and attack conditions (gray and black solid line, respectively), and a report of water level data monitored by PLC3 and transmitted to the SCADA; (b) comparison between tank T4 water level during normal and attack conditions and a report of water level data monitored by PLC6 and transmitted to the SCADA

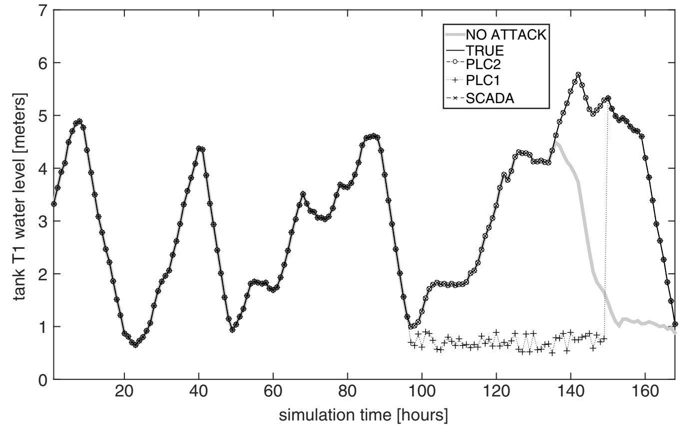

Fig. 6. Attack Scenario 3 with a comparison between tank T1 water level during normal and attack conditions (gray and black solid line, respectively), and a report of water level data monitored by PLC2 and transmitted to PLC1 and SCADA

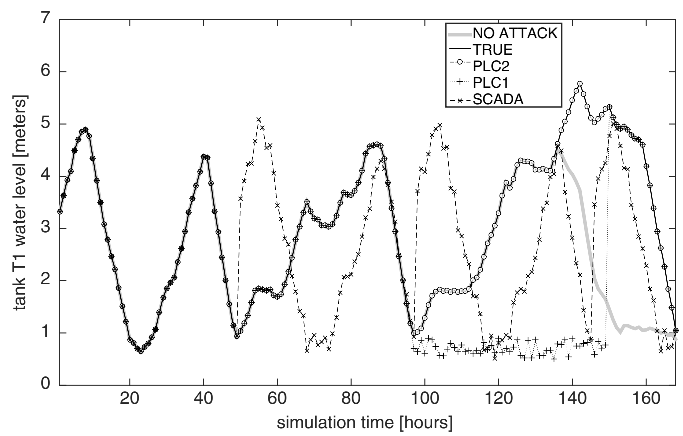

Fig. 7. Attack Scenario 4 with a comparison between tank T1 water level during normal and attack conditions (gray and black solid line, respectively), and a report of water level data monitored by PLC2 and transmitted to PLC1 and SCADA; note the difference between the SCADA time series with respect to Scenario 3

and stores wrong information on the system status, potentially making attack detection more difficult.

Attack Scenario 5: Tank Overflow due to Wrong Settings Sent by SCADA

This scenario consists of an attack to the SCADA-to-PLC5 connection. In particular, the attacker modifies the thresholds for the activation and deactivation of pump PU11 for approximately 50 h [Fig. 8(c)], causing PU11 to be active during the entire period. This results in an increase of tank T7 water level, which triggers PLC9 to de-activate pump PU10 [Fig. 8(b)]. Nonetheless, the attack causes an overflow of tank T7 [Fig. 8(a)]. Similarly to Scenarios 1, 3, and 4, an increase in pumps usage and no low level conditions are observed (Table 4).

Attack Scenario 6: Random Multiple Attacks on PLC

Fig. 9 illustrates the response of C-Town network under 100 randomized attacks targeting three tanks directly or indirectly connected to PLC3, i.e., tanks T2, T3, and T4. Each simulation features a sequence of three attacks aimed at driving each tank to overflow, either simultaneously or in short succession. Specifically, the sequence comprises a manipulative attack on tank T2 water level readings being sent to PLC3, as well as two attacks on PLC6-to-PLC3 and PLC4-to-PLC3 communication links. Results show that the hydraulic response of the network is largely influenced by the starting time and duration of each attack; note the difference between the trajectory generated under normal and attack conditions (gray and black solid lines). The indices for this attack scenario are not computed because each simulation features different attack specifications.

Insights

The explicative attacks on C-Town network illustrated previously help draw some important, preliminary conclusions regarding the hydraulic response of water distribution systems to cyber threats. First, the same hydraulic response (e.g., a tank overflow) can be obtained through different attacks, for example by altering the information sent by the SCADA to a PLC controlling an actuator or by jamming the communication link between two PLCs. This implies that while an operator may easily detect an anomalous behavior of the water network (through the SCADA system or direct observation), they may struggle to identify the cause of the problem, that is, the cyber component that has been attacked. One might imagine that this problem is of particular relevance for systems

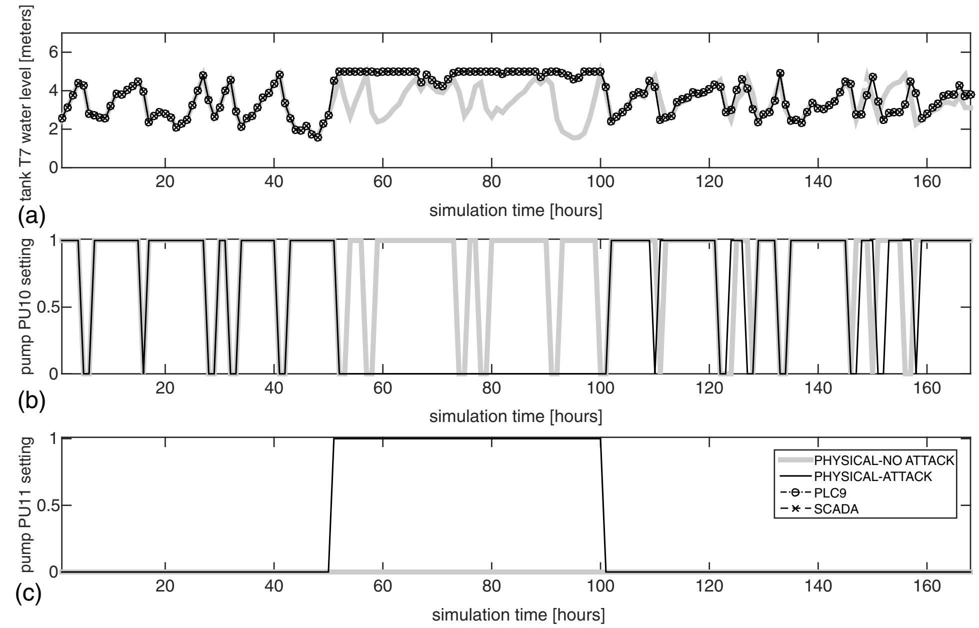

Fig. 8. Attack Scenario 5: (a) comparison between tank T7 water level during normal and attack conditions (gray and black solid line, respectively), and a report of water level data monitored by PLC9 and transmitted to SCADA; (b and c) settings of pump PU10 and PU11, respectively

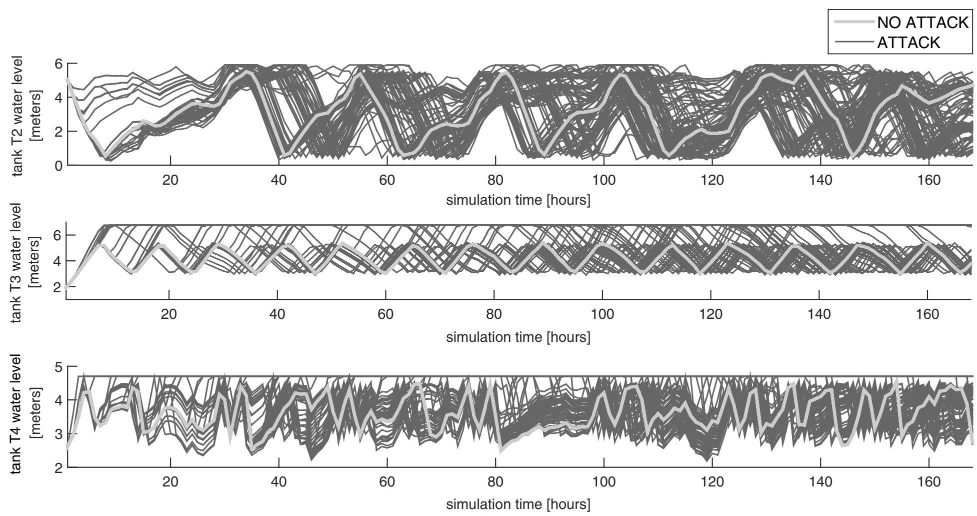

Fig. 9. Comparison between tank T2, T3, and T4 water level during normal and attack conditions generated with multiple combined random attacks

having complex, extended communication networks. Second, eavesdropping attacks are potentially very dangerous because the adversary can use information on the system behavior (e.g., time series of tank water levels or boosting station settings) to design sophisticated attacks that not only undermine the system availability, but also the integrity of the data received and analyzed by the operators. For example, in Scenario 4 the hypothetical attacker uses eavesdropped readings of tank T1 water level to send plausible information to the SCADA while causing an overflow of the tank. This implies that attacks affecting the integrity of the data received and stored by the SCADA may require more time to be discovered. Third, results show that the hydraulic response of a water distribution network to a cyber-physical attack is largely influenced by the system initial conditions and demand at the junctions (as well as the specifications of the attack). The illustrative examples show that adequate representation of the complex interaction between cyber and physical space requires sophisticated models.

Toward Simulation-Based Risk Assessment

Risk is defined as the product between the likelihood of an event and the adverse consequences it generates. Probabilistic analysis and impact assessments are thus needed to estimate the risks associated to any attack scenario. Despite the heightened alert for cyber attacks on water utilities, the number of reported attacks is still too low for estimating their probability of occurrence. More data could be available if water utilities were willing to share information on security breaches as they do for other events, such as pipe breaks (Shortridge and Guikema 2014) and accidental contamination (Rasekh and Brumbelow 2013). As far as the impact assessments are concerned, it should be noted that the type and extent of the adverse consequences of an attack are potentially very broad. In this work, such diversity was reflected by the impact quantification indices. Although these indices were useful for the analysis presented in this paper, they may not be directly employed for risk

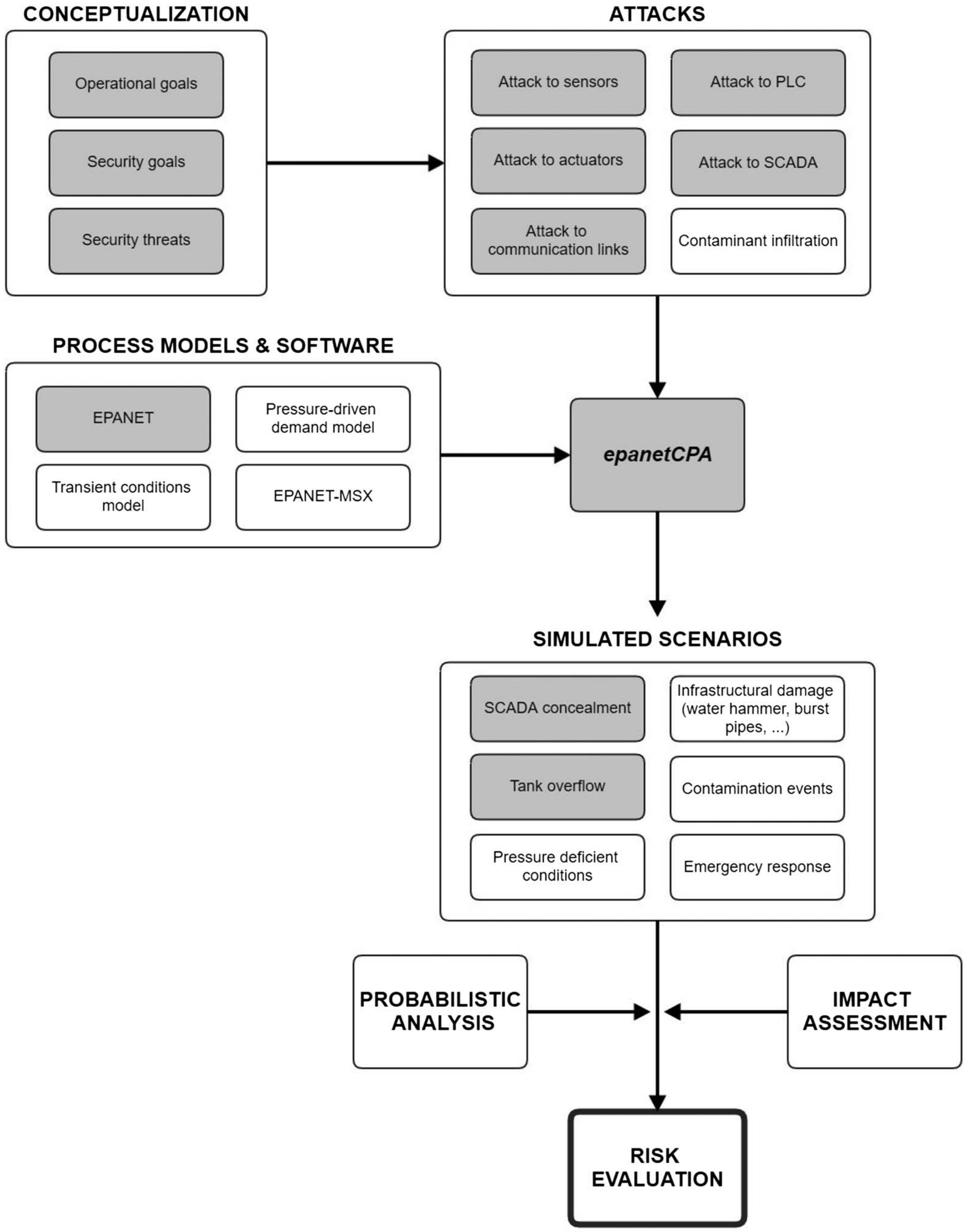

Fig. 10. Interplay between components for simulation-based risk assessment of cyber-physical attacks on water distribution systems; components in gray are provided by this work, components in white are still missing

assessments, which generally build on cost estimates. For example, it is not the amount of tank overflow per se that quantifies the consequence of an attack, but rather the collateral costs due to endangered infrastructures and personnel safety. Similar considerations apply for attacks aimed at disrupting operations, reducing water supply, or damaging the elements of the distribution network. Further research is thus needed to estimate the costs associated to cyber attacks. Similarly, the impact of an attack causing or supporting a contamination event should be estimated with appropriate exposure models for the susceptible population (Davis and Janke 2008).

While simulation-based assessment has proven successful in estimating the risks of accidental contamination (Rasekh and Brumbelow 2013), several key issues need to be addressed before it can be fully employed for cyber-physical security threats. In Fig. 10, the interplay of components required to achieve such goal is shown; missing components are highlighted in white, along with the contributions made in this paper in grey. The scheme is made of five main interconnected areas that pertain to system conceptualization, attacks, modeling tools, simulated scenarios, and risk evaluation. *EpanetCPA* plays a pivotal role, as it implements cyber-physical attacks and allows the simulation of their effects by harnessing models and simulation engines.

Enhanced capabilities are needed to reproduce a wider spectrum of attack scenarios. For instance, complex contamination scenarios involving the interaction of multiple chemical and biological species would require sophisticated water quality models. Similarly, a pressure-driven hydraulic engine is necessary to reproduce pressure-deficient conditions determined by adversarial actions aimed at reducing or cutting off water supply. Some *epanetCPA* features might be extended to model such processes, for example by interfacing the toolbox with *EPANET*-MSX (Multi-Species eXtension) routines (Shang et al. 2008), or by adopting recent solutions that entail incorporating artificial elements in the *EPANET* map as in the approach recently proposed by Sayyed et al. (2015). Conversely, the lack of public domain libraries for modeling transient flows may hinder the simulation of attacks causing pipe bursts, pipe collapses, or damages to actuators and other physical water assets. Eventually, the range of attacks should be further extended to include adversarial attempts aimed at thwarting emergency responses, such as during contamination events (Rasekh and Brumbelow 2014) or major firefighting operations (Bristow et al. 2007). These actions are particularly appealing to terrorists that want to maximize the damage of a simultaneous physical attack (Lewis 2002).

Conclusions

This work paves the way for a simulation-based assessment of the risks associated with cyber-physical attacks on modern water distribution systems. Such an approach would allow reliable estimates of local and systemic vulnerabilities, as well as enable a cost-benefit analysis of the solutions aimed at improving systems' security. The authors conceptualize water distribution networks as cyber-physical systems characterized by operational and security goals, and contribute an attack model and *epanetCPA* toolbox. The attack model is conceived to design attack profiles targeting hydraulic actuators, sensors, PLCs, SCADA, and communication links. These profiles may also be relevant to adversaries targeting water quality processes, but further research is required to define intentional injection of contaminants in pipes, storage tanks, and water treatment plants (Rasekh and Brumbelow 2013; Ostfeld and Salomons 2004). By interfacing with *EPANET*, the *epanetCPA* toolbox allows a first assessment of the hydraulic response of water networks to cyber attacks. Its application to C-Town network shows that the hydraulic response depends not only on the attack specifications, but also on the system initial conditions and demand at the junctions. It was also found that the same hydraulic response can be obtained by implementing completely different attacks. This has important implications on the design of attack detection mechanisms, which should identify anomalous behaviors in a water network as well as the cyber components being hacked. While the full development of a simulation-based approach to risk assessment requires further research, the proposed attack model and *epanetCPA* toolbox are expected to provide a sound foundation for future work.

Acknowledgments

This work was supported by the National Research Foundation (NRF), Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-40).

Supplemental Data

The *EPANET* input file containing the C-Town water distribution network used in this study is available in the ASCE Library (http://www.ascelibrary.org).

References

Ackerman, G. (2015). "New York and Jerusalem partnership plans to defend water supply." ⟨http://www.bloomberg.com/news/articles/2015-10-20/new-york-and-jerusalem-partnership-plans-to-defend-water-supply⟩ (Jun. 20, 2016).

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 Trans. Control Syst. Technol.*, 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 Trans. Control Syst. Technol.*, 21(5), 1679–1693.

Atzori, L., Iera, A., and Morabito, G. (2010). "The internet of things: A survey." *Comput. networks*, 54(15), 2787–2805.

Bobat, A., Gezgin, T., and Aslan, H. (2015). "The SCADA system applications in management of Yuvacik Dam and Reservoir." *Desalin. Water Treat.*, 54(8), 2108–2119.

Bristow, E., Brumbelow, K., and Kanta, L. (2007). "Vulnerability assessment and mitigation methods for interdependent water distribution and urban fire response systems." *World Environmental and Water Resources Congress*, ASCE, Reston, VA, 1–10.

Cardenas, A. A., Amin, S., and Sastry, S. (2008). "Secure control: Towards survivable cyber-physical systems." *28th Int. Conf. on Distributed Computing Systems Workshops*, IEEE, New York, 495–500.

Cominola, A., Giuliani, M., Piga, D., Castelletti, A., and Rizzoli, A. E. (2015). "Benefits and challenges of using smart meters for advancing residential water demand modeling and management: A review." *Environ. Modell. Software*, 72, 198–214.

Creaco, E., Alvisi, S., and Franchini, M. (2015). "Multistep approach for optimizing design and operation of the C-Town pipe network model." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)WR.1943-5452.0000585, C4015005.

Creaco, E., Franchini, M., and Todini, E. (2016). "Generalized resilience and failure indices for use with pressure-driven modeling and leakage." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)WR.1943-5452.0000656, 04016019.

Dakin, R., Newman, R., and Groves, D. (2009). "The case for cyber security in the water sector." *J. Am. Water Works Assoc.*, 101(12), 30.

Davis, M. J., and Janke, R. (2008). "Importance of exposure model in estimating impacts when a water distribution system is contaminated." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)0733-9496(2008)134:5(449), 449–456.

EPA (Environmental Protection Agency). (2011). "EPA has taken steps to address cyber threats but key actions remain incomplete." *Rep. No. 11-P-0277*, Office of Inspector General, Washington, DC.

EPANET [Computer software]. U.S. Environmental Protection Agency, Cincinnati.

Gong, W., et al. (2016). "Mobile sensor networks for optimal leak and backflow detection and localization in municipal water networks." *Environ. Modell. Software*, 80, 306–321.

Hart, W. E., and Murray, R. (2010). "Review of sensor placement strategies for contamination warning systems in drinking water distribution systems." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)WR.1943-5452.0000081, 611–619.

Horta, R. (2007). "The city of Boca Raton: A case study in water utility cybersecurity." *J. Am. Water Works Assn.*, 99(3), 48.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). (2014). "The industrial control systems-cyber emergency response team." *Rep. No. ICS-MM201408*, Dept. of Homeland Security, Washington, DC.

Krotofil, M., Cárdenas, A. A., Manning, B., and Larsen, J. (2014). "CPS: Driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals." *Proc., Computer Security Applications Conf. (ACSAC)*, ACM, New York, 146–155.

Lee, E. A. (2008). "Cyber physical systems: Design challenges." *2008 11th IEEE Int. Symp. on Object Oriented Real-Time Distributed Computing (ISORC)*, IEEE, New York, 363–369.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*, Center for Strategic and International Studies, Washington, DC.

MATLAB [Computer software]. MathWorks, Natick, MA.

Ostfeld, A., et al. (2008). "The battle of the water sensor networks (BWSN): A design challenge for engineers and algorithms." *J. Water*

Resour. Plann. Manage., 10.1061/(ASCE)0733-9496(2008)134:6(556), 556–568.
Ostfeld, A., et al. (2012). "Battle of the water calibration networks." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)WR.1943-5452.0000191, 523–532.
Ostfeld, A., and Salomons, E. (2004). "Optimal layout of early warning detection stations for water distribution systems security." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)0733-9496(2004)130:5(377), 377–385.
Perelman, L., and Amin, S. (2014). "A network interdiction model for analyzing the vulnerability of water distribution systems." *Proc., 3rd Int. Conf. on High Confidence Networked Systems*, ACM, New York, 135–144.
Raad, D., Sinske, A., and Van Vuuren, J. (2010). "Comparison of four reliability surrogate measures for water distribution systems design." *Water Resour. Res.*, 46(5), 1–11.
Rasekh, A., and Brumbelow, K. (2013). "Probabilistic analysis and optimization to characterize critical water distribution system contamination scenarios." *J. Water Resour. Plann. Manage.*, 10.1061/(ASCE)WR.1943-5452.0000242, 191–199.
Rasekh, A., and Brumbelow, K. (2014). "Drinking water distribution systems contamination management to reduce public health impacts and system service interruptions." *Environ. Modell. Software*, 51, 12–25.
Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., and Banks, M. K. (2016). "Smart water networks and cyber security." *J. Water Resour. Plann. Manage.*, 01816004.
Saldarriaga, J., et al. (2015). "Rehabilitation and leakage reduction on C-Town using hydraulic criteria." *J. Water Resour. Plann. Manage.*, C4015013.
Sayyed, M. A. H. A., Gupta, R., and Tanyimboh, T. T. (2015). "Noniterative application of epanet for pressure dependent modelling of water distribution systems." *Water Resour. Manage.*, 29(9), 3227–3242.
Schwab, K. (2016). "The fourth industrial revolution." World Economic Forum, Geneva.
Shang, F., Uber, J. G., and Rossman, L. (2008). "EPANET multi-species extension user's manual." *Risk reduction engineering laboratory*, U.S. Environmental Protection Agency, Cincinnati.
Shortridge, J. E., and Guikema, S. D. (2014). "Public health and pipe breaks in water distribution systems: Analysis with internet search volume as a proxy." *Water Res.*, 53, 26–34.
Slay, J., and Miller, M. (2008). *Lessons learned from the Maroochy water breach*. Springer, Boston.
Sousa, J., Muranho, J., Sá Marques, A., and Gomes, R. (2015). "Optimal management of water distribution networks with simulated annealing: The C-Town problem." *J. Water Resour. Plann. Manage.*, C4015010.
Spellman, F. R. (2013). *Handbook of water and wastewater treatment plant operations*, CRC Press, Boca Raton, FL.
Taormina, R., Galelli, S., Tippenhauer, N., Ostfeld, A., and Salomons, E. (2016). "Assessing the effect of cyber-physical attacks on water distribution systems." *World Environmental and Water Resources Congress*, ASCE, Reston, VA, 436–442.
Todini, E. (2000). "Looped water distribution networks design using a resilience index based heuristic approach." *Urban water*, 2(2), 115–122.
Urbina, D., Giraldo, J., Tippenhauer, N. O., and Cárdenas, A. (2016). "Attacking fieldbus communications in ICS: Applications to the SWaT testbed." *Proc., Singapore Cyber Security Conf. (SG-CRC)*, IOS Press BV, Amsterdam, Netherlands.