Cyber-Physical Stress-Testing Platform for Water Distribution Networks

Dionysios Nikolopoulos[1]; Georgios Moraitis[2]; Dimitrios Bouziotas[3]; Archontia Lykou[4]; George Karavokiros[5]; and Christos Makropoulos[6]

Abstract: The water sector is facing emerging challenges, as cyber-physical threats target Supervisory Control and Data Acquisition (SCADA) systems of water utilities. A cyber-physical stress-testing platform is presented in this work, named RISKNOUGHT, which is able to model water distribution networks as cyber-physical systems, simulating the information flow of the cyber layer and the feedback interactions with the physical processes under control. RISKNOUGHT utilizes an EPANET-based solver for the physical process and a customizable network model for the SCADA system, capable of implementing complex control logic schemes within a simulation. The platform enables the development of composite cyber-physical attacks on various elements of the SCADA, including sensors, actuators, and PLCs, assessing the impact they have on the hydraulic response of the distribution network and the level of service. The platform is tested on a proof-of-concept benchmark network with promising results that demonstrate that the platform can form an innovative cyber-physical tool to support strategic planning and risk management. **DOI: 10.1061/(ASCE)EE.1943-7870.0001722.**

Author keywords: Water distribution systems; Cyber-physical systems; Cyber-physical attacks; Water cyber security; Stress-testing platform.

Introduction

Cyber-physical systems (CPSs) are an integration of physical processes with computational engineered systems (Lee 2008). The operations of the physical processes are monitored, coordinated, and controlled by a networking, computing, and communication core (Rajkumar et al. 2017) usually in real time via feedback loops, where physical processes affect computations and vice versa (Lee 2015). Automated control systems have existed since the 1940's and mainframe computer controlled systems appeared in the 1960's (Nicholson et al. 2012); however, the first true CPSs emerged with the rise of the microprocessor units in the 1970s (Wolf 2009) with progress following the boom of computer technology. Modern CPSs are evolving rapidly aided by recent developments on sensor technology and networked machines, information and communications technology (ICT), Internet Of Things (IoT), and Big Data (McAfee et al. 2012). Hence, CPS applications are transforming infrastructure and revolutionizing industrial applications (e.g., in energy, transportation, manufacture, water supply) in an unprecedented way that led to the term "Industry 4.0" (Lu 2017). Among others, advantages of CPSs are increased automation, improving the adaptability, efficiency, functionality, reliability, safety, and usability of large systems (Chen 2017). However, a major disadvantage of the networking, communication, and remote control schemes within the critical infrastructures (CIs) of CPSs is their exposure to an expanded attack surface (Rasekh et al. 2016), which aside from typical physical attacks (e.g., component destruction, sabotage) includes cyber-attacks [e.g., Denial of Service (DoS) attacks to disrupt communication between components or Structured Query Language (SQL) injection to destroy databases] or combinations (e.g., in the case of water CPS, manipulation of quality sensor readings, and deliberate contamination of water sources) in the form of cyber-physical attacks (CPA) (Taormina et al. 2017). This attack surface can be exploited by a wide range of adversaries for different motives, from penetration testers for CPS protection reasons (Nicholson et al. 2012) to state hackers (i.e., as a means of cyber-warfare), terrorists, hacktivists, disgruntled employees, or organized crime. Usually attacks are focused on the supervisory control and data acquisition (SCADA) system, which forms part of the cyber layer of the

[1] Civil Engineer and Ph.D. Candidate, Dept. of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical Univ. of Athens, Heroon Polytechneiou 5, 15780 Zografou, Greece (corresponding author). ORCID: https://orcid.org/0000-0002-3934-4746. Email: nikolopoulosdio@central.ntua.gr

[2] Ph.D. Candidate, Civil Engineer, Dept. of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical Univ. of Athens, Heroon Polytechneiou 5, 15780 Zografou, Greece. Email: georgemoraitis@central.ntua.gr

[3] Civil Engineer and Researcher, KWR Water Research Institute, Groningenhaven 7, 3433 PE Nieuwegein, Netherlands. ORCID: https://orcid.org/0000-0003-2172-350X. Email: Dimitrios.Bouziotas@kwrwater.nl

[4] Ph.D. Candidate, Civil Engineer, Dept. of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical Univ. of Athens, Heroon Polytechneiou 5, 15780 Zografou, Greece. ORCID: https://orcid.org/0000-0002-1623-2290. Email: alykou@central.ntua.gr

[5] Computer Scientist, Dept. of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical Univ. of Athens, Heroon Polytechneiou 5, 15780 Zografou, Greece. Email: gkaravo@itia.ntua.gr

[6] Associate Professor, Dept. of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical Univ. of Athens, Heroon Polytechneiou 5, 157 80 Zografou, Greece; Principal Scientist, KWR Water Research Institute, Groningenhaven 7, 3433 PE Nieuwegein, Netherlands. ORCID: https://orcid.org/0000-0003-0308-4265. Email: cmakro@mail.ntua.gr

Note. This manuscript was submitted on August 26, 2019; approved on December 23, 2019; published online on April 30, 2020. Discussion period open until September 30, 2020; separate discussions must be submitted for individual papers. This paper is part of the ***Journal of Environmental Engineering***, © ASCE, ISSN 0733-9372.

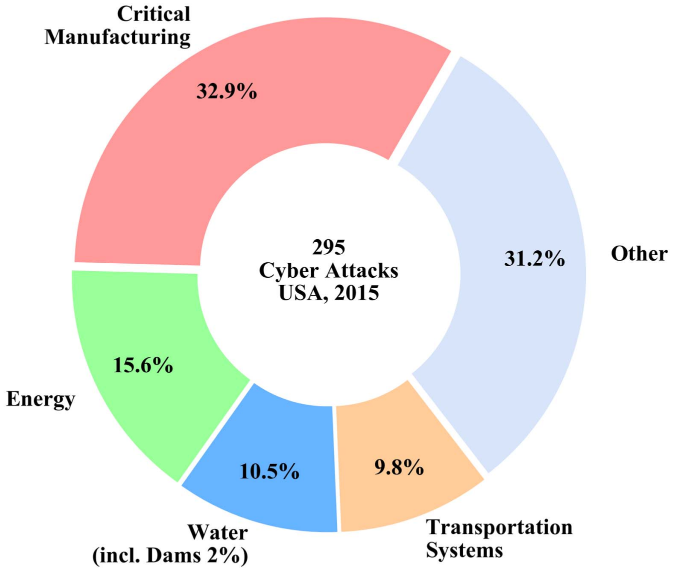


Fig. 1. Distribution of 295 cyber-attacks incidents recorded in USA, 2015. (Data from ICS-CERT 2016.)

CPS. Older SCADA systems (relying on communication protocols such as Modbus or DNP3) were connected to local intranets isolated from public networks (Fovino et al. 2010) and this led the industry to adopt a sense of false sandbox-security. Modern SCADA systems and upgrades of older systems, however, are connected to the main corporate/business network of the infrastructure operator to take advantage of ICT technologies and increased connectivity, making them much more vulnerable now than in the past. Several security breaches have been recorded in recent years, of which the most notable and well-known example is probably the Stuxnet incident (late 2009 or early 2010). Stuxnet is a sophisticated quasi-autonomous computer worm that establishes control over remote systems. The worm hijacked programmable logic controller (PLC) programs operating centrifuges in the Natanz uranium enrichment facility, caused the centrifuges to wildly alternate speeds, and ultimately destroyed a large number of them (Falliere et al. 2011; Langner 2011).

Modern water systems (distribution networks, treatment plants, etc.) are CPS, because the physical system is supervised and operated by sets of sensors and actuators through SCADA systems and embedded PLCs in real-time. Although water infrastructure is not usually associated with CPAs, several incidents of cyber-physical attacks have threatened real-world water CPS, making them among the most targeted critical infrastructure (ICS-CERT 2016) as shown in a recent study (Fig. 1).

Perhaps the first widely known cyber-attack on water CPS was the 2000 Maroochy Shire incident in an era when security issues were not common in SCADA systems (Sayfayn and Madnick 2017). A disgruntled engineer worked with a private company on the installation of the new radio-controlled SCADA system in the sewage system run by the Maroochy Shire Council. Later, he left the company and immediately thereafter applied for a job at the Maroochy Shire Council, but his application was rejected. As an act of vengeance, the perpetrator stole radio equipment and repeatedly issued radio commands to the wireless network, altering control signals to sewage pumps (Abrams and Weiss 2008). This caused massive runoffs, estimated at nearly a million liters of unprocessed sewage into a local park, a river, and a hotel, which incurred damages of more than 1 million dollars. Cyber-physical attacks can be even more serious, like the 2013 Bowman Dam hack in New York (Thompson 2016), when a hacker broke into the control system of the dam through a cellular modem and gained access to a sluice gate. The incident could have had serious implications, had the sluice gate not been manually disconnected at the time for maintenance. Another serious event was the infiltration of a water treatment plant (Leyden 2016) where attackers changed the mixing of chemicals by valve manipulation, fortunately without serious implications, in what could have been a public healthcare issue. Moreover, the trend in recent attacks revolve around ransomware that ties down operation in utilities (Germano 2018), which may or may not affect system control but could potentially have disastrous cascading effects or monetary losses.

These incidents suggest the need for developing robust tools that are able to assess the performance of water CPS under cyber-physical threat scenarios. Moreover, as the resilience of water systems is emerging in policy discourse and strategic planning (Makropoulos et al. 2018), it is imperative to rethink water systems as CPS in resilience-oriented stress-testing procedures (Nikolopoulos et al. 2019b). Promising conceptual and technological solutions to water systems security and resilience do exist (Cook and Bakker 2012), but further work is required to bring them together in an overarching risk management framework, strengthen the capacities of water utilities to protect their systems in a systematic and standardized way, and determine gaps in security technologies and improve their risk management approaches and technologies (Mittelstadt et al. 2015). Real SCADA testbeds have been used for security research (Oman and Phillips 2007); however, these solutions are normally cost prohibitive for actual deployment and proprietary and are thus nonscalable to other utilities (Nikolopoulos et al. 2018). Therefore, various CPS modelling tools have emerged including emulators, virtual machines, software-defined networks (SDNs), and network function virtualization (NFV) (Piedrahita et al. 2017), all of which have potential.

MiniCPS (Antonioli and Tippenhauer 2015) is an extension of Mininet (Lantz et al. 2010), a light network virtualization tool, allowing communication between PLCs. A further extension of MiniCPS is used to implement the field network (connections between PLCs, sensors, and actuators) via SDN functionalities and interact with physical processes in a water treatment process (Piedrahita et al. 2017). SCADAVt (Almalawi et al. 2013) is a SCADA testbed based on the CORE (Ahrenholz et al. 2008) emulator, expanded through plugin systems with the Modbus/TCP slave master protocols and simulators of field devices. SCADAVt is coupled through server simulation with the well-known pressurized pipe network EPANET modelling tool (Rossman 2000) and manipulated with a TCP-based protocol to open or close pumps in the system. Other similar tools used for security research of CPS, such as EPIC (Siaterlis et al. 2013), which is based on Emulab (White et al. 2004) and can be coupled with physical process simulation tools, or even discrete event simulators like OMNET++ (Varga and Hornig 2008) and NS-3 (NS-3 Consortium 2019), can also be used for the same purpose after customization. Such tools provide high fidelity in the actual modeling of the cyber-element of any CPS (especially when using emulators), because it is explicitly represented through the emulation or simulation of real virtual components, networks, software, and protocols (Siaterlis et al. 2013). However, the emulation/virtualization or discreet event simulation type of approaches to water cyber-physical modeling and stress-testing have some trade-offs:

- Creating a digital twin of the cyber layer of respective water CPS is a demanding task that must be performed by an IT/ICT expert.

- It is not intuitive to perform a multitude of cyber-physical attacks for stress-testing, because this results essentially in a form of penetration-testing to uncover unpatched processes, security issues, backdoors, bugs, glitches, etc.
- These solutions tend to be proprietary and tailored for a specific CPS. Also, in large-scale systems they gravitate towards being cost intensive (in terms of development at least).
- While more precise, experiment and measurement repeatability is not ensured with cyber layer emulators (Fovino et al. 2010). On the contrary, cyber layer simulation (Queiroz et al. 2009) usually trades-off fidelity with strong repeatability for security experiments (Siaterlis et al. 2013). Thus, choice of tool type may affect the reproducibility of stress-testing results.
- Extensive work may be needed to couple these tools with a physical process simulator and because many of these tools employ real-time emulation or discrete event simulation, the physical process simulator should be compatible.

Another emergent approach is purely simulation-based for both the cyber and physical layers. The information flow in the cyber layer is represented with lower fidelity, because the focus is on the outcome of a cyber-operation or the state of a cyber-component, rather than the representation of the exact real interaction bit-wise. Seminal work in this field is introduced by Taormina et al. (2017), with the conceptualization of models for cyber-physical attacks in water distribution systems, methodologies based on deep-learning for detection of such attacks (Taormina and Galelli 2018), and the release of epanetCPA, an EPANET-based MATLAB modeling toolbox (Taormina et al. 2019). This simulation approach, despite the lower fidelity in the cyber layer, has the following advantages:

- Straight-forward modeling of various types of cyber-physical attacks, because the attack is modeled as a definitive event and not as a series of very detailed steps involving discovering possibly unknown vulnerabilities in a CPS with specific components. This also enables testing of "what-if" scenarios of cyber-physical nature and risk assessment.
- Easier coupling to models of the physical processes, because the cyber layer model should issue control statements and receive feedback from operation without the use of complex middleware (software to interconnect the discrete event emulation/virtualization processes with translated inputs/outputs of the physical model). The coupling can be implemented with direct use of software wrappers for the physical model, or through calling dynamic link libraries.

This work introduces a new modeling platform for water cyber-physical distribution networks, based on a purely simulation approach, able to simulate information flow, control logic, and interconnections with the physical processes in a higher fidelity, more realistic, and extensible way than existing simulation solutions. The platform aims at stress-testing distribution networks and aids in risk management practices. Stemming from its objective, the platform is named RISKNOUGHT, i.e., "to risk nothing" (Nikolopoulos et al. 2019a).

RISKNOUGHT Modeling Platform

Physical Layer Simulation

The foundation of the platform is the realistic representation of the physical processes of water distribution networks, and as such RISKNOUGHT relies on a robust hydraulic model. Among various existing free and commercial hydraulic solvers, including EPANET (Rossman 2000), WATER-GEMS (Bentley Systems Incorporated 2006), and INFOWORKS (Wallingford Software 2012), EPANET was selected as the base model. Extensive use in the literature has proven that it offers a potent simulation base, features an open source repository (USEPA, epanet-solver 2019) supporting future extensibility, and includes a dynamic link library called Programmer's Toolkit. The library exposes the software's routines written in C programming language, allowing developers to customize their models embedding EPANET with additional functionality. Various software wrappers take advantage of the Programmer's Toolkit and allow the utilization of EPANET routines via other programming languages, e.g., Python (Klise et al. 2017a), C# (Salomons 2014), MATLAB (Eliades et al. 2016), and R (Arandia and Eck 2018). Because RISKNOUGHT is Python-based, it employs the Water Network Tool for Resilience (WNTR) Python package (Klise et al. 2017a, 2018), version 0.1.7 at the time of writing. The package originally presents a comprehensive software framework for assessing the resilience of drinking water systems to disasters. It includes bindings to original EPANET routines, as well as a complete port of EPANET routines to Python, called the WNTR simulator [with only some minor limitations to be addressed in future versions (Klise et al. 2017b)]. WNTR's port of routines facilitates pressure-driven analysis (PDA) hydraulic equations (Wagner et al. 1988) as opposed to demand-driven analysis (DDA) equations that EPANET uses. The use of PDA hydraulic equations is important because the default DDA setting of EPANET requires that demand is always covered (Ciaponi and Creaco 2018), even when the solution leads to physically infeasible pressures. PDA equations are vital in the representation of sudden failures of the system resulting in inadequate pressure or rapid changes in system operation, because they allow demand to not be fully met; this is of paramount importance to disaster modeling as well as cyber-physical attacks. The usage of WNTR within RISKNOUGHT also allows handling of input/output files, enriched interaction with network elements (add/remove/modify properties), and permits simulation of physical damage due to disasters, i.e., pipe leaks, tank leaks, etc. RISKNOUGHT further enhances WNTR capabilities with geospatial input/output capabilities (I/O) using geopandas (Jordahl et al. 2019), shapely (Gillies et al. 2007), and gdal (GDAL/OGR Contributors 2019) packages, allowing the definition of pressure zones imported from shapefiles with nominal and minimum pressure levels as attributes for the nodes of the zone for PDA purposes.

Cyber Layer Simulation and Interconnection with Physical Layer

The cyber layer of RISKNOUGHT is built based on the complex network analysis NetworkX (Hagberg et al. 2008) Python package as a network of interconnected cyber components. The whole cyber infrastructure is represented as a directed graph, with nodes acting as the components (sensors, actuators, PLCs, etc.) and connections (wireless transmission, fiber, etc.) between components as edges. Components are built as classes that include the following common types of cyber components:

- **Sensor**: acquire data from the physical layer.
- **Actuator**: perform an action on the physical layer.
- **Logic**: virtual components (software bits), that implement control logic via using input data from sensors to decide physical procedures as outputs through actuators. Logic components are assembled into PLC units.
- **PLC**: oversees and interconnects Logic components.
- **Central SCADA**: oversees and interconnects all connected PLCs and also acts as the Human-Machine-Interface (HMI). Gathers all I/O data.

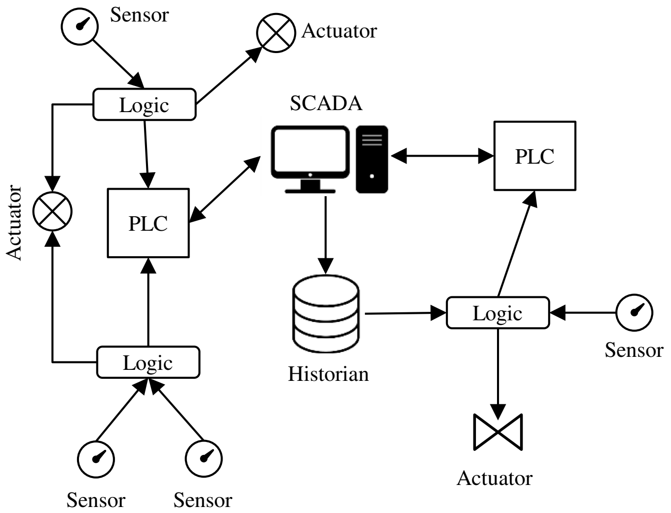


Fig. 2. Schematic overview of the cyber layer.

- **Historian**: records all operations and I/O (input/output) data (essentially the SCADA database).

A schematic overview of the cyber layer is represented in Fig. 2.

Cyber and physical layers are coupled through a unified simulation process, with feedback loops between each discrete cyber and physical layers simulation step. In a single timestep, the physical layer feeds input data (e.g., node pressure, tank level, pipe velocities, etc.) from the hydraulic simulation to the cyber layer, which ultimately passes decisions to the physical layer, affecting the hydraulic state for the next step of the hydraulic simulation (e.g., valve state, pump state, etc.), as shown in Fig. 3. The following sections explain the operation of all components in more detail.

Sensors

Sensors are physical devices of the cyber layer that receive an input from physical processes and provide an output signal as a reading to the rest of the cyber layer components, usually to a PLC. In RISKNOUGHT, input is acquired in raw data information from EPANET nodes or links during the hydraulic simulation at each simulation step or at a specified sampling interval. Node data that can be sensed include pressure, head (also from reservoir variable head), tank level (applicable for tank nodes), and node quality in case of a coupled EPANET quality simulation. Sensed link data refer to pipe velocity and flowrate as well as link quality. RISKNOUGHT modeling assumes that these data after capture are subsequently transferred through the respective connection to a Logic software part of a PLC. Also, various characteristics can be attributed to sensors in order to differentiate them, namely their type, e.g., digital, analog with DAC (digital to analog converter), etc., and the connection type, e.g., wireless, optical fiber, and Ethernet. Sensor components and their connections can form an attack vector if data feedback is manipulated to send deceitful signals or the sensor/connection is disabled.

Actuators

Actuators are physical devices of the cyber layer, able to alter the hydraulic conditions of the physical process by changing the state of physical components with which they are coupled. Actuators wait for input that usually comes in the form of a control signal (e.g., switch on/off) sent from a PLC. In RISKNOUGHT, actuators are coupled to an actionable component of the physical layer. They receive (as input) commands (actions) from Logic components of a connected PLC and subsequently (as output) alter the coupled component's state in the same physical simulation step. Actionable physical network components in EPANET and exposed by WNTR are pumps, valves, and the isolation of pipes. Also, a new actionable object is implemented in RISKNOUGHT, i.e., the flushing unit (representing for example a dual purpose fire hydrant) for removing water from system, e.g., in a contamination event. Actuators are modeled also as feedback devices, i.e., they send an acknowledgement (ACK) signal as part of their communications protocol to inform the controlling PLC that they received the command and executed it. Characteristics that can be attributed to actuators are their type, e.g., servo electric, mechanical, etc. and the connection type, similar to sensors. Actuators and their connections can form attack vectors if disabled and can be manipulated to send false ACK or receive malicious commands.

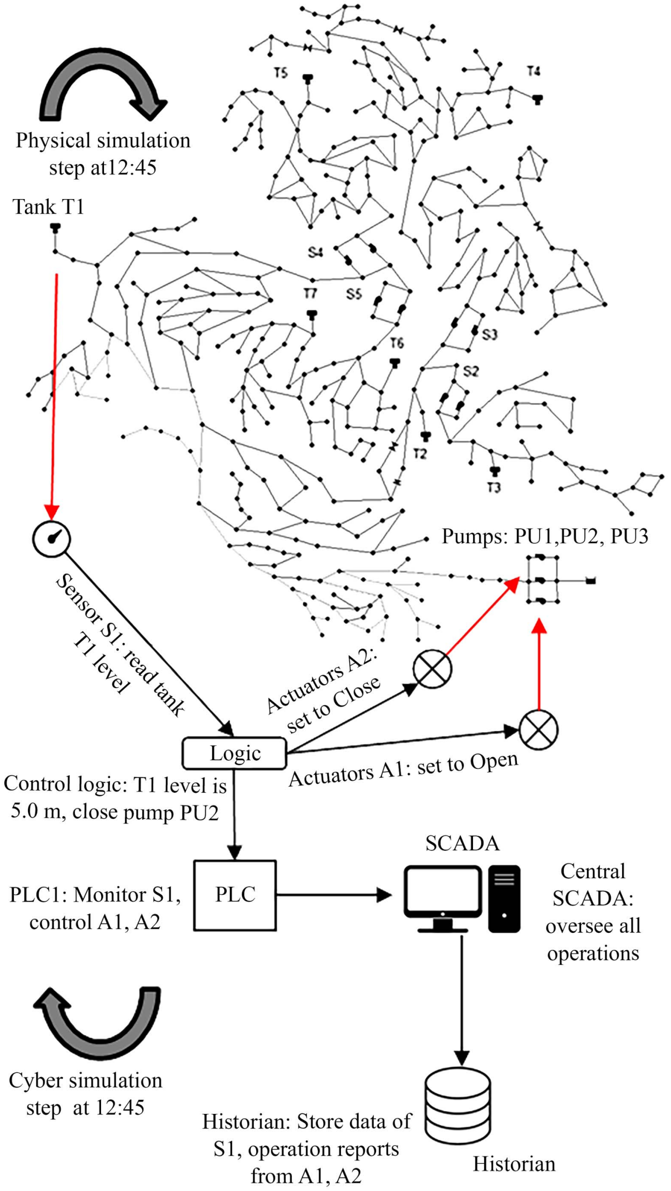

Physical simulation step at12:45
Tank T1
T5
T4
S4
T7
S5
S3
T6
S2
T2
T3
Pumps: PU1,PU2, PU3
Sensor S1: read tank T1 level
Actuators A2: set to Close
Logic
Actuators A1: set to Open
Control logic: T1 level is 5.0 m, close pump PU2
SCADA
PLC1: Monitor S1, control A1, A2
PLC
Central SCADA: oversee all operations
Cyber simulation step at 12:45
Historian: Store data of S1, operation reports from A1, A2
Historian

Fig. 3. Feedback loop example between cyber and physical layers.

Logic Parts

In RISKNOUGHT, all control logic of the distribution network is performed by "virtual" Logic components, which essentially simulate software commands at a very high level. Each distinct command

Table 1. Example of an *AttackEvent* object

Class attributes	Instance values
Name	Attack1
EndTime	10:00
EventType	Sensor manipulation
Target	Sensor1
Special	Assign specific value
Values	10

of the cyber layer forms a new logic object. Logic components in a group are assigned to a PLC, the "nonvirtual" component of the control logic scheme. Logic components can have multiple inputs from sensor data, as well as time data, i.e., information about date time as reported from the physical process, e.g., 07/31/19 12:45:32, or simulation time, e.g., "12:45:32 from simulation start," or data from the Historian stored records, e.g., "the 4-h moving average of node N100 pressure." Multiple inputs can be compared, aggregated, or utilized into complex "and"/"or" boolean-logic operators. Logic components can output all available actions that are sent

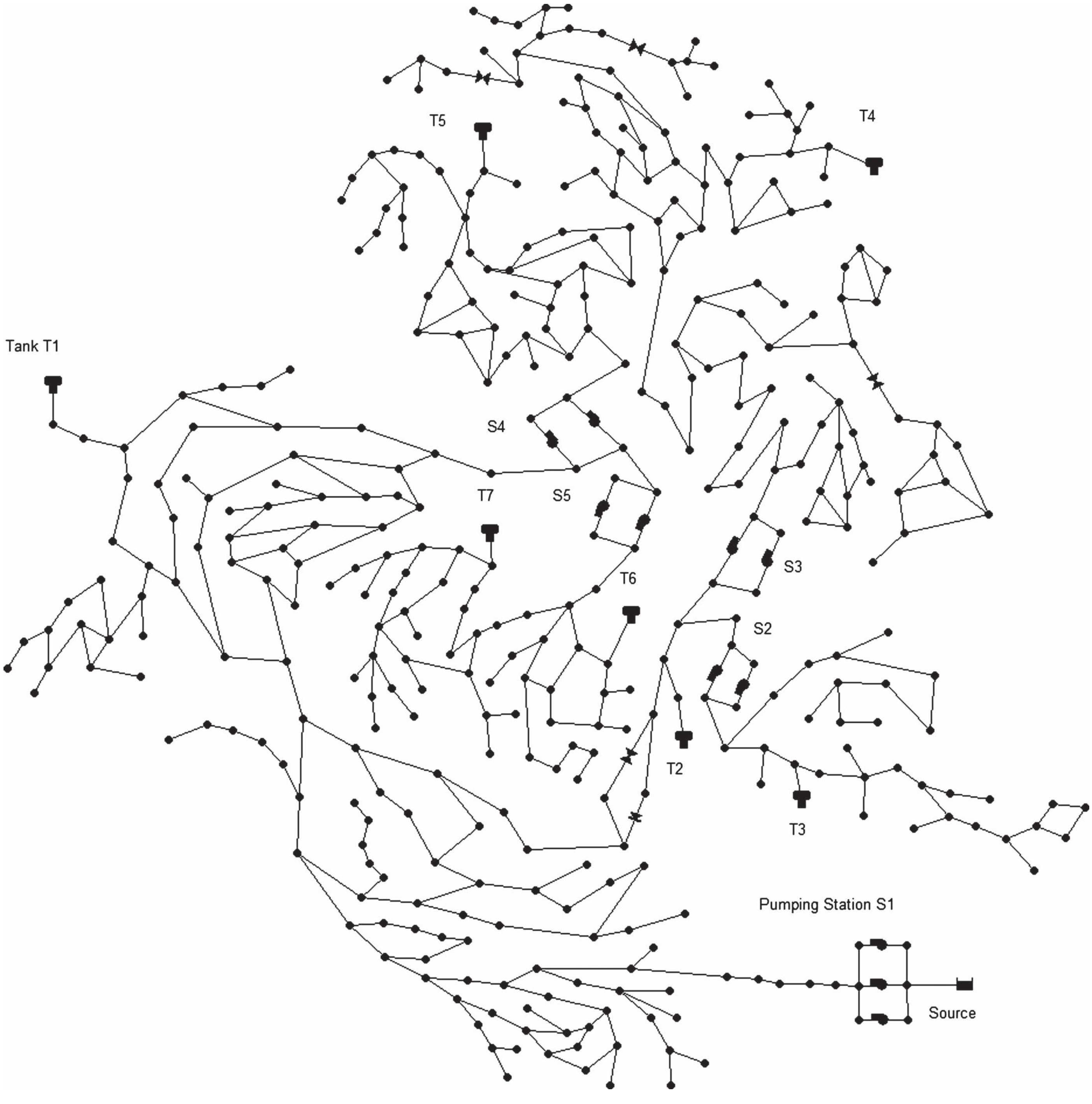


Fig. 4. C-town benchmark model EPANET topology.

to the actuators. With these conventions, advanced control logic can be formulated that extends beyond typical EPANET functionality. If the PLC hosting the logic parts is compromised, control logic can be altered, e.g., change threshold values, reverse switch on/off conditions, suspended certain functions, etc.

PLCs

PLC components act as the physical remote control units [also called remote terminal or remote telemetry units (RTU), with subtle differences in operation] of the cyber layer and are containers for the logic parts, handling the input/output connections and physical operation (i.e., connection to power grid, managing network switches and relays, etc.). In modeling PLCs, there are two options (*slave* and *auto*), according to the communication protocol and design paradigm between the central SCADA unit and the PLCs. In the case of central SCADA systems directly receiving data from PLCs and then issuing commands to the PLC (logic parts are essentially contained by SCADA), the centralized communication protocol is characterized as Master-Slave, and PLCs cannot act autonomously. In contrast, if a distributed or semi-distributed design is in place, PLCs can act without the overseeing of the central SCADA. Because PLCs are networked devices, they can be exploited as an attack vector, e.g., a denial-of-service attack (DoS Attack), physical destruction, etc. Also, because these are the hosts of logic components in RISKNOUGT modeling, the control logic of the system can be altered or manipulated through PLC exploits. The connection type between PLCs and SCADA can be applied as an attribute.

Central SCADA Unit

The central SCADA is responsible for overseeing the entire operation of the CPS and contains the primary HMI in the system. It is the most important component in the cyber layer, because all information from the cyber layer finally flows to the central SCADA for monitoring and control purposes before being stored in the Historian. In RISKNOUGHT the central SCADA unit acts as the hub for all networking processes; therefore in the event of a SCADA downtime PLCs can lose their communications when set to *slave* mode. RISKNOUGHT allows the simulation of multiple discrete SCADA systems operating independently at different areas of a complex network.

Historian

The Historian unit acts like a database server, where information about operations is stored. This includes sensor data time series, status logs of the actuators, and commands issued. Historian units are vulnerable to cyber-physical threats with attacks that target the data

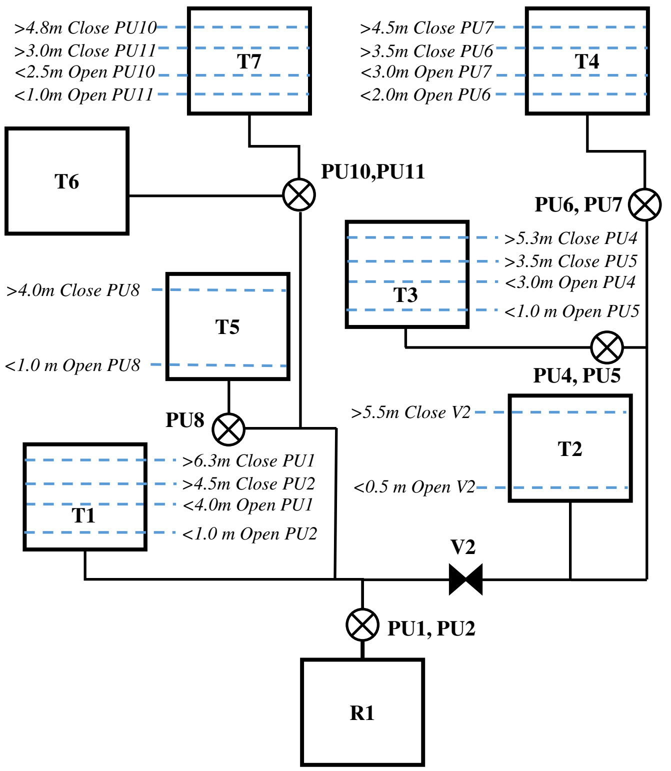


Fig. 5. Schematization of C-town control logic and critical network elements.

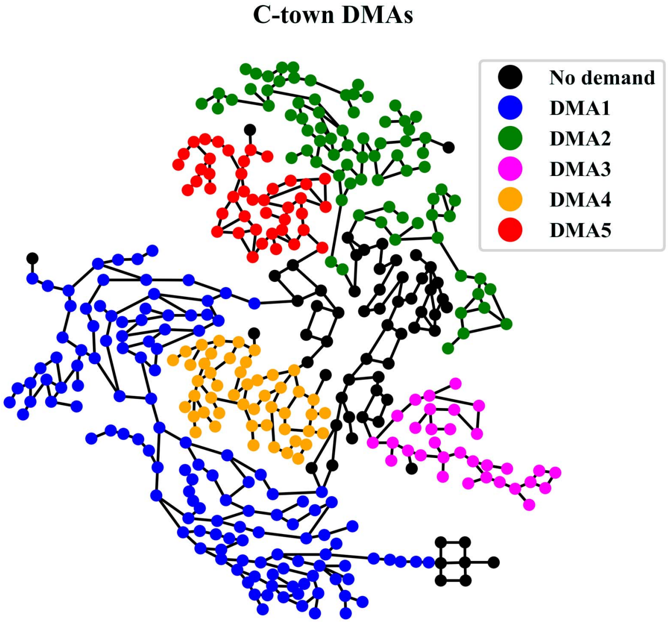


Fig. 6. C-town DMAs, as represented by a modified WNTR graphics method.

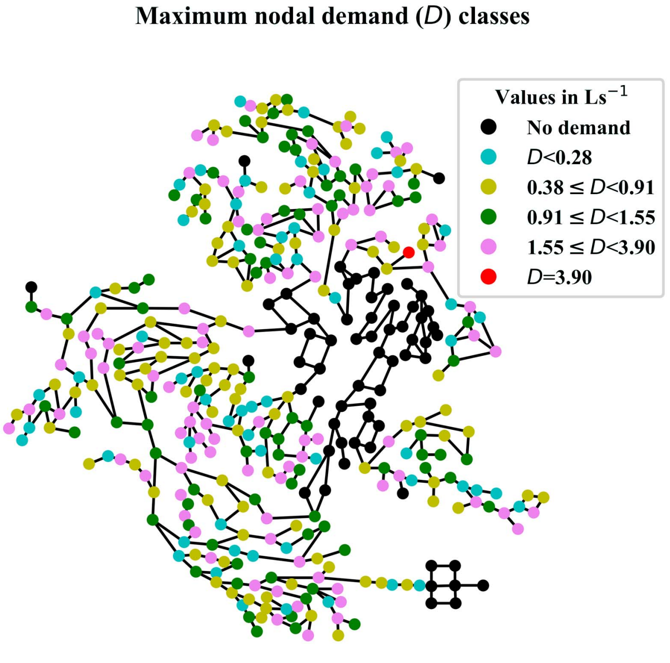


Fig. 7. Maximum nodal demand of C-town in Ls^{-1}.

Table 2. Excerpt from the cyber topology of the C-town CPS in tabular form

ID	Logic part	Sensor	Actuator	PLC
Control1	if Tank('T1').level < = 4.0 then set HeadPump('PU1').status to Open with priority 3	ST1	APU1	PLC1
Control2	if Tank('T1').level > = 6.3 then set HeadPump('PU1').status to Closed with priority 3	ST1	APU1	PLC1
Control5	if Tank('T2').level < = 0.5 then set FCValve('V2').status to Open with priority 3	ST3	AV2	PLC2
Control6	if Tank('T2').level > = 5.5 then set FCValve('V2').status to Closed with priority 3	ST3	AV2	PLC2

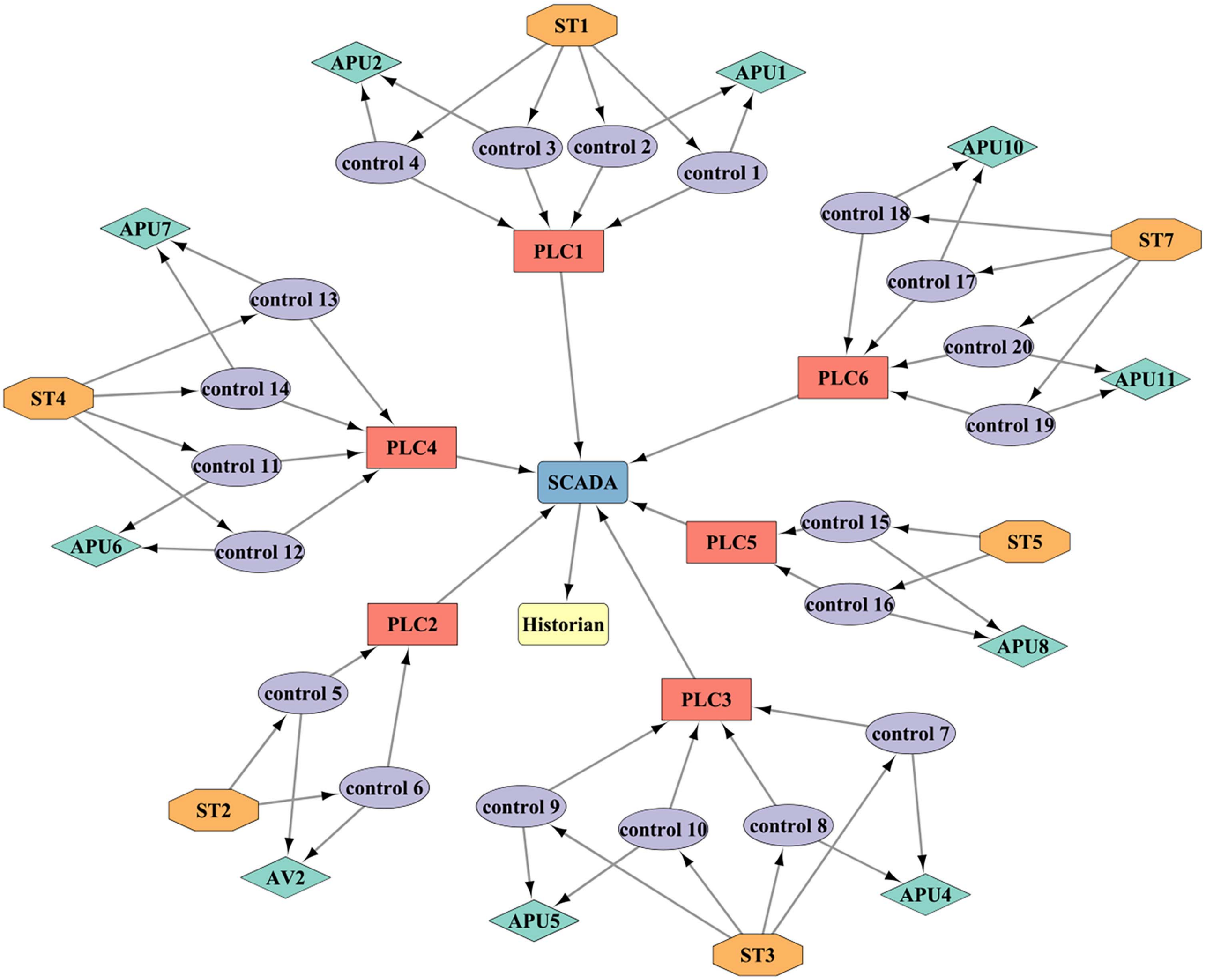


Fig. 8. C-town's cyber layer network view as generated by RISKNOUGHT and visualized by Cytoscape.

itself, like SQL-injection type (Zhu et al. 2011), where it is possible for hackers to issue malicious SQL commands and gain access to the database or even to the whole system, or a DoS attack that prevents communication between SCADA and the server database. Especially when past data is used in a control logic scheme, these attacks can harm operations. Historian units can have attributes discerning the database type and connection type. In the modeling environment of RISKNOUGHT, the Historian is represented as a dataframe of organized logs for each other cyber component, which can also contain some past (i.e., before the simulation starts) data.

Creating a Cyber-Physical Water Distribution Network

Any existing EPANET network model can be transformed into a cyber-physical water distribution network in RISKNOUGHT just by importing an EPANET model in the platform. A new instance (object) of *cpmodel* class is automatically formed, containing a

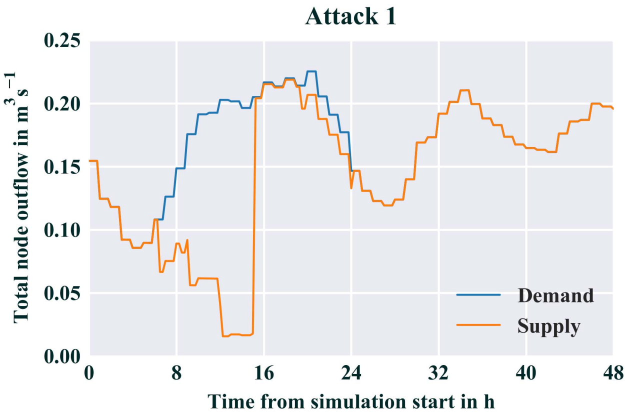


Fig. 9. Total demand versus total supply of water in C-town in attack scenario 1.

WNTR water distribution network object identical to the imported one, except it is stripped from the installed *controls* and *rules*. The new network is coupled with an automatically generated cyber layer instance of *SCADA* class contained within the *cpmodel*, incorporating logic parts that preserve the described functionality of EPANET controls/rules. Sensors are placed at nodes or links that are part of the original control/rule conditions and actuators at the links where an action is performed. All logic parts by default are incorporated into a single PLC, which is connected to a central SCADA that stores its data in a Historian unit. The generated cyber layer can be further modified at will after importing the EPANET model, i.e., add new PLCs and place some of the logic parts to them, add more logic parts, new sensors and actuators, define connections, and other attributes to components. This modification is available through the manipulation of the *cybertopology* object. All properties of the imported physical layer are also customizable, e.g., add new demand patterns, change pump curves, etc.

Because RISKNOUGHT is built on the basis of WNTR, it is possible to define a new *cpmodel* from scratch, starting from the actual creation of the EPANET model (define nodes, links, tanks, demand patterns, etc.) and then create the *cybertopology* object, which spawns the cyber layer.

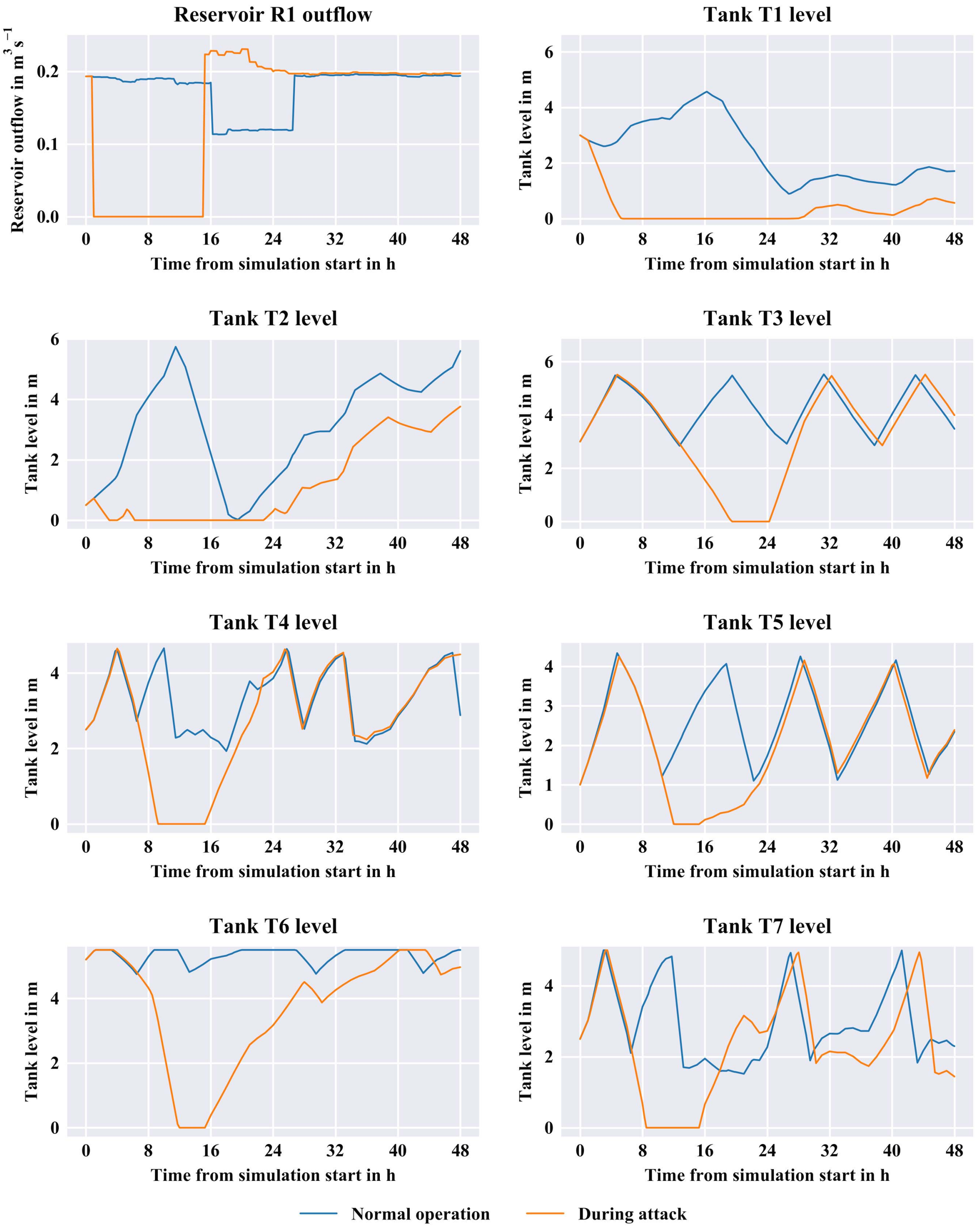


Fig. 10. Major elements' status of C-town during the attack scenario 1 versus normal operation.

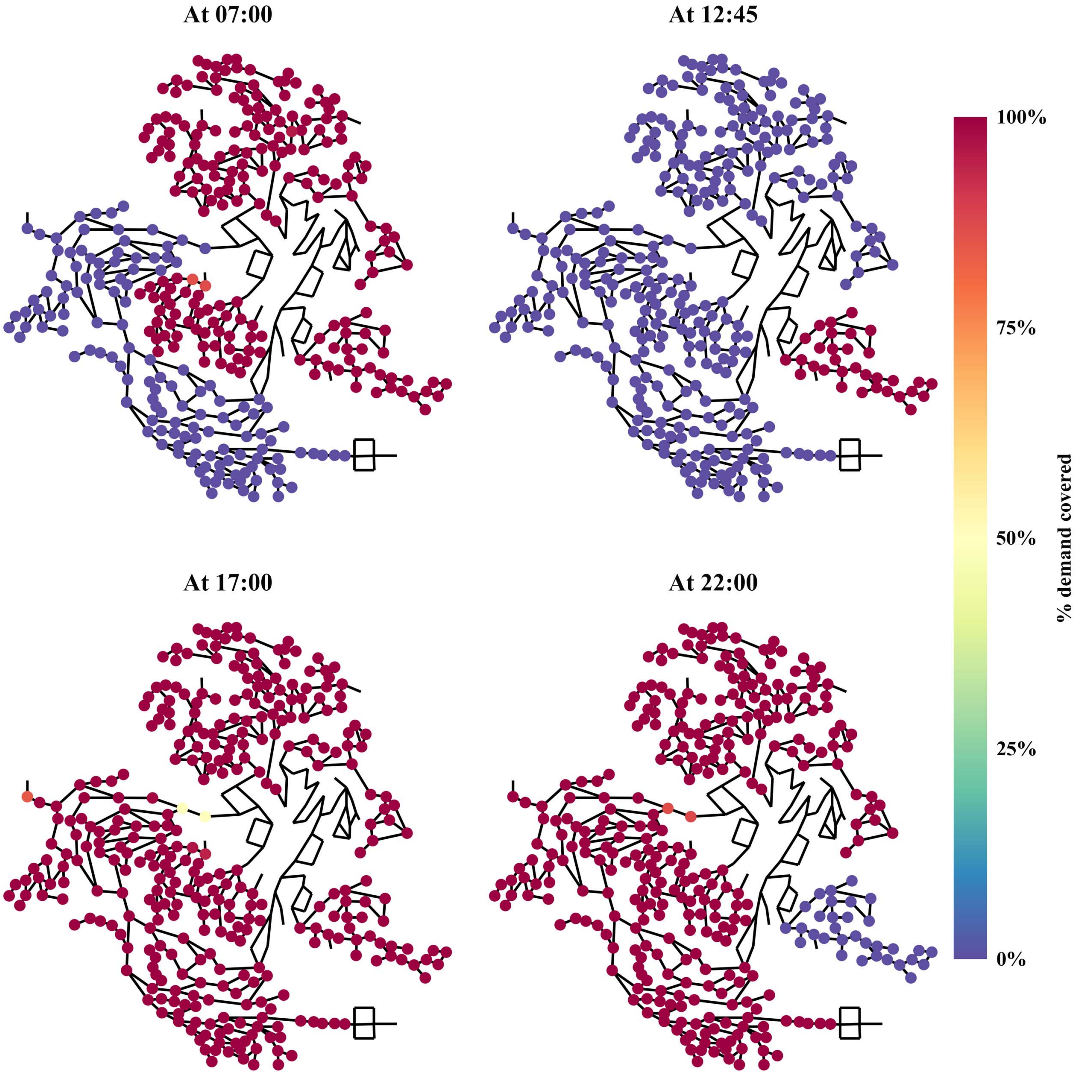


Fig. 11. Spatial representation of affected nodes during attack scenario 1 at different time snapshots. To avoid confusion, nodes without demand are not mapped.

All options available in an EPANET simulation are available in RISKNOUGHT as well, like hydraulic duration, pattern timestep, and hydraulic timestep. By default RISKNOUGHT uses the hydraulic timestep as the cyber simulation step (*cybersimstep* attribute) of the *cpmodel* object, defining the common discrete simulation step in seconds of both the hydraulic process (physical layer) and the control logic of the cyber layer. This functionality is customizable and the *cybersimstep* can be modified at will. Small values of *cybersimstep* can be used to approximate real-time operation control schemes.

Cyber-physical simulation for normal operational conditions without attacks [i.e., business as usual (BAU)] can be performed with the *cyberSimulationBAU* method of the *cpmodel* object. The results of a BAU simulation act as the ground truth to compare with results of the system under cyber-physical attacks (or disruptions/malfunctions/accidental events of the physical layer, which RISKNOUGHT handles as well, but are outside the scope of this article).

Cyber-Physical Attacks Modelling

In order to model cyber-physical attacks, RISKNOUGHT employs an *AttackEvent* class, each instance of which holds the information that define a single generic attack event, i.e., start time, end time, event type, target, special characteristics of the attack (if any, from a predefined dictionary), and special values to be used in the attack generation (if any). An example use of the attributes could be seen in tabular form in Table 1, where an attack event occurs between 01:00 and 10:00, manipulating the sensor readings of Sensor1, by assigning a constant value of 10.

More than one *AttackEvent* instance can be executed in the same cyber-physical simulation, making the cyber-attack as complex as the modeler needs. The *AttackEvent* instances can be overlapping or not, or have the same or different targets without restrictions. *AttackEvent* instances are passed in Python list format as argument to a *cpmodel* method called *cpa_simulation*, which performs the simulation of the compromised system.

In order to execute the cyber-physical simulation under attack, the *cpa_simulation* method passes information from *cpmodel* and *AttackEvent* objects to an instance of the helper class *cpaEventManager*, which implements most of the methods of altering the behavior of the cyber layer. Without going into coding detail, these include the methods to perform attacks on sensors, actuators, logic parts, PLCs, central SCADA, and Historian units. The *cpaEventManager* updates every simulation step both the cyber and the physical layers.

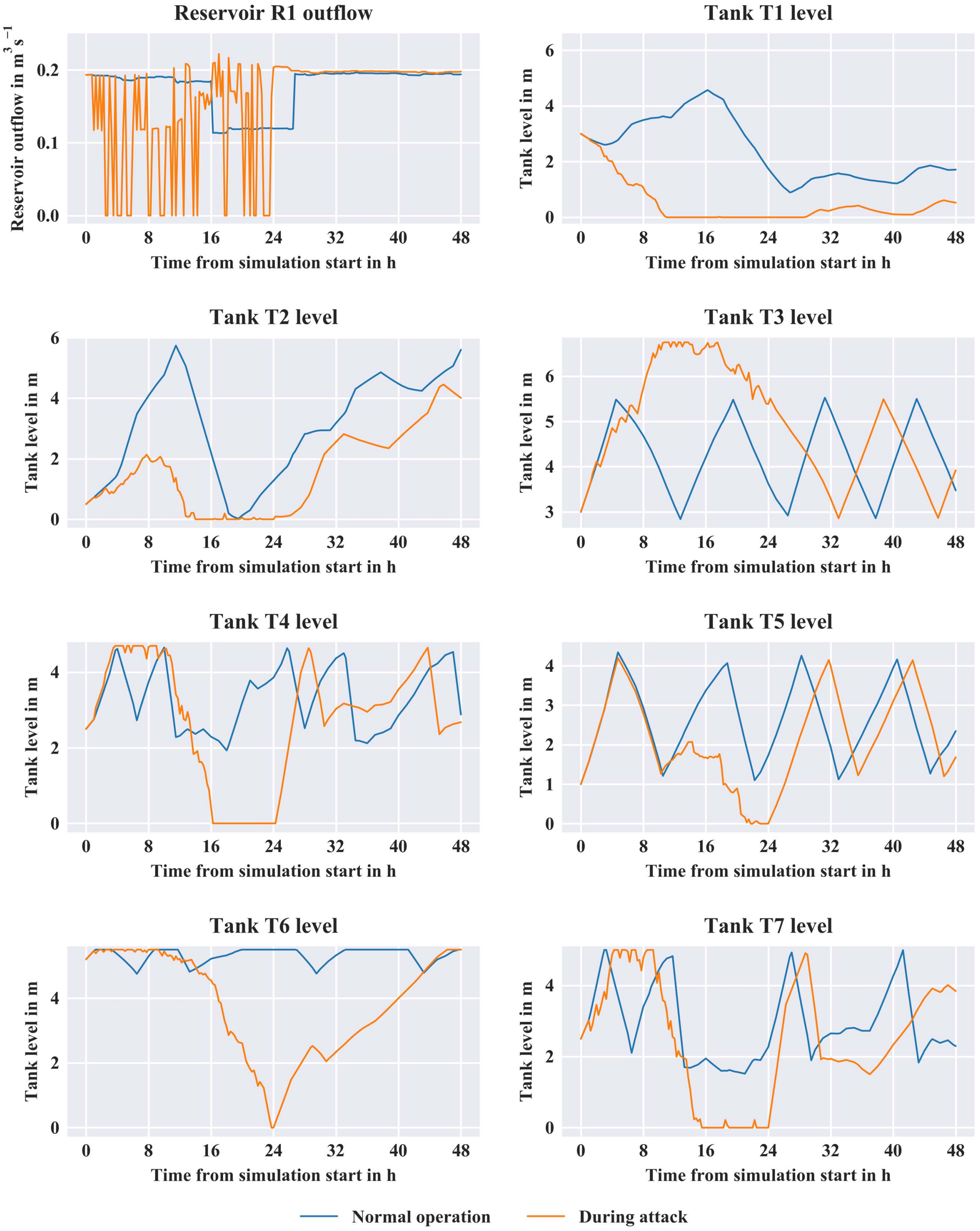


Fig. 12. Major elements' status of C-town during the attack scenario 2 versus normal operation.

In the current version, RISKNOUGHT is able to simulate several types of cyber-attacks and is under active development to enrich them. What is now available can be summarized by target in the following list:

- Sensor: DoS on the connection with PLC, data manipulation types: assign specific value or time series to output data, do not let the sensor update output data, replace output data values from a sinewave function, add random noise to output data.
- Actuator: DoS on the connection with PLC, action manipulation by: do not send ACK and do not perform action, send ACK and perform random action, send ACK and do not perform action, do not send ACK and perform action.
- Logic part: modify the logic part by: change threshold, change action output, delete logic part, suspend logic part from execution.
- PLC: DoS on the connection with central SCADA, allow exploitation of logic parts.
- Central SCADA: DoS on all connections.
- Historian: SQL injection attacks that lead to data loss or replacing data by: specific time series, random values.

Proof-of-Concept Setup

Benchmark Cyber-Physical Topology

The benchmark model of C-town (Ostfeld et al. 2012) is used as a proof-of-concept case study in order to showcase RISKNOUGHT capabilities. C-town is based on a real-world medium sized network and consists of one reservoir, seven tanks, 388 demand junctions, 429 pipes, eleven head pumps and four valves [three pressure relief valves (PRV), one flow control valve (FCV)]. This benchmark is used extensively in the literature for various studies (e.g., Chandy et al. 2018; Mahmoud et al. 2017; Pesantez et al. 2019; Sankary and Ostfeld 2019). The EPANET network topology is displayed in Fig. 4. The main pumping station S1 feeds the network water from the reservoir Source and has three pumps, PU1, PU2, and PU3. Pumps PU1 and PU2 are operated with regard to the water level in tank T1, while PU3 is a redundant pump that is kept off during standard operating conditions. The secondary branch pertaining to T2 is connected to the reservoir through valve V1, which is regulated by the water level in T2. There are five more tanks (T3, T4, T5, T6, and T7) refilled by four secondary booster stations that pump water from T1 and T2, namely pumping station S2 employing PU4 and PU5 to refill T3; S3 employing PU6 and PU7 to refill T4; S4 employing PU8 and PU9 to refill T5; and finally S5 employing PU10 and PU11 to refill T6 and T7. The connections and the control logic are schematized in Fig. 5. In the particular setup PU9 remains closed like PU3, and all other have controls based on the water level in the respective tank they refill. C-town encompasses five DMAs (District Metered Areas), each with its

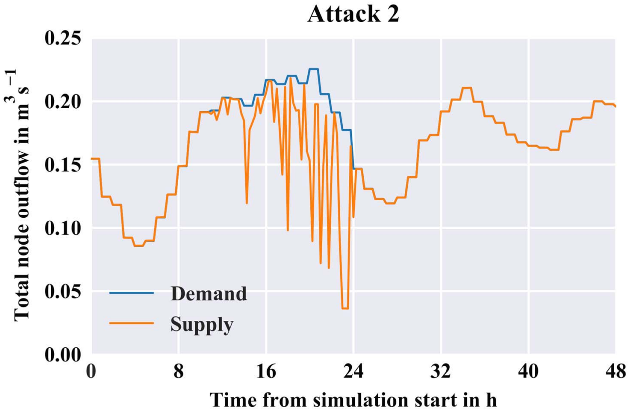


Fig. 13. Total demand versus total supply of water in C-town in attack scenario 2.

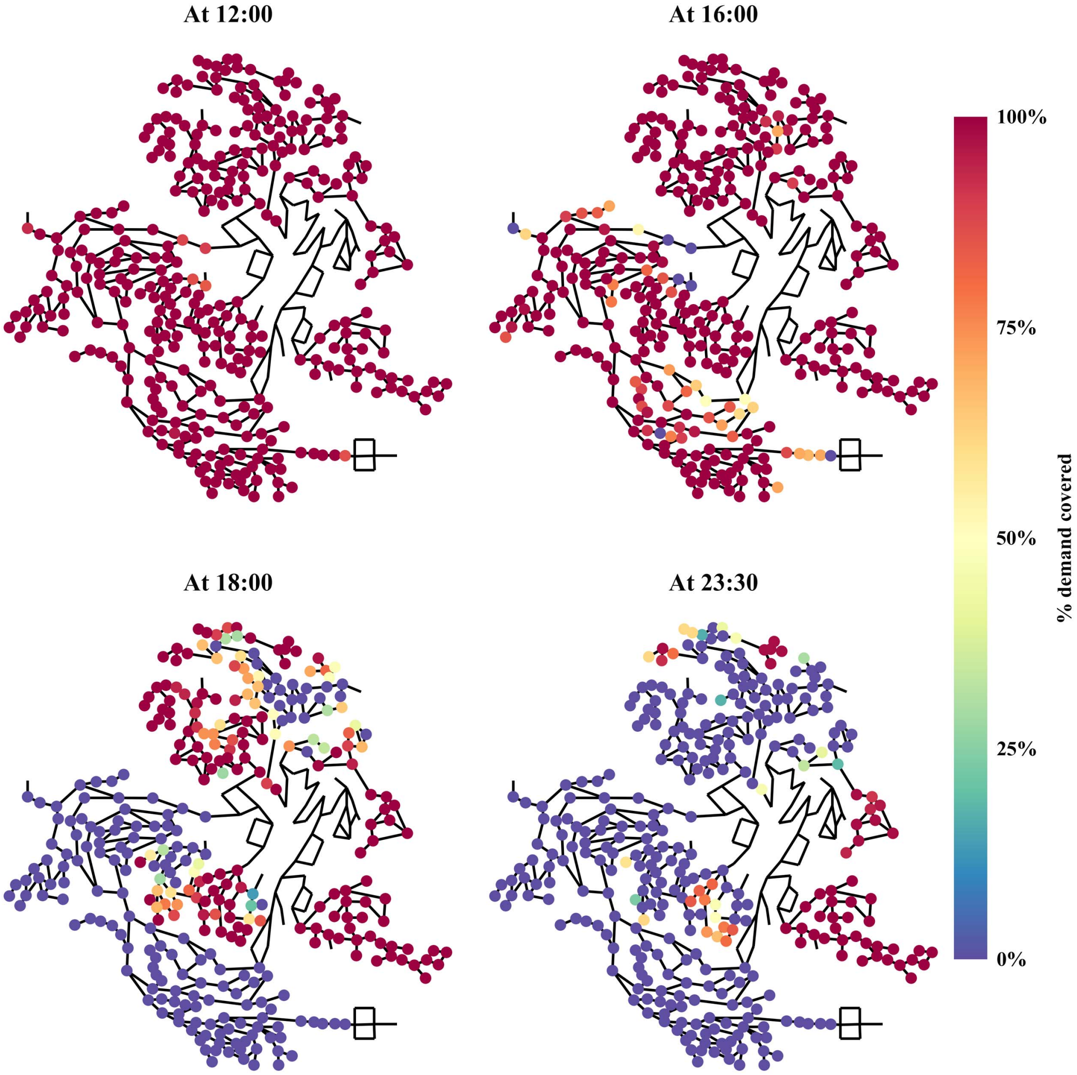


Fig. 14. Spatial representation of affected nodes during attack scenario 2 at different time snapshots. To avoid confusion, nodes without demand are not mapped.

own demand pattern (nodes in the same DMA can have different base demands), as seen in Fig. 6. The five hourly demand patterns cover a period of 168 h (a full week). By multiplying the patterns with nodes base demands, the demand at nodes ranges from 1.15e-07 to 0.0039 $m^3 s^{-1}$ (1.15e-04 to 3.9 $L s^{-1}$), with maximum nodal demand plotted in Fig. 7. For the purposes of PDA simulation, for convenience the nominal P_{nom} and minimum P_{min} pressure levels for Wagner equations are set to 20.0 m and 0.0 m, respectively, for every node, which are characteristic values typically seen in the literature (Morley and Tricarico 2008). The hydraulic timestep is set to 15 min (900 s), and the simulation starts from time 0:00.

By importing the .inp file format EPANET topology in RISKNOUGHT, the cyber topology with control logic of is automatically generated, and by default all control logic is attributed to a single PLC (namely PLC1). The cyber topology is then modified interactively to account for six different PLCs. In Table 2 an excerpt from the topology is tabularized. The complete cyber topology can be found in the Appendix, and the network graph is visualized by exporting from RISKNOUGHT to Cytoscape (Shannon et al. 2003) in Fig. 8. The value of *cybersimstep* is set to 900 s, unchanged from the original hydraulic one.

Cyber-Physical Attacks

For the demonstration of cyber-physical attacks, five attack scenarios are formed, comprising the case of a perpetrator remotely gaining access to controls or exploiting vulnerabilities in order to alter the physical processes of the system. It is assumed that no other human intervention is possible, for instance from the SCADA's staff through the duration of the attacks (e.g., turning the system on manual mode).

Attack Scenario 1: Manipulation of Sensors
In this scenario, a perpetrator manipulates the readings of the Sensors ST1 and ST3.

- The attack on Sensor ST1 occurs between 01:00 and 15:00, with the Sensor deceptively reporting a tank level of 6.9 m, i.e., at full capacity.
- The attack on ST3 occurs between 12:00 and 0:00 of the following day, with the Sensor deceptively reporting a tank level of 5.9 m, i.e., at full capacity.

Attack 2: Exploitation of Actuators
In this scenario, a perpetrator exploits a zero-day vulnerability [i.e., a previously unknown, thus unpatched, software vulnerability (Ayala 2016)] in the networking components of the actuators controlling pumps in the system, while the V2 valve employs a different type of network components and is unaffected. The attacker manages to issue repeating random commands (open/close) to each pump unit individually instead of the actual command issued by the systems control logic. Actuators also deceptively respond back with an ACK signal, so the attack goes unnoticed for long. Attack starts simultaneously for all actuators at 1:00 and ends at 0:00 of the following day.

Attack 3: SCADA DoS Attack
Attack scenario 3 comprises a successful DoS attack of the perpetrator to the central SCADA system that enables all the networking functions of the cyber layer. It is assumed that the PLCs of the system are connected through a Master-Slave communication protocol. The DoS attack manages to completely cut off connections between SCADA and PLCs, and as the networking functions depend on the central SCADA, between sensors and actuators to PLCs. The attack is initialized at 01:00 and ends at 11:00.

Attack 4: SCADA DoS Attack with Insider Knowledge
Attack scenario 4 is a variant of attack scenario 3, where the perpetrator has insider knowledge of the best timing to initialize the DoS attack. This can happen either through having a collaborator in the staff, or by possessing the required knowledge of water distribution systems and snooping through the data in the compromised HMI (e.g., through access of the Historian database). The attack duration is the same as in attack 3, but the timing is different; the start time is at 5:00 to 15:00, when most of the systems pumps are off.

Attack 5: SCADA DoS Attack with Insider Knowledge on a Semidistributed System
Attack scenario 5 is a variant of attack scenario 4, where the perpetrator has insider knowledge of the best timing to initialize the DoS attack; however, some parts of the cyber layer are modernized and operate in a semiautomatic, distributed way. It is assumed that the cyber infrastructure of the secondary branch pertaining to T2 with PLC2, PLC3, and PLC4 is modernized, allowing it to operate without input from SCADA (in *auto* mode in event of lost communication with SCADA), and with new communication links between the components of the branch. The attack occurs between 5:00 to 15:00, like attack scenario 4.

Results

Attack Scenario 1 Results

The total demand versus total supply of water during the attack of scenario 1 is presented in Fig. 9. As communicated by the large difference of the two aggregated time series, attack 1 is quite severe. The total volume of water not delivered equals 4,268.32 m^3. Detailed analysis of tank levels and reservoir outflow, shown in Fig. 10, explains the physical effect of the attack. The deceptive signal of ST1, leads the control logic of PLC1 to shut down the main pumps PU1 and PU2, and the primary tanks T1 and T2 start to empty, when they are supposed to refill with water. By the time the second attack starts at ST3 leading to the shutting down of PU4 and PU5 by the control logic of PLC2, only T3 has still water in storage and DMA3 is the only area still served. As time progresses, the first attack ends; however, the lasting second attack manages to cut-off supply in DM3 as well, while other DMA's recover operational status. The spatial effect of the attack is depicted in Fig. 11 at different snapshots. An animation of the complete system behavior

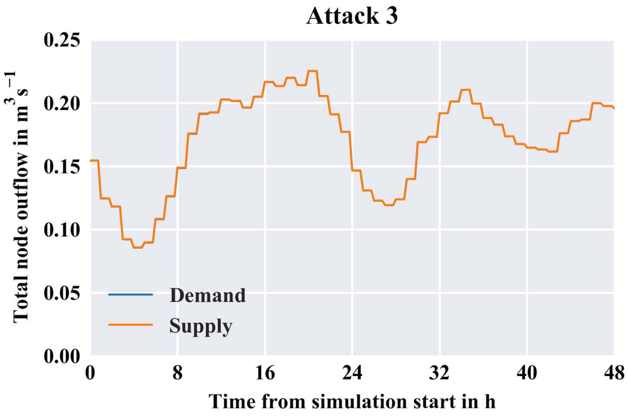


Fig. 15. Total demand versus total supply of water in C-town in attack scenario 3.

in the duration of the cyber-physical simulation can be found in the supplementary material. Interestingly, as seen in Fig. 10, the attack has a lasting hydraulic effect, even when supply recovers, as the system struggles to refill the primary tank T1.

Attack Scenario 2 Results

Attack scenario 2 has a wider range of implications in the system. As shown in Fig. 12, the outflow of the reservoir is substantially varying during the attack, due to the random powering on and off of PU1 and PU2. This finally leads to the emptying of T1 and T2, with cascading effects to other tanks in the system that are fed from the primary tanks, by the other also randomly actuated pumps of the system. This attack, however, does not have a rapid effect on the supply of water as showcased by the aggregated demand versus supply time series of Fig. 13. Actually, there is a lag of several hours from the start of the attack to the actual first supply problems. Also, the random actuation of pumps, and in particular the main ones, allows the system some leeway through the attack's duration to supply intermittently water to the DMAs as depicted in Fig. 14 and animated in supplementary material. In total, 1,719.12 m^3 of water are not delivered to consumers.

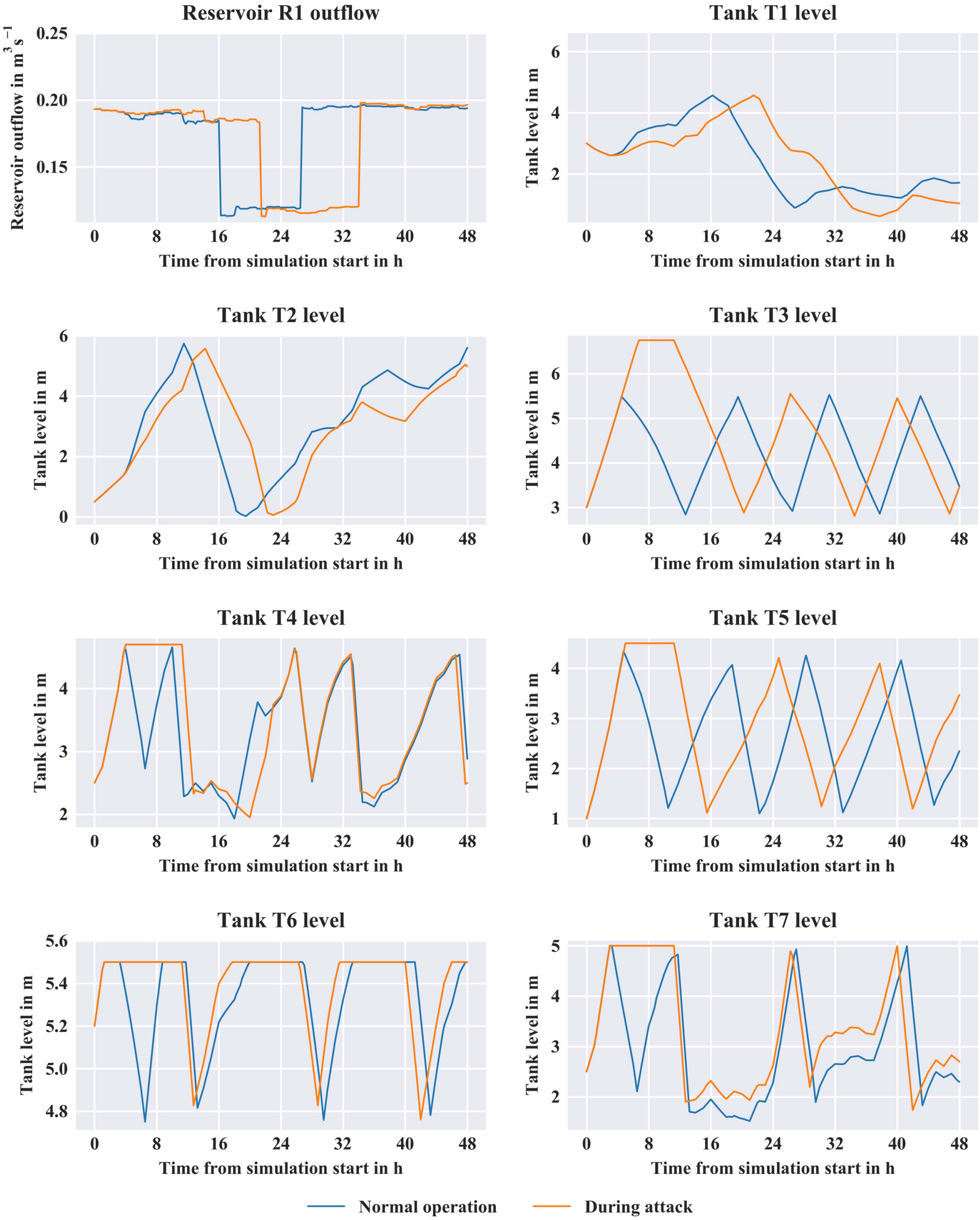


Fig. 16. Major elements' status of C-town during the attack scenario 3 versus normal operation.

Attack Scenario 3 Results

Attack scenario 3 is unique, because the effect of the attack is not perceptible by the costumers; therefore the attack can go unnoticed by the public if undisclosed. As seen in Fig. 15, demand is met throughout the cyber-physical simulation period. This fortunate outcome is based on the fact that at the time of the attack six of the pumps, including the main ones are in operation (PU1, PU2, PU4, PU7, PU8, and PU10) and the important to the secondary branch V2 open, and therefore all DMAs were served by at least one pump. Of course, though, the hydraulic behavior is altered, as can be seen in Fig. 16; however, the system has more than enough redundancy with storage and head/flow rate from the six pumps to continue operating.

Attack Scenario 4 Results

In contrast to attack scenario 3, attack scenario 4 poses significant challenges to the system. The timing of the attack coincides with only the main pumps in operation and V2 open. Therefore as time progresses, tanks T4, T5, T6, and T7 empty (Fig. 17), leaving DMA2, DMA4, and DMA5 unserved (Fig. 18). In total, 1,745.27 m^3 of water is not delivered, as presented in Fig. 19.

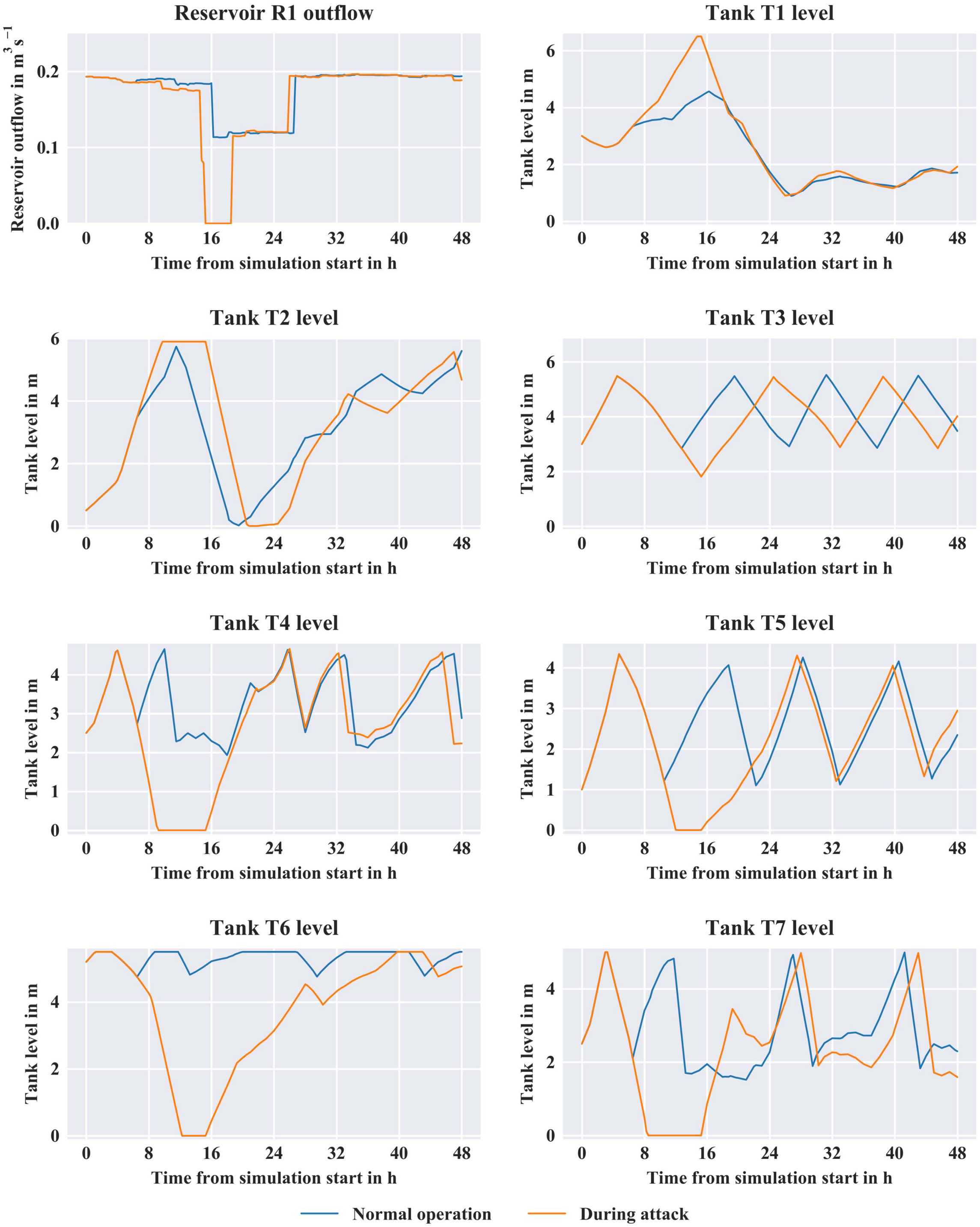


Fig. 17. Major elements' status of C-town during the attack scenario 4 versus normal operation.

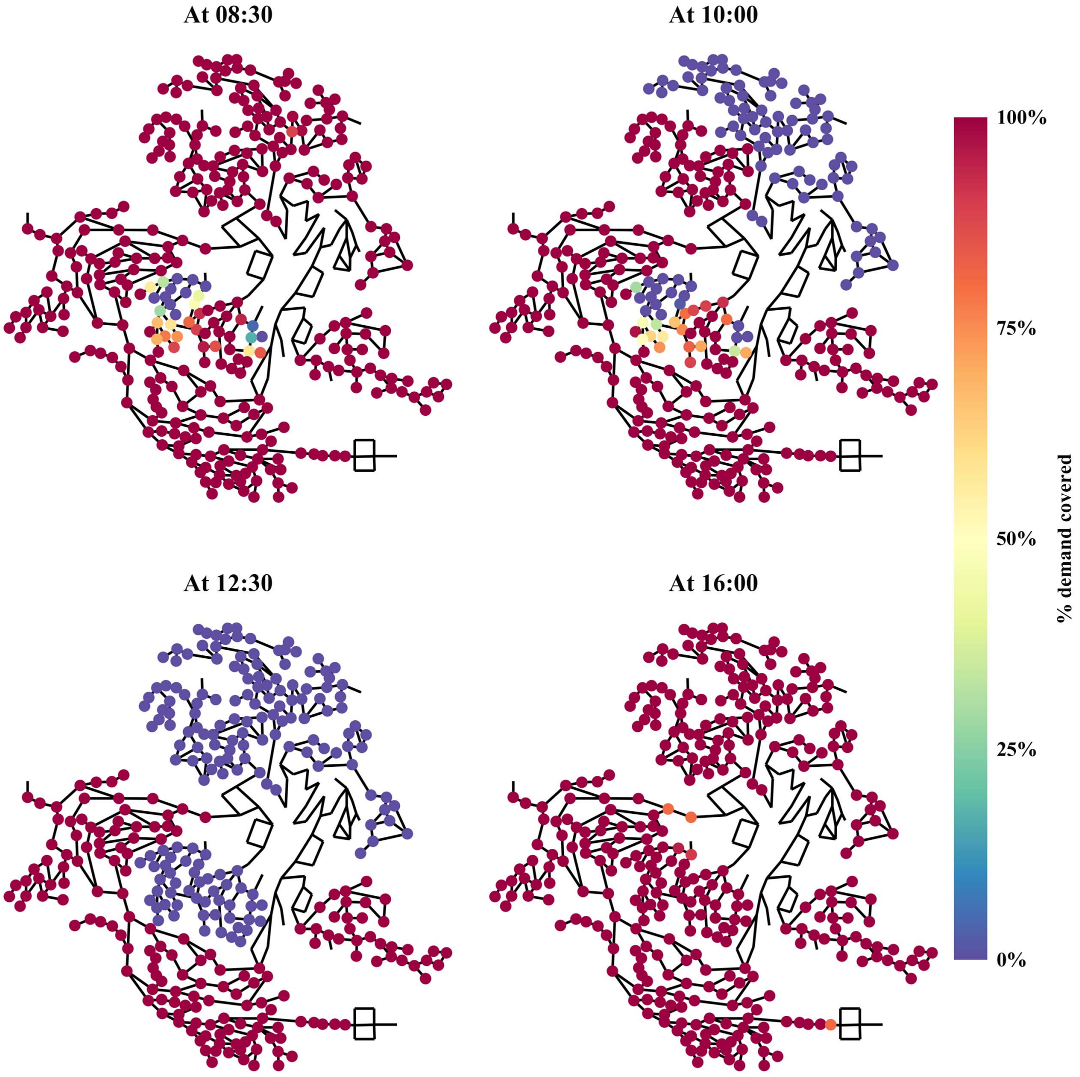


Fig. 18. Spatial representation of affected nodes during attack scenario 4 at different time snapshots. To avoid confusion, nodes without demand are not mapped.

Attack Scenario 5 Results

The modernized cyber layer in attack scenario 5 manages to mitigate the effect of the DoS attack on the central SCADA compared to otherwise identical attack scenario 4. As seen in Fig. 20, there is a substantial reduction in volume not delivered, which amounts to 734.38 m^3. The autonomous operation of PLC2, PLC3 and PLC4 allowed T2, T3 and T4 to operate practically as they should during the attack, as depicted in Fig. 21. Compared to scenario 4, DMA2's level of service remains unaltered, whereas only DMA4 and DMA5

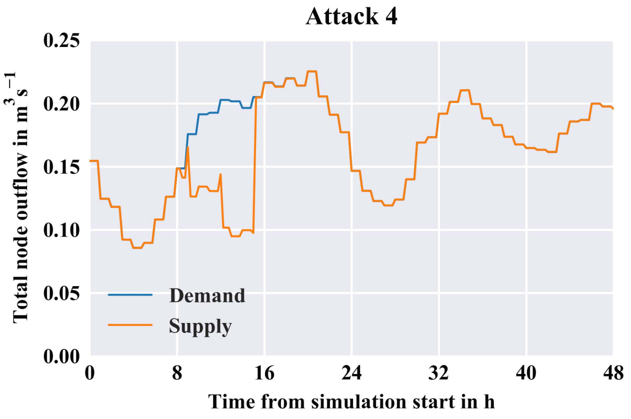


Fig. 19. Total demand versus total supply of water in C-town in attack scenario 4.

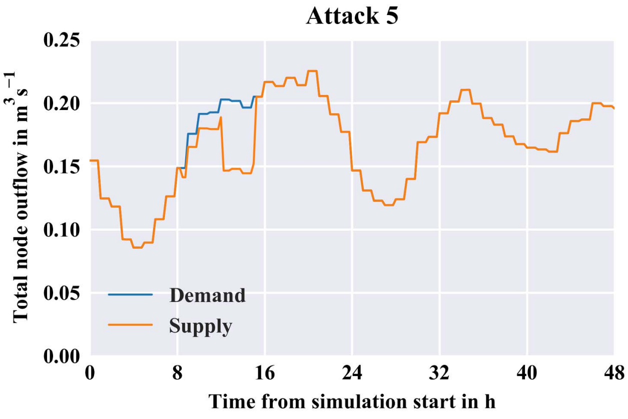


Fig. 20. Total demand versus total supply of water in C-town in attack scenario 4.

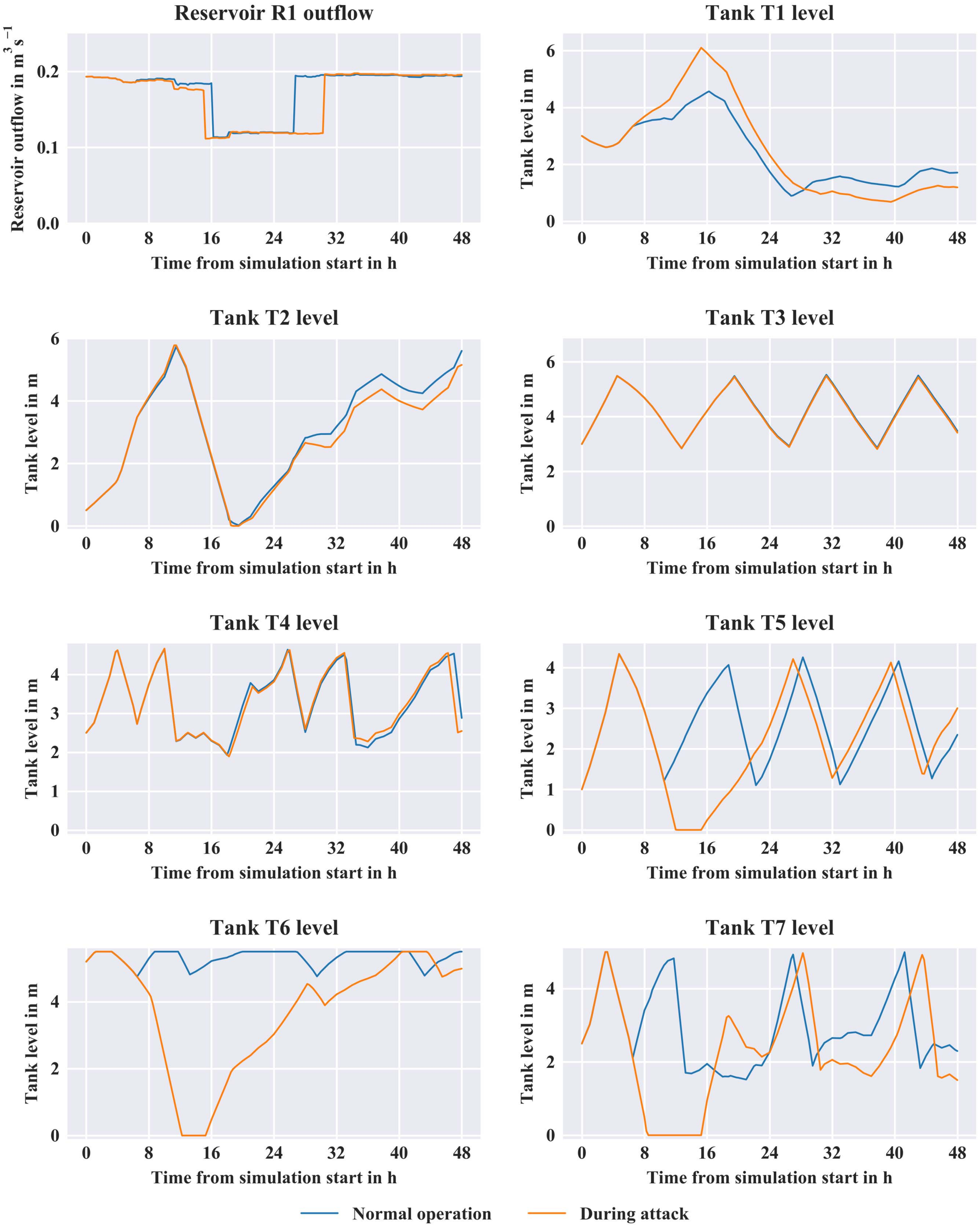


Fig. 21. Major elements' status of C-town during the attack scenario 5 versus normal operation.

experience supply problems and ultimately cut-off, as shown in Fig. 22.

Discussion

Cyber-Physical Simulation of C-Town

The deployment of RISKNOUGHT cyber-physical stress testing modeling platform on the C-town benchmark model highlights the platform's capability of both: (a) simulating the distribution system as a CPS, i.e., a physical process governed by a control logic cyber layer; and (b) assessing the effect of cyber-physical threats on water distribution networks. For the latter, the model captures effectively the interplay between altered command signals and the hydraulic response, which potentially leads to service unavailability or has lasting hydraulic consequences with the emptying of tanks and pressure drops. Attacks that target sensitive control instruments could have adverse effects given enough time, as in the case of attack scenario 1 and 2. Scenario 1 only targets specific sensors in order to make the attack felt ultimately in all DMAs in C-town, whereas scenario 2 targets all instances of a type

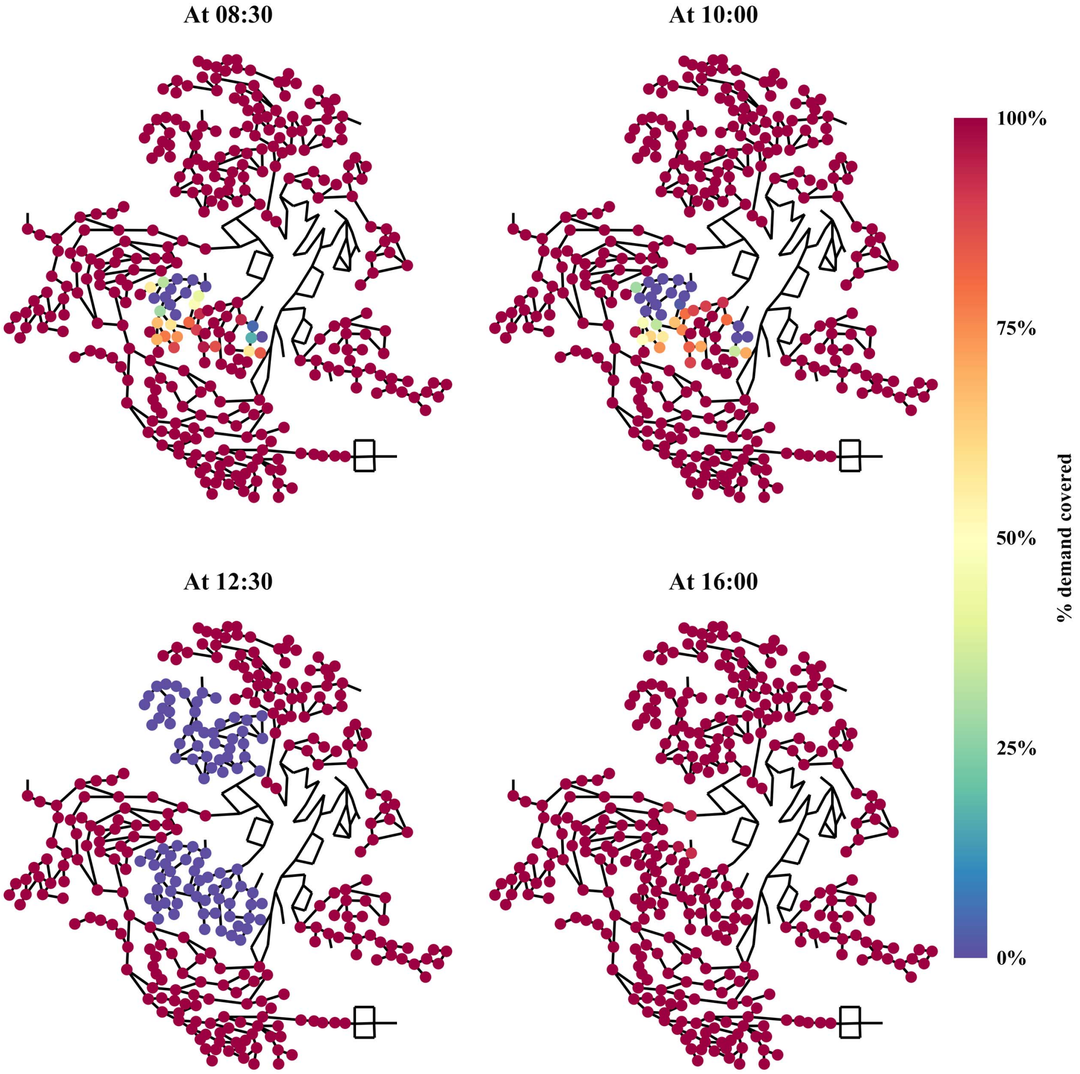


Fig. 22. Spatial representation of affected nodes during attack scenario 5 at different time snapshots. To avoid confusion, nodes without demand are not mapped.

of component in the network bringing chaos with different local nodes being out of supply intermittently at each simulation step. The modeling of full-blown DoS attacks on the SCADA validates the possibility of such attacks being particularly severe to water distribution systems. This is evident especially when there is knowledge for how and when to perform the attack as demonstrated in attack scenario 4 versus attack scenario 3, which had no detrimental effects on the system. Interestingly, design philosophy shifts in managing cyber elements, as the semidistributed scheme if scenario 5, can successfully mitigate risk and impact, and some changes can be incorporated in the RISKNOUGHT cyber-physical stress-testing platform.

Remarkably, as shown from the results of all examined scenarios, most attacks need time to unravel and have perceptible negative effects on the system. C-town, being a medium sized system seems to implement enough built-in redundancy in the form of water stored in tanks, number of parallel pumps, isolated DMAs, etc., to withstand cyber-physical attacks for enough time for operators to counter the attacks. This suggests that time is crucial for recovery in water distribution system cyber-security and risk management plans should focus on minimizing response time.

Insights for the Cyber-Physical Stress Testing Platform

The simulation-based approach of two coupled interactive models allows the representation of the information flow from the physical components to the cyber layer devices and the complete feedback loop of issuing commands and gathering new readings.

The cyber layer model of RISKNOUGHT provides a low-fidelity simulation option, in the sense of not emulating the actual low-level function of the networked devices and the software running in the SCADA but rather aiming on simulating the interactions between components and the impact these interactions have on physical assets. However, this approach yields a high-exploration ability, i.e., a multitude of complex attack scenarios can be tested without knowing how the perpetrator will succeed but focusing on what implications the attack will impose to the physical processes. Nonetheless, RISKNOUGHT cyber layer is customizable and with proper attributes in the components more detailed simulation of attacks can be performed, like a targeted attack to specific brands of sensors, if such real world vulnerability is discovered. This makes RISKNOUGHT suitable for users who need to assess security of their water distribution network, at a higher level, i.e., for informing strategic decisions, rather than IT experts, who focus at the actual protection and patching of software and hardware components.

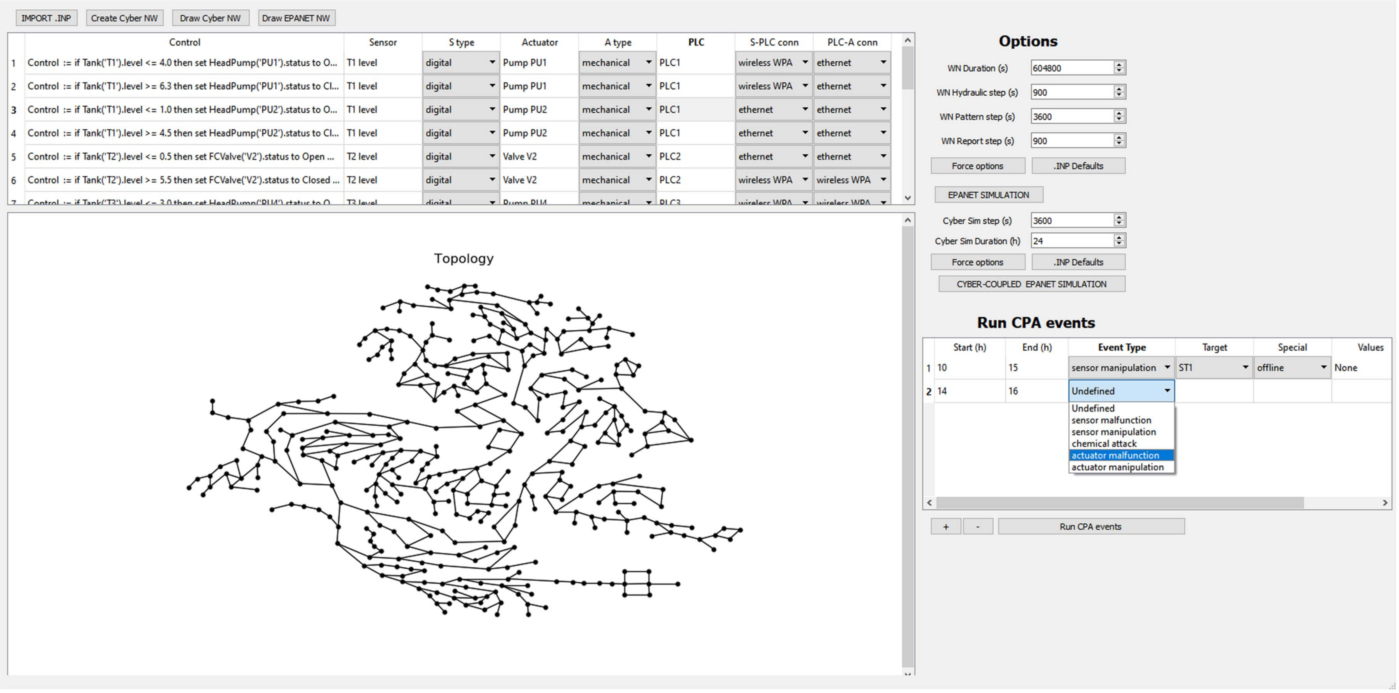
Moreover, the assembly of the cyber layer conveniently requires little input from the user when importing an existing EPANET network file, because it is automatically generated from EPANET rules and controls and requires minor customization from the user, if needed. The supported attacks on the distribution network are easily declared for cyber-physical modeling. This is in contrast with other cyber-physical simulation tools like epanetCPA, which require additional user-constructed structured files (for instance, a text .cpa file in epanetCPA) to pass the necessary cyber topology and definition of cyber-attacks. Also, RISKNOUGHT is built on top of open source libraries and packages, and does not depend on proprietary licensed software like MATLAB. Because it is a Python based application, users can interface it with a multitude of other third party packages ensuring future extensibility. A graphical user interface (GUI) is currently under development, to aid inexperienced in Python scripting users formulate their case studies. A working example of the GUI is shown in Fig. 23.

On the physical layer side, the EPANET solver, as adapted by the WNTR simulator, produces realistic pressure deficient conditions that result in service unavailability in affected DMAs. The ability to simulate pressure deficient conditions is a prerequisite when assessing the effect of prolonged or severe cyber-physical attacks as showcased by the attack scenarios examined. Moreover, RISKNOUGHT includes tools to assign different nominal and minimum pressure characteristics for the PDA analysis per node, as opposed to the uniform 20.0 m nominal – 0.0 m minimum pressure settings used in the proof-of-concept set-up. Testing RISKNOUGHT to a new hydraulically conditioned benchmark network with defined pressure zones should yield interesting and diverse results.

The present study has also focused solely on attacks that target quantity (i.e., unmet demands) in water distribution systems. However, the interfacing of RISKNOUGHT with WNTR also enables the possibility to run quality simulations with EPANET as the quality solver during the cyber-physical simulation, which currently is not supported by other cyber-physical tools like epanetCPA. The control logic built-in the cyber layer allows conditions to be set for quality indices and several quality related actions for flushing contaminants or, for instance, isolating DMAs. However, the original EPANET quality solver is not sophisticated enough for usage in complex contamination scenarios where the interaction of multiple chemical (or biological) species is necessary to produce accurate results for risk assessment and management, and also recent research found inconsistencies in quality modeling (Davis et al. 2018). It is entirely possible nonetheless to perform cyber-physical attacks involving at the same time contamination events using RISKNOUGHT. Still, the authors refrained at this stage from showcasing such scenarios and focused on quantitative CPS threats, aiming at substantially extending qualitative functionality before presenting results. Further development of RISKNOUGHT aims at interfacing the package with EPANET-MSX extension (Shang et al. 2008) to handle complex quality modeling and simulation.

With regards to the representation and interpretation of results stemming from cyber-simulation, the authors suggest that a comprehensive, generic, and software-agnostic framework of performance indicators for cyber-physical water distribution networks is needed in the emerging field of water system cyber-security.

A final note with regards to the inputs (e.g., demand time series, etc.) of the model per se. In this work we formulated the problem as a deterministic one, while a possible reformulation could view it as a stochastic one. In such a formulation, one could take advantage of a well-established hydrological paradigm, and employ the notion of synthetic time series. Recent advances in the domain of stochastic hydrology (Tsoukalas et al. 2017, 2018a, b) offer novel (copula-based) models that move beyond the classical, yet risky, paradigm of moment-based processes representation (Tsoukalas et al. 2018c), and are able to simulate a wide range of processes of any time scale, explicitly reproducing any marginal distribution



	Control	Sensor	S type	Actuator	A type	PLC	S-PLC conn	PLC-A conn
1	Control := if Tank('T1').level <= 4.0 then set HeadPump('PU1').status to O...	T1 level	digital	Pump PU1	mechanical	PLC1	wireless WPA	ethernet
2	Control := if Tank('T1').level >= 6.3 then set HeadPump('PU1').status to Cl...	T1 level	digital	Pump PU1	mechanical	PLC1	wireless WPA	ethernet
3	Control := if Tank('T1').level <= 1.0 then set HeadPump('PU2').status to O...	T1 level	digital	Pump PU2	mechanical	PLC1	ethernet	ethernet
4	Control := if Tank('T1').level >= 4.5 then set HeadPump('PU2').status to Cl...	T1 level	digital	Pump PU2	mechanical	PLC1	ethernet	ethernet
5	Control := if Tank('T2').level <= 0.5 then set FCValve('V2').status to Open ...	T2 level	digital	Valve V2	mechanical	PLC2	ethernet	ethernet
6	Control := if Tank('T2').level >= 5.5 then set FCValve('V2').status to Closed ...	T2 level	digital	Valve V2	mechanical	PLC2	wireless WPA	wireless WPA
7	Control := if Tank('T3').level <= 3.0 then set HeadPump('PU4').status to O...	T3 level	digital	Pump PU4	mechanical	PLC3	wireless WPA	wireless WPA

WN Duration (s) 604800
WN Hydraulic step (s) 900
WN Pattern step (s) 3600
WN Report step (s) 900

Cyber Sim step (s) 3600
Cyber Sim Duration (h) 24

	Start (h)	End (h)	Event Type	Target	Special	Values
1	10	15	sensor manipulation	ST1	offline	None
2	14	16	Undefined			

Undefined
sensor malfunction
sensor manipulation
chemical attack
actuator malfunction
actuator manipulation

Fig. 23. RISKNOUGHT GUI, currently under development.

(e.g., non-Gaussian) and any valid correlation structure stationary or nonstationary [see also the R-package anySim (Tsoukalas and Kossieris 2019)]. Such models can also be used for the generation/disaggregation of coarse scale time series into finer temporal scales (Tsoukalas 2019; Tsoukalas et al. 2019). Such modeling/simulation schemes can easily be employed for the simulation of nonphysical processes, such as those employed herein; see for example recent work by Kossieris and Makropoulos (2018) and Kossieris et al. (2019), for the simulation of fine time-scale water demand processes. Such modeling schemes, and particularly disaggregation ones, can be valuable in water distribution network studies where available time series are typically of coarse resolution (e.g., hourly data).

By building upon the flexibility provided by RISKNOUGHT, and coupling it with the notion of stochastic time series generation, it is possible to enable the development of an uncertainty-aware cyber-physical framework. Such a framework will be able to propagate the uncertainty of inputs to the model's outputs, and thus provide robust, probabilistically-based results and metrics for water distribution cyber-physical systems.

Conclusions

The work presented here introduces a new cyber-physical stress-testing platform, RISKNOUGHT. The platform allows users to simulate water distribution systems as cyber-physical systems, implementing complex control logic via a simulation-based approach. This approach enables the modeling of a multitude of cyber-physical attacks and assessment of their impact in what-if exploration scenarios, while retaining enough fidelity in the representation of interacting processes and information flow in the cyber layer. We argue that the study of a water system's behavior under attack in RISKNOUGHT can inform the definition of cyber-physical risk management strategies for cyber-wise water utilities. RISKNOUGHT uses the industry standard EPANET format and solver and as such leverages extensive modelling know-how and experience, already present even in smaller utilities that may lack resources and technical personnel to adopt solutions such as SCADA testbeds, emulators, or heavy virtualization approaches. It is envisaged that this platform could help water utilities navigate the ever-changing risk landscape and help address some of the challenges emerging due to the ongoing transformation of water infrastructure into cyber-physical systems.

Appendix. Control Logic Implemented in the C-Town Simulation

Appendix. (*Continued.*)

ID	Logic part	Sensor	Actuator	PLC
Control1	if Tank('T1').level < = 4.0 then set HeadPump('PU1').status to Open with priority 3	ST1	APU1	PLC1
Control2	if Tank('T1'). level > = 6.3 then set HeadPump('PU1'). status to Closed with priority 3	ST1	APU1	PLC1
Control3	if Tank('T1').level < = 1.0 then set HeadPump('PU2').status to Open with priority 3	ST1	APU2	PLC1
Control4	if Tank('T1').level > = 4.5 then set HeadPump('PU2').status to Closed with priority 3	ST1	APU2	PLC1
Control5	if Tank('T2').level < = 0.5 then set FCValve('V2').status to Open with priority 3	ST3	AV2	PLC2
Control6	if Tank('T2').level > = 5.5 then set FCValve('V2').status to Closed with priority 3	ST3	AV2	PLC2
Control7	if Tank('T3').level < = 3.0 then set HeadPump('PU4').status to Open with priority 3	ST3	APU4	PLC3
Control8	if Tank('T3').level > = 5.3 then set HeadPump('PU4').status to Closed with priority 3	ST3	APU4	PLC3
Control9	if Tank('T3').level < = 1.0 then set HeadPump('PU5').status to Open with priority 3	ST3	APU5	PLC3
Control10	if Tank('T3').level > = 3.5 then set HeadPump('PU5').status to Closed with priority 3	ST3	APU5	PLC3
Control11	if Tank('T4').level < = 2.0 then set HeadPump('PU6').status to Open with priority 3	ST4	APU6	PLC4
Control12	if Tank('T4').level > = 3.5 then set HeadPump('PU6').status to Closed with priority 3	ST4	APU6	PLC4
Control13	if Tank('T4').level < = 3.0 then set HeadPump('PU7').status to Open with priority 3	ST4	APU7	PLC4
Control14	if Tank('T4').level > = 4.5 then set HeadPump('PU7').status to Closed with priority 3	ST4	APU7	PLC4
Control15	if Tank('T5').level < = 1.5 then set HeadPump('PU8').status to Open with priority 3	ST5	APU8	PLC5
Control16	if Tank('T5').level > = 4.0 then set HeadPump('PU8').status to Closed with priority 3	ST5	APU8	PLC5
Control17	if Tank('T7').level < = 2.5 then set HeadPump('PU10').status to Open with priority 3	ST7	APU10	PLC6
Control18	if Tank('T7').level > = 4.8 then set HeadPump('PU10').status to Closed with priority 3	ST7	APU10	PLC6
Control19	if Tank('T7').level < = 1.0 then set HeadPump('PU11').status to Open with priority 3	ST7	APU11	PLC6
Control20	if Tank('T7').level > = 3.0 then set HeadPump('PU11').status to Closed with priority 3	ST7	APU11	PLC6

Data Availability Statement

Some or all data, models, or code generated or used during the study are available from the corresponding author by request. These include the network model, the cyber layer topology, the cyber-physical events tested, and the results of the simulations.

Acknowledgments

This work was partially supported by STOP-IT research project, which received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610. The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

Supplemental Data

Animations of attack scenarios 1 and 2 are available online in the ASCE Library (www.ascelibrary.org).

References

Abrams, M., and J. Weiss. 2008. *Malicious control system cyber security attack case study—Maroochy water services, Australia*. McLean, VA: MITRE Corporation.

Ahrenholz, J., C. Danilov, T. R. Henderson, and J. H. Kim. 2008. "CORE: A real-time network emulator." In *Proc., IEEE Military Communications Conf. MILCOM*. Piscataway, NJ: IEEE.

Almalawi, A., Z. Tari, I. Khalil, and A. Fahad. 2013. "SCADAVT-A framework for SCADA security testbed based on virtualization technology." In *Proc., Conf. on Local Computer Networks, LCN*, 639–646. Piscataway, NJ: IEEE.

Antonioli, D., and N. O. Tippenhauer. 2015. "MiniCPS." In *Proc., 1st ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy—CPS-SPC '15*, 91–100. New York: ACM Press.

Arandia, E., and B. J. Eck. 2018. "An R package for EPANET simulations." *Environ. Modell. Software* 107 (Oct): 59–63. https://doi.org/10.1016/j.envsoft.2018.05.016.

Ayala, L. 2016. *Cybersecurity lexicon*. Berkeley, CA: Apress.

Bentley Systems Incorporated. 2006. *Water-GEMS*. Exton, PA: Bentley Systems Incorporated.

Chandy, S. E., A. Rasekh, Z. A. Barker, and M. E. Shafiee. 2018. "Cyberattack detection using deep generative models with variational inference." *J. Water Resour. Plann. Manage.* 145 (2): 04018093. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001007.

Chen, H. 2017. "Applications of cyber-physical system: A literature review." *J. Ind. Integr. Manage.* 2 (3): 1750012. https://doi.org/10.1142/S2424862217500129.

Ciaponi, C., and E. Creaco. 2018. "Comparison of pressure-driven formulations for WDN simulation." *Water* 10 (4): 523. https://doi.org/10.3390/w10040523.

Cook, C., and K. Bakker. 2012. "Water security: Debating an emerging paradigm." *Global Environ. Change* 22 (1): 94–102. https://doi.org/10.1016/j.gloenvcha.2011.10.011.

Davis, M. J., R. Janke, and T. N. Taxon. 2018. "Mass imbalances in EPANET water-quality simulations." *Drinking Water Eng. Sci.* 11 (1): 25–47. https://doi.org/10.5194/dwes-11-25-2018.

Eliades, D. G., M. Kyriakou, S. G. Vrachimis, and M. M. Polycarpou. 2016. "EPANET-MATLAB toolkit: An open-source software for interfacing EPANET with MATLAB." In *Proc., Computing and Control for the Water Industry CCWI 2016*, 1–8. Amsterdam, Netherlands: Elsevier.

Falliere, N., L. O. Murchu, and E. Chien. 2011. "W32.Stuxnet Dossier." In *Symantec-security response, version 1*, 1–69. Mountain View, CA: Symantec.

Fovino, I. N., M. Masera, L. Guidi, and G. Carpi. 2010. "An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants." In *Proc., 3rd Int. Conf. on Human System Interaction, HSI'2010*, 679–686. New York: IEEE.

GDAL/OGR Contributors. 2019. "{GDAL/OGR} Geospatial data abstraction software library." Accessed December 10, 2019. https://gdal.org/.

Germano, J. H. 2018. *Cybersecurity risk & responsibility in the water sector*. Denver: American Water Works Association.

Gillies, S., A. Bierbaum, K. Lautaportti, and O. Tonnhofer. 2007. *Shapely: Manipulation and analysis of geometric objects*. San Francisco: GitHub.

Hagberg, A. A., D. A. Schult, and P. J. Swart. 2008. "Exploring network structure, dynamics, and function using NetworkX." In *Proc., 7th Python in Science Conf. (SciPy 2008), (SciPy)*, 11–15.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). 2016. *ICS-CERT year in review*. Arlington, VA: Cybersecurity and Infrastructure Security Agency.

Jordahl, K., J. Van den Bossche, J. Wasserman, J. McBride, J. Gerard, J. Tratner, M. Perry, and C. Farmer. 2019. *Geopandas/geopandas: v0.5.0*. Geneva: Zenodo.

Klise, K. A., M. Bynum, D. Moriarty, and R. Murray. 2017a. "A software framework for assessing the resilience of drinking water systems to disasters with an example earthquake case study." *Environ. Modell. Software* 95 (Sep): 420–431. https://doi.org/10.1016/j.envsoft.2017.06.022.

Klise, K. A., D. Hart, D. M. Moriarty, M. L. Bynum, R. Murray, J. Burkhardt, and T. Haxton. 2017b. *Water network tool for resilience (WNTR) user manual*. Oak Ridge, TN: Office of Scientific and Technical Information.

Klise, K. A., R. Murray, and T. Haxton. 2018. "An overview of the water network tool for resilience (WNTR)." In *Proc., 1st Int. WDSA/CCWI Joint Conf.*, 8. Albuquerque, NM: Sandia National Lab.

Kossieris, P., and C. Makropoulos. 2018. "Exploring the statistical and distributional properties of residential water demand at fine time scales." *Water* 10 (10): 1481. https://doi.org/10.3390/w10101481.

Kossieris, P., I. Tsoukalas, C. Makropoulos, and D. Savic. 2019. "Simulating marginal and dependence behaviour of water demand processes at any fine time scale." *Water* 11 (5): 885. https://doi.org/10.3390/w11050885.

Langner, R. 2011. "Stuxnet: Dissecting a cyberwarfare weapon." *IEEE Secur. Privacy* 9 (3): 49–51. https://doi.org/10.1109/MSP.2011.67.

Lantz, B., B. Heller, and N. McKeown. 2010. "A network in a laptop." In *Proc., 9th ACM SIGCOMM Workshop on Hot Topics in Networks—Hotnets '10*, 1–6. New York: ACM Press.

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

Lee, E. A. 2015. "The past, present and future of cyber-physical systems: A focus on models." *Sensors* 15 (3): 4837–4869. https://doi.org/10.3390/s150304837.

Leyden, J. 2016. "Water treatment plant hacked, chemical mix changed for tap supplies." Accessed August 5, 2019. https://www.theregister.co.uk/2016/03/24/water_utility_hacked/.

Lu, Y. 2017. "Industry 4.0: A survey on technologies, applications and open research issues." *J. Ind. Inf. Integr.* 6 (Jun): 1–10. https://doi.org/10.1016/j.jii.2017.04.005.

Mahmoud, H. A., D. Savić, and Z. Kapelan. 2017. "New pressure-driven approach for modeling water distribution networks." *J. Water Resour. Plann. Manage.* 143 (8): 04017031. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000781.

Makropoulos, C., et al. 2018. "A resilience assessment method for urban water systems." *Urban Water J.* 15 (4): 316–328. https://doi.org/10.1080/1573062X.2018.1457166.

McAfee, A., E. Brynjolfsson, T. H. Davenport, D. J. Patil, and D. Barton. 2012. "Big data: The management revolution." *Harvard Bus. Rev.* 90 (10): 60–68.

Mittelstadt, S., X. Wang, T. Eaglin, D. Thom, D. Keim, W. Tolone, and W. Ribarsky. 2015. "An integrated in-situ approach to impacts from natural disasters on critical infrastructures." In *Proc., 2015 48th Hawaii Int. Conf. on System Sciences*, 1118–1127. New York: IEEE.

Morley, M. S., and C. Tricarico. 2008. *Pressure-driven demand extension for EPANET (EPANETpdd)*. Technical Rep. No. 2008/02. Exeter, UK: Centre for Water Systems, Univ. of Exeter.

Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. 2012. "SCADA security in the light of cyber-warfare." *Comput. Secur.* 31 (4): 418–436. https://doi.org/10.1016/j.cose.2012.02.009.

Nikolopoulos, D., C. Makropoulos, D. Kalogeras, K. Monokrousou, and I. Tsoukalas. 2018. "Developing a stress-testing platform for cyber-physical water infrastructure." In *Proc., 2018 Int. Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater)*, 9–11. New York: IEEE.

Nikolopoulos, D., G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, and C. Makropoulos. 2019a. "RISKNOUGHT: A cyber-physical stress-testing platform for water distribution networks." In *Proc., 11th World Congress on Water Resources and Environment (EWRA 2019) Managing Water Resources for a Sustainable Future*. New York: Springer.

Nikolopoulos, D., H.-J. van Alphen, D. Vries, L. Palmen, S. Koop, P. van Thienen, G. Medema, and C. Makropoulos. 2019b. "Tackling the 'new normal': A resilience assessment method applied to real-world urban water systems." *Water* 11 (2): 330. https://doi.org/10.3390/w11020330.

NS-3 Consortium. 2019. "NS-3 network simulator." Accessed August 5, 2019. https://www.nsnam.org/.

Oman, P., and M. Phillips. 2007. "Intrusion detection and event monitoring in SCADA networks." In Vol. 253 of *Proc., IFIP Int. Federation for Information Processing*, 161–173. New York: Springer.

Ostfeld, A., et al. 2012. "Battle of the water calibration networks." *J. Water Resour. Plann. Manage.* 138 (5): 523–532. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000191.

Pesantez, J. E., E. Z. Berglund, and G. Mahinthakumar. 2019. "Multiphase procedure to design district metered areas for water distribution networks." *J. Water Resour. Plann. Manage.* 145 (8): 04019031. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001095.

Piedrahita, A. F. M., V. Gaur, J. Giraldo, A. A. Cardenas, and S. J. Rueda. 2017. "Leveraging software-defined networking for incident response in industrial control systems." *IEEE Software* 35 (1): 44–50. https://doi.org/10.1109/MS.2017.4541054.

Queiroz, C., A. Mahmood, J. Hu, Z. Tari, and X. Yu. 2009. "Building a SCADA security testbed." In *Proc., NSS 2009—Network and System Security*, 357–364. New York: IEEE.

Rajkumar, R., I. Lee, L. Sha, and J. Stankovic. 2017. "Cyber-physical systems: The next computing revolution." *Cybern. Syst. Anal.* 53 (6): 821–834. https://doi.org/10.1145/1837274.1837461.

Rasekh, A., A. Hassanzadeh, S. Mulchandani, S. Modi, and M. K. Banks. 2016. "Smart water networks and cyber security." *J. Water Resour. Plann. Manage.* 142 (7): 01816004. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646.

Rossman, L. A. 2000. *Epanet 2 users manual*, 1–200. Washington, DC: USEPA.

Salomons, E. 2014. "EPANET class for C#." Accessed September 5, 2019. http://www.water-simulation.com/wsp/2014/02/25/epanet-class-for-c-sharp/.

Sankary, N., and A. Ostfeld. 2019. "Bayesian localization of water distribution system contamination intrusion events using inline mobile sensor data." *J. Water Resour. Plann. Manage.* 145 (8): 04019029. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001086.

Sayfayn, N., and S. Madnick. 2017. *Cybersafety analysis of the maroochy shire sewage spill cybersafety analysis of the maroochy shire sewage spill (preliminary draft)*, 1–29. Cambridge, MA: Massachusetts Institute of Technology.

Shang, F., J. G. Uber, and L. Rossman. 2008. *EPANET multi-species extension user's manual*. Cincinnati: USEPA.

Shannon, P., A. Markiel, O. Ozier, N. S. Baliga, J. T. Wang, D. Ramage, N. Amin, B. Schwikowski, and T. Ideker. 2003. "Cytoscape: A software environment for integrated models of biomolecular interaction networks." *Genome Res.* 13: 2498–2504. https://doi.org/10.1101/gr.1239303.

Siaterlis, C., B. Genge, and M. Hohenadel. 2013. "EPIC: A testbed for scientifically rigorous cyber-physical security experimentation." *IEEE Trans. Emerging Top. Comput.* 1 (2): 319–330. https://doi.org/10.1109/TETC.2013.2287188.

Taormina, R., and S. Galelli. 2018. "Deep-learning approach to the detection and localization of cyber-physical attacks on water distribution systems." *J. Water Resour. Plann. Manage.* 144 (10): 04018065. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000983.

Taormina, R., S. Galelli, H. C. Douglas, N. O. Tippenhauer, E. Salomons, and A. Ostfeld. 2019. "A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems." *Environ. Modell. Software* 112 (May): 46–51. https://doi.org/10.1016/j.envsoft.2018.11.008.

Taormina, R., S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld. 2017. "Characterizing cyber-physical attacks on water distribution systems." *J. Water Resour. Plann. Manage.* 143 (5): 04017009. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000749.

Thompson, M. 2016. "Iranian cyber attack on new york dam shows future of war." Accessed August 5, 2019. https://time.com/4270728/iran-cyber-attack-dam-fbi.

Tsoukalas, I. 2019. "Modelling and simulation of non-Gaussian stochastic processes for optimization of water-systems under uncertainty." Ph.D. thesis, Dept. of Water Resources and Environmental Engineering, National Technical Univ. of Athens.

Tsoukalas, I., A. Efstratiadis, and C. Makropoulos. 2017. "Stochastic simulation of periodic processes with arbitrary marginal distributions." In *Proc., 15th Int. Conf. on Environmental Science and Technology, CEST 2017*. Lesbos, Greece: Global Network for Environmental Science and Technology.

Tsoukalas, I., A. Efstratiadis, and C. Makropoulos. 2018a. "Stochastic periodic autoregressive to anything (SPARTA): Modeling and simulation of cyclostationary processes with arbitrary marginal distributions." *Water Resour. Res.* 54 (1): 161–185. https://doi.org/10.1002/2017WR021394.

Tsoukalas, I., A. Efstratiadis, and C. Makropoulos. 2019. "Building a puzzle to solve a riddle: A multi-scale disaggregation approach for multivariate stochastic processes with any marginal distribution and correlation structure." *J. Hydrol.* 575 (Aug): 354–380. https://doi.org/10.1016/j.jhydrol.2019.05.017.

Tsoukalas, I., and P. Kossieris. 2019. "AnySim: Stochastic simulation of processes with any marginal distribution and correlation structure." Accessed December 10, 2019. http://www.itia.ntua.gr/en/softinfo/33/.

Tsoukalas, I., C. Makropoulos, and D. Koutsoyiannis. 2018b. "Simulation of stochastic processes exhibiting any-range dependence and arbitrary marginal distributions." *Water Resour. Res.* 54 (11): 9484–9513. https://doi.org/10.1029/2017WR022462.

Tsoukalas, I., S. Papalexiou, A. Efstratiadis, and C. Makropoulos. 2018c. "A cautionary note on the reproduction of dependencies through linear stochastic models with non-gaussian white noise." *Water* 10 (6): 771. https://doi.org/10.3390/w10060771.

USEPA, epanet-solver. 2019. "GitHub repository." Accessed January 22, 2020. https://github.com/USEPA/Water-Distribution-Network-Model.

Varga, A., and R. Hornig. 2008. "An overview of the OMNeT++ simulation environment." In *Proc., 1st Int. ICST Conf. on Simulation Tools and Techniques for Communications Networks and Systems*. Gent, Belgium: Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.

Wagner, J., U. Shamir, and D. Marks. 1988. "Water distribution reliability: Simulation methods." *J. Water Resour. Plann. Manage.* 114 (3): 276–294. https://doi.org/10.1061/(ASCE)0733-9496(1988)114:3(276).

Wallingford Software. 2012. *Infoworks*. Oxfordshire, UK: HR Wallingford.

White, B., J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar. 2004. "An integrated experimental environment for distributed systems and networks." Supplement, *ACM SIGOPS Operating Syst. Rev.* 36 (S1): 255. https://doi.org/10.1145/844128.844152.

Wolf, W. 2009. "Cyber-physical systems." *Computer* 42 (3): 88–89. https://doi.org/10.1109/MC.2009.81.

Zhu, B., A. Joseph, and S. Sastry. 2011. "A taxonomy of cyber attacks on SCADA systems." In *Proc., 2011 IEEE Int. Conf. on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom*. Piscataway, NJ: IEEE.