URBAN WATER JOURNAL
https://doi.org/10.1080/1573062X.2021.1995446

Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

Stress-testing water distribution networks for cyber-physical attacks on water quality

Dionysios Nikolopoulos[a] and Christos Makropoulos[a,b]

[a]Department of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical University of Athens, Athens, Greece; [b]KWR Watercycle Research Institute, Nieuwegein, The Netherlands

ABSTRACT

The interplay between cyber and physical elements of water systems and the corresponding security challenges are fast becoming a key topic for the water sector. Of special concern is the absence of simulation tools for deliberate contamination attacks on water distribution networks (WDNs), in conjunction with cyber attacks on the contamination warning system. RISKNOUGHT is a cyber-physical stress-testing platform that simulates WDNs as integrated cyber-physical systems and models complex cyber-physical attacks. Supported tasks include modelling of contamination incidents and complex control logic schemes acting as mitigation measures against contamination (e.g. DMA isolation and flushing). RISKNOUGHT simulates composite scenarios of cyber-physical attacks on various elements of the SCADA and the physical network and assesses impact on the network and consumers through several metrics. Testing the platform on a benchmark network demonstrates its capabilities and provides insights for water utilities regarding cyber-physical attacks that include contamination events.

ARTICLE HISTORY
Received 26 October 2020
Accepted 13 October 2021

KEYWORDS
Water distribution networks; cyber-physical systems; cyber-physical drinking water quality attacks; water cyber security; stress-testing platform

Introduction

Water distribution networks (WDNs) are core systems for the welfare of any society because their role in providing safe to drink water in a distributed manner is irreplaceable. Thus, WDNs are considered part of the critical infrastructure (CI) of any community. Due to their dispersed nature, accessibility and large population coverage (Schwartz, Lahav, and Ostfeld 2014; Rasekh and Brumbelow 2015) are attractive for a multitude of deliberate malicious actions by perpetrators (Gleick 2006), including chemical and biological contamination. The serious implications of such threats include health and sociopolitical impacts (Rasekh and Brumbelow 2014), and can be deduced from similar experiences occurring from accidental (unintentional) contamination events (Eliades et al. 2014). For example, a failure in Milwaukee Water Works southern treatment plant led to a cryptosporidium outbreak in the Milwaukee (USA) WDN in 1993 (Mac Kenzie et al. 1994) that affected 403,000 people, resulted in approximately 50 to 70 deaths (Hoxie et al. 1997) and an estimated economic damage of $96.2 million (Corso et al. 2003). Another example is the 2014 West Virginia (USA) chemical spill. Approximately 40,000 liters of the toxic compound methylcyclohexanemethanol (MCHM) and ether were leaked from an industrial complex to Elk river, entered the water treatment plant and contaminated the main water source of West Virginia American Water in Charleston, leaving 300,000 people without potable water (Cooper 2014).

In the past, a main 'security' notion has been that 'dilution is the solution' (i.e. any contamination will not be significant enough in volume terms) (Ginsberg and Hock 2004) due to the large volumes of water involved. However, there is a variety of chemical and biological (CB) agents (some being also weaponized) that can be dangerous even in small concentrations in the water (Salem 2003) or become even more toxic when oxidized by residual chlorine in the WDN (Schwartz, Lahav, and Ostfeld 2014; Ginsberg and Hock 2004). More over, large parts of WDNs are physically unprotected and have multiple access points. Regarding this, it was generally thought that an attack with CB agents would require expensive equipment and several technicians. However, it has been proven that injection of CB agents in a WDN is in fact possible by exploiting what is termed a 'backflow attack' (Rasekh and Brumbelow 2015; Ginsberg and Hock 2004; Allmann and Carlson 2005; Laird et al. 2005). For such an attack, any water outlet (e.g. faucets, fire hydrants etc.) can be used as an intrusion point (Laird et al. 2005) with the help of a low-cost pump that can overcome the pressure of the service line (Schwartz, Lahav, and Ostfeld 2014), provided that there is no backflow protection (Allmann and Carlson 2005), e.g. in the form of a backflow valve.

Water security in either deliberate or accidental contamination events is an active topic in the literature, with research focusing on many different aspects, such as modelling the fate of different CB agents transported though the WDN (e.g. Schwartz, Lahav, and Ostfeld 2014; Burkhardt et al. 2017; Shang, Uber, and Rossman 2008; Albert et al. 2017), source identification of the detected contaminant (e.g. Zechman and Ranji Ranjithan 2009; Laird et al. 2005; Seth et al. 2016), quality sensor placement (e.g. Giudicianni et al. 2020; Chang, Pongsanone, and Ernest 2013), modelling response and mitigation strategies (e.g. Shafiee and Berglund 2017; Alfonso, Jonoski, and Solomatine 2010) and improving the hydraulic and quality models to accommodate more sophisticated analyses (e.g. Seyoum and Tanyimboh 2017; Xing and Sela 2020).

CONTACT Dionysios Nikolopoulos nikolopoulos.dio@gmail.com

However, there is a major gap in the water security literature and in risk management frameworks (Nikolopoulos et al. 2018); modern WDN are cyber-physical systems (Nikolopoulos et al. 2020), as they are an integration of physical processes with computational engineered systems (Lee 2008). The typical WDN is controlled and monitored by a Supervisory Control and Data Acquisition system (SCADA), which uses sensors, actuators, and other field devices to operate. In the context of cyber-physical quality monitoring, there are online quality sensors or probes that automatically sample water characteristics and relay the information to programmable logic controllers (PLCs), remote terminal units (RTUs) or to the SCADA to perform some action via actuators, issue a warning etc. Therefore, cyber-physical WDNs besides deliberate contamination (a form of *physical* attack) are exposed to a bigger attack surface (Rasekh et al. 2016) with additional threats taking the form of cyber-attack that hinders the monitoring and/or remote control operations of the WDN. A particularly concerning combinatory cyber-physical attack is an event where perpetrators contaminate the WDN and at the same time perform a cyber-attack on the SCADA to make the attack go unnoticed, e.g. the perpetrator hijacks the connection, eavesdrops the data transmitted by the sensor and replays normal readings. Denial of service (DoS) attacks can also have a significant impact in conjunction with the contamination attack, as for example DoS attack to cut-off communication with actuator devices etc., with the intent to make it impossible to remotely activate emergency response measures. Another interesting scenario would be to fake a severe contamination event (i.e. without actually performing the physical part of the attack) by manipulating sensor readings in order to cause chaos, as the utility would have to take drastic mitigation and response measures in vain. There are also other possible attack vectors that do not concern sensor or SCADA tampering, like physical destruction of flushing units for decontamination, cyber-attacks on the connected actuator units etc.

It is argued that the operational integration of cyber and physical systems will be important in the risk management approach of water systems in the future (Makropoulos and Savić 2019). The growing number of cyber-physical incidents (for example, the Riviera Beach ransomware attack in 2019, the hacking of Maroochi Shire Waste Water Treatment Plant in 2000, the remote access to a sluice gate on the Bowman Dam in 2013, the reported cyber attacks on the Israeli water industry in 2020 etc., seen in the reviews of Hassanzadeh et al. (2020) and Tuptuk et al. (2021) supports this notion and there is a growing interest in EU for the protection of such systems, especially with water quality in mind (e.g. Ed and Ed 2019; Coelho et al. 2020). Also, recent reports in the US (ICS-CERT 2016), show that the water sector ranks among the most prominent critical infrastructure sectors for cyber-attacks, with hundreds attempts yearly (many of which undisclosed to the general public and others still undetected). Nevertheless, there are currently only a few cyber-physical tools that can aid in analysis of cyber-physical risk assessment and impact evaluation of cyber-physical attacks on a WDN. Such cyber-physical tools include epanetCPA (Taormina et al. 2019, 2017) and DHALSIM (Murillo et al. 2020). However, both currently do not support the ability to simulate quality related attacks. RISKNOUGHT (Nikolopoulos et al. 2020, 2019a) is a cyber-physical stress-testing platform that supports quality related cyber-physical attacks and response measures for mitigation. In this work, we present in depth the cyber-physical quality modelling capabilities of RISKNOUGHT.

RISKNOUGHT modelling platform

RISKNOUGHT (Nikolopoulos et al. 2020, 2019a) is a simulation platform coupling two interacting models, one for the cyber layer, governing the control logic, and one for the physical layer, responsible for hydraulics. The modelling of interactions and feedback loops between the two models allows users to simulate water distribution systems as cyber-physical systems, implementing complex control logic via a purely simulation-based approach. The processes and information flow between components are mathematically modelled, i.e. the cyber layer is represented as a graph, where the central SCADA system is represented as a node, an online sensor is represented as another node type, the connection between the sensor and a PLC is represented as an edge, and the measurement of the sensor is a signal traversing the graph, interacting with a software function with the physical model, such as affecting the decision on a pump control. This approach is in contrast with emulation-based approaches (e.g. Almalawi et al. 2013; Antonioli and Tippenhauer 2015) that employ emulators, virtual machines, or software defined networks. These modelling methods construct a detailed emulation model of each component, representing its original operation accurately in a software environment. While more detailed, many emulation approaches are proprietary, tethered to a specific system topology (Fovino et al. 2010; Siaterlis, Garcia, and Genge 2013; Queiroz et al. 2009; Queiroz, Mahmood, and Tari 2011; Siaterlis, Genge, and Hohenadel 2013). Emulation is not easily implemented in system-wide cyber-physical risk assessment studies; While it is very useful as a means of penetration testing to discover new vulnerabilities to cyber-attacks for components, in order to describe a cyber-physical attack, a definite series of detailed steps regarding software/hardware exploitation must be modelled. On the other hand, simulation approaches enable the representation of cyber-physical attacks as events and assess their impact in system-wide what-if exploration scenarios that explain the interaction of processes and information flow in the cyber layer and the resulting cascading effects in the physical layers with a level of abstraction and the focus being on the outcome of the event (Nikolopoulos et al. 2020).

A variety of cyber-physical attacks can be modelled by RISKNOUGHT and incorporated in stress-testing scenarios, including: DoS attacks (e.g. DoS on a PLC, DoS on the connection to an actuator etc.), tampering with sensor data/transmitted information (Man-in-the-middle (MITM) attacks, such as fabrication of data, replay attacks etc.), physical sabotage/destruction of cyber as well as physical components etc.

The current version of RISKNOUGHT fully supports the simulation of deliberate contamination events, along with the ability to monitor water quality through sensors in the WDN and

issuing control logic commands for response and mitigation measures for emergencies as a contamination warning system (CWS).

RISKNOUGHT physical and cyber layers and interactions

RISKNOUGHT leverages the recently released EPANET 2.2 (Rossman et al. 2020) through the usage of the WNTR Python package (Klise et al. 2017) for representing in detail any WDN. The new version of EPANET facilitates natively pressure driven analysis (PDA) equations. These produce realistic pressure deficient conditions which may result in service unavailability in a WDN, in contrast with the normal setting of demand driven analysis (DDA) equations of previous EPANET versions (Ciaponi and Creaco 2018). This is of paramount importance in disaster modelling and when assessing the effect of prolonged or severe cyber-physical attacks. The water quality solver of EPANET 2.2. is also compatible with the PDA solver, allowing the handling of a single-species water contaminant fate and transportation analysis along with the hydraulics of the network. This used to not be a seamless process in the past), requiring extensions such as EPANET-PDX (Seyoum and Tanyimboh 2014, 2016) and EPANET-PMX (Seyoum and Tanyimboh 2017).

For the cyber layer, a user-customizable object-oriented network digraph model is employed, that leverages the NetworkX (Hagberg, Schult, and Swart 2008) Python package, with nodes acting as sensors, actuators, programmable logic controllers (PLCs), the central SCADA mainframe, human–machine interface (HMI),and the historian (the SCADA database infrastructure), and edges acting as the wired/wireless connections between them . At each simulation step, the physical layer object (the WDN) feeds input data (e.g. node pressure, tank level, pipe velocities etc.) from the hydraulic simulation to the cyber layer, which, depending on the deployed control logic schemes, passes decisions to the physical layer, affecting the hydraulic state for the subsequent simulation step. RISKNOUGHT returns results to the user about all system properties in the form of pandas dataframes(McKinney 2010).

Water quality cyber-physical simulation

Specifically for the cyber-physical water quality simulation, RISKNOUGHT uses a sophisticated procedure, that couples the water quality simulation, the PDA hydraulic simulation, and the remote monitoring and control model. It is imperative to run both the physical layer and the cyber layer in a stepwise manner and concurrently, i.e. run a PDA hydraulics simulation with the discretization step of the control and monitoring scheme, run the quality simulation with regard to these hydraulic conditions, then update the monitoring scheme (sensors) of the SCADA and apply controls/changes to the network (via actuators). The previous version of RISKNOUGHT (Nikolopoulos et al. 2020) used as the hydraulic solver the WNTRsimulator (Klise et al. 2017), a Python EPANET compatible solver (but without water quality capabilities), that allowed the pause of a simulation, the change of parameters and the continuation of the altered scheme. This enabled the cyber layer to seamlessly alter processes in the physical layer, simulating monitor and control operations. The EPANET 2.2. simulation engine wrapper in WNTR though does not support the stepwise pause and continuation of simulations. To solve this issue in cyber-physical stepwise water quality simulation along with a concurrent control scheme, the following process is used:

For the first simulation step, the initial conditions of the water network (water quality at nodes, tank levels etc.) are monitored from the cyber layer, which generates a set of commands. The duration of the hydraulic simulation is set to a single timestep. Any change of state to a pump, valve etc. is transformed to an EPANET *'time control'* object of the form '*LINK x status AT TIME t'* and added to the control list. The WDN's operation is simulated, and all hydraulic results are added to respective dataframes.

For the second and each subsequent step, the cyber layer's information is updated with the results of the last physical simulation step, culminating the monitoring process. New commands are generated based on this information, which is translated into EPANET time controls and added to the WDN object. The hydraulic simulation duration is set to the previous one plus a single timestep, and the simulation is re-run. The results of the last timestep are added to the respective dataframes, concluding the cycle of a single cyber-physical simulation step.

With the aforementioned procedure, RISKNOUGHT accomplishes the task of solving both the hydraulics of the network with PDA equations and the water quality aspect concurrently, allowing also the implementation of controls based on attributes like water quality (e.g. *if concentration at node X is above a certain threshold, close Y valve*) that EPANET currently does not allow, as all commands are passed to the WDN as time controls affecting pipes, pumps and valves. This interplay brings the benefit of allowing monitoring of water quality changes in the network and deciding on control actions. The coupling with the PDA in EPANET 2.2. proves to be useful in cases of control actions that can drastically alter pressure in the distribution network (e.g. close valves) and thus hinder the ability to supply water. However, the process of re-running the physical model with an increasing number of timesteps may prove slow for very large networks and long period simulation with small hydraulic timesteps, despite the fast EPANET 2.2 solver. The process of cyber-physical quality simulation is schematically presented in Figure 1.

Quality monitoring and response model using RISKNOUGHT

Various components (sensors, PLCs, actuators, etc.) are included in the cyber layer representation for the cyber-physical WDN simulation. RISKNOUGHT uses the following components (Nikolopoulos et al. 2020):

- Sensor: acquires data from the physical layer, e.g. tank levels, node pressure, water quality (concentration) etc., from a node or link of the WDN. Sensors have a user-specified sampling ratio, which defaults to once in every cyber-physical simulation step and can have as attributes systematic biases and random error probabilities.

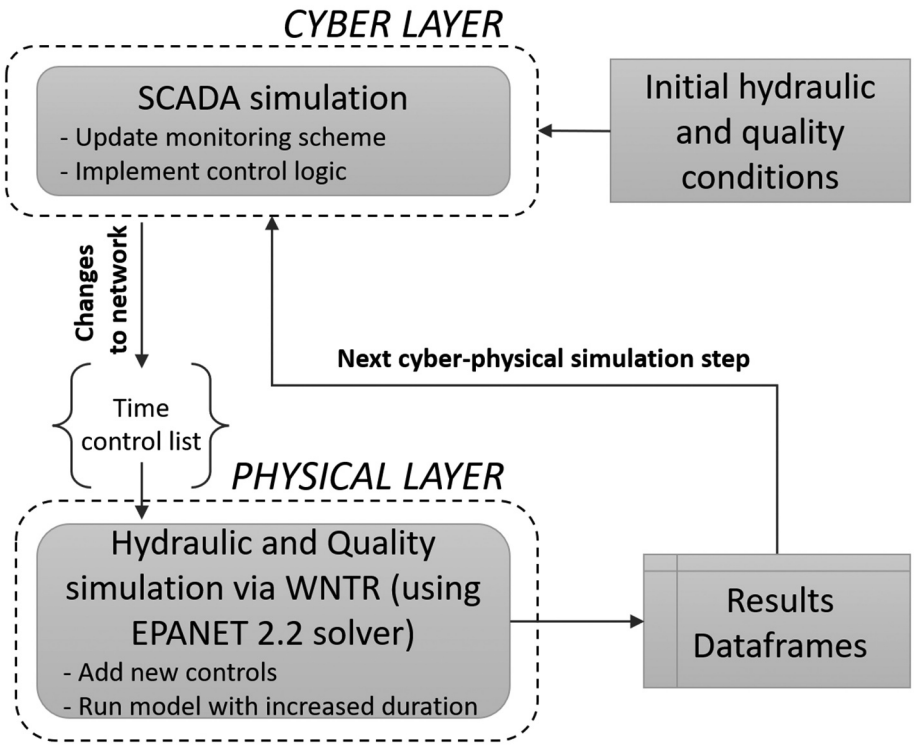

Figure 1. RISKNOUGHT cyber-physical quality simulation.

- Actuator: performs an action on the physical layer, e.g. in the form of opening or closing a valve or pump, or activating a flushing unit.
- Logic: virtual components that implement control logic for responding to a detected contamination event and mitigating its impact via using input data from sensors to decide physical actions as outputs through actuators.
- PLC: holds Logic components, linked to the Central SCADA unit with slave/master or semi-autonomous relations, transmitting data and receiving master commands. PLC to PLC direct communication (without linking to central SCADA node) is not supported yet.
- Central SCADA: interconnects all field devices (PLCs) gathering all input/output (I/O) data.
- Historian: records all I/O data in a database.

A schematic overview of the cyber layer is represented in Figure 2, where components for hydraulic operation and quality monitoring are shown.

RISKNOUGHT is enhanced with new control logic to supplement the water quality monitoring capabilities provided by the sensor objects. The following new control actions can be implemented with the condition '*quality sensor detects concentration over a specific threshold*':

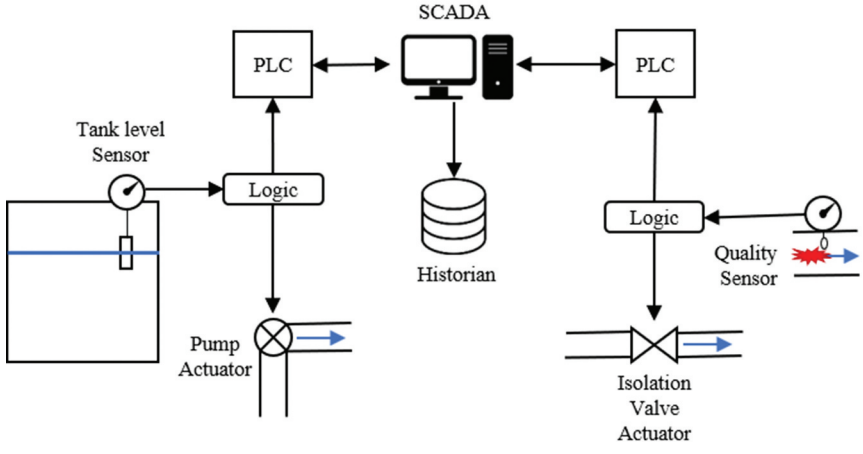

Figure 2. RISKNOUGHT cyber layer schem]atic overview for both hydraulics operation and quality monitoring.

- *Close a set of DMA isolation valves*: A user-specified set of pipes are regarded as isolation valves and can be closed by the SCADA system if a contamination event is detected. This action isolates DMAs to prevent contamination expansion.
- *Close a set of pumps/valves*: Similar to basic EPANET hydraulic controls, with the intent to cut-off supply to a specific contaminated area or isolate a non-contaminated one.
- *Activate a set of flushing units*: For these controls, RISKNOUGHT functions alter the topology of the WDN by automatically adding for each flushing unit a new node *f* and an initially closed pipe *p* connecting it to another user-specified node *n*. Node *f* is assigned a 'demand' that denotes its capacity to remove water from the system. All aforementioned properties are user-customizable. When the quality sensor associated with a flushing unit reads concentration values over the specified threshold, the respective monitoring PLC sends a signal to all actuators in the set to open the pipes connecting the flushing units.

It should be noted that due to EPANET's engine being in use there is a modelling constraint: if an area of the system is isolated, i.e. not connected with open pump/valves/pipes to a reservoir or a tank as the result of an action, no water will move through the network. Thus, water supply will stop immediately and a small albeit relevant portion of additional contaminated water volume found in pipes will not be consumed as it may be in real-world conditions. The same limitation appears in the case of flushing water from the system or from an isolated DMA. Without a reservoir or tank connected and supplying water, the simulation results will not show 'supply' to the flushing node, as well as other nodes in the same isolated area. Thus, no water will move through and out of the area. This can be alleviated by dividing the system to DMAs that have at least one tank or reservoir attached. If this is not possible due to network topology, another solution is to modify the system by including a virtual inflow node in the isolated area, connected with an initially closed pipe. The pipe should open with the response action and provide the flow to 'flush' out the contaminant from the flushing node.

RISKNOUGHT attack model for combinations of contamination attacks and cyber attacks

The cyber-physical attack model of RISKNOUGHT can accommodate combinations of physical attacks (e.g. sabotage, destruction of components, etc.) that during simulation affect the physical state of a component or an attribute of the WDN with cyber attacks (e.g. DoS, communication hijacking etc.) that during simulation affect the behaviour of the control scheme implemented. In this work, it is updated to include deliberate contamination attacks on the WDN, accompanied by cyber attacks to the CWS part of the SCADA. As such, on the physical side, RISKNOUGHT includes two types of contamination attacks:

- *Backflow contaminant injection attacks*: Simulates the perpetrator's intent of contaminating the network by injecting the contaminant directly to the network through a junction. Customizable attributes are *injection junction* (given by the name/ID), *start time* (s), *end time* (s) and *strength* (kg/s).
- *Tank/Reservoir contamination*: Simulates the contamination of the network through contaminating the volume of water in a tank or reservoir of the WDN. Customizable attributes are *initial contaminant's concentration* (mg/L) and the *target* (given by the name/ID).

RISKNOUGHT also includes a function to set-up initial contaminant concentration in nodes (i.e. junctions, tanks, reservoirs) for a specific scenario, instead of acquiring this info from the input .*inp* file. More than one physical attacks can be simulated in the same scenario e.g. two backflow contamination attacks at different nodes and starting at a different time. The physical attack routines can also be used for accidental contamination events in addition to deliberate actions. On the cyber side, RISKNOUGHT attack model includes a multitude of cyber attacks, as presented in Nikolopoulos et al. (2020). These attacks include:

- Sensor manipulation: Interception of transmitted sensor data and modification, fabrication of data (e.g. fake a contamination event).
- DoS on cyber components (sensors, actuators, PLCs, central SCADA, historian etc.): disruption of communication between targeted field devices and the system, or complete system take-down.
- Cyber attacks on the historian (e.g. an SQL injection attack, data record manipulation etc.): useful in simulating attacks that modify records of the system in cases where controls rely in past data and not on current sensor readings.
- Actuator/ACK (acknowledgment) signal manipulation: attacks that alter the response of the system to controls and can mask their presence by faking correct orders.

As with physical attacks, various combinations of cyber attacks can happen in conjunction. Of particular interest within this paper are cyber-physical attacks with a backflow injection attack happening at the same time with sensor manipulation attempts to mask the contamination and blind the monitoring system, or DoS attacks to make the CWS unable to function. Another special type of sensor manipulation attacks is the fabrication of fake contamination events that aim to only disrupt service without risking public health. For cyber-attacks on sensors, the following attributes are needed:

- Cyber-attack type: *assign value* or *DoS*
- start time: *s*
- end time: *s*
- target:*valid sensor name/ID*

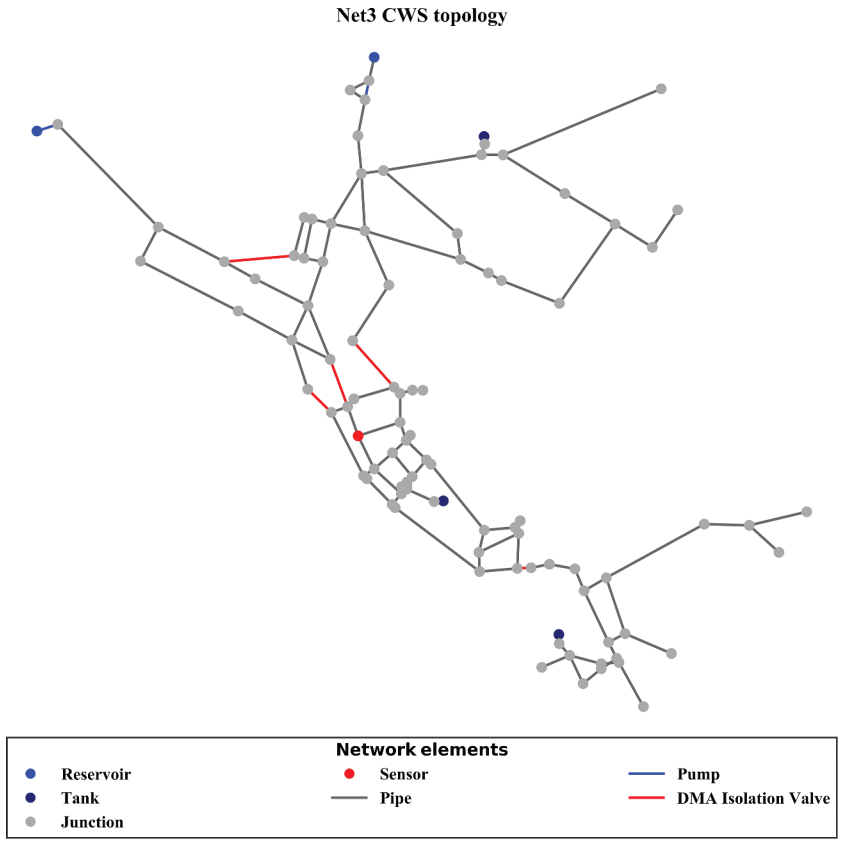

Figure 3. Net3 network topology.

Example of RISKNOUGHT monitoring and response measures simulation

Figure 3 depicts the simple EPANET test network 'Net 3'. We define a baseline scenario in RISKNOUGHT, without a quality monitoring control scheme, where the following physical attack is happening (see the injection node in Figure 3):

- *Backflow injection attack* at junction '*115*', from start time *0 s* to end time *3600 s*, with injection strength *1 kg/s*, of a conservative contaminant (i.e. there is no bulk/wall reactions and no diffusion).

RISKNOUGHT automatically constructs the SCADA representation of the hydraulic control logic. The scenario simulation duration is set to 24 hours with a hydraulics timestep of 15 min and a quality solver timestep of 5 min. As there are no quality sensors, the contamination is unnoticed, and in total 3219.05 kg of contaminant mass is consumed. The total unaltered water supply, the growing cumulative mass consumption and the contamination extents to the whole WDN downstream of node '115' are presented in Figure 4. Then, the same network is modified by RISKNOUGHT to include a single quality sensor and a set of isolation valves dividing the WDN to four DMAs and a flushing unit as described in Table 1 and shown in Figure 3. The contamination attack is identified at simulation time 6300 *s*, the DMAs are isolated and in total 2919.30 kg of contaminant mass is consumed. The water supply is reduced as tanks empty, the cumulative mass consumption stops growing early as the contaminant mass is either consumed or contained within isolated DMAs without water supply and the extent of the contamination is reduced, as shown in Figure 4. Finally, using the last topology, a flusher unit is added near the junction with the sensor. The unit is activated when a contamination event is detected, with an outflow of 0.25 m^3/s (Table 1). The activation of the flushing unit results in total consumption of 2266.58 kg of contaminant mass, signifying an improvement in the response strategy, as seen in Figure 4.

Demonstrating the platform's stress-testing capability through a synthetic case study

C-Town (Ostfeld et al. 2012) is a known benchmark model based on a real medium-sized WDN, that has been previously used for cyber-physical studies (Taormina et al. 2017; Nikolopoulos et al. 2020) and quality simulation (Sankary and Ostfeld 2019). We use RISKNOUGHT to create a SCADA for the hydraulic controls that are based on the tanks' levels, with a set of 20 controls, as shown in Nikolopoulos et al. (2020) and described in the network's .inp file. A topology of seven sensors is generated with the Threat Ensemble Vulnerability Assessment and Sensor Placement Optimization Tool (TEVA-SPOT) (Berry et al. 2012) using the mean contamination extent objective function (Kessler, Ostfeld, and Sinai 1998; Watson, Greenberg, and Hart 2004). Assuming perfect sensors, this ensemble of sensors accomplishes the detection of contamination events that cover 43.8% (170 out of 388) possible entry

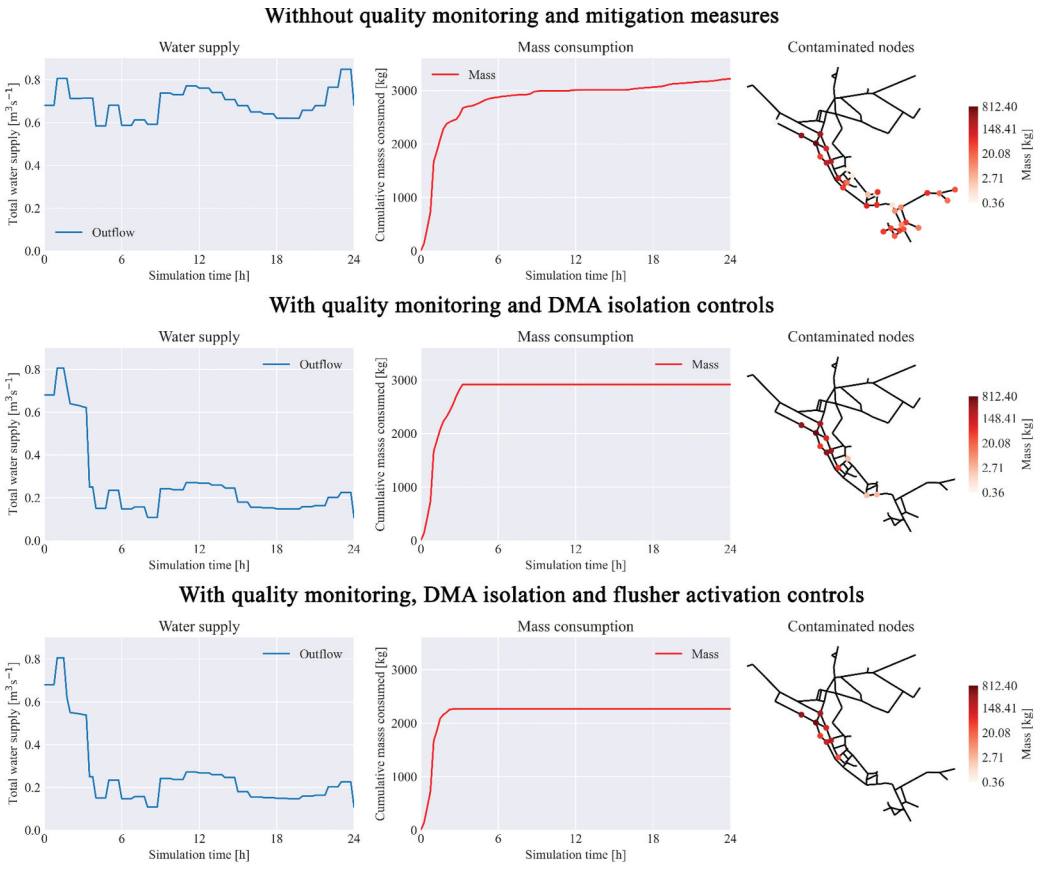

Figure 4. Illustration of Net3 performance for different cyber-physical schemes under the same backflow attack.

Table 1. New components added to cyber and physical layers.

Components	Elements
Sensors	Placed at junction 267, named S267
Isolation valves	Placed at pipes 117, 116, 177, 223, 238
Isolation valves control logic	'If concentration readings of S267 above 0.001 mg/L close pipes 117, 116, 177, 223, 238'
Flushing unit	New junction F267, connected to junction 267 with a new initially closed pipe I267, demand: 0.25 m^3/s
Flushing unit control logic	'If concentration readings of S267 above 0.001 mg/L open I267'

points for contaminant of the network, with the non-monitored location residing in remote branches of the WDN (a contamination there will be not detected but self-contained due to water flow conditions). The physical layer is updated with the inclusion of four isolation valves that separate the WDN into five DMAs, and five flushing units in the form of water hydrants, one in each DMA in lower elevation points. The cyber layer is updated with the respective sensor and actuator units, as well as control logic to be used as response and mitigation measures in the event of contamination detection. The modified C-Town topology is shown in Figure 5, a schematic representation of the cyber layer in and the cyber elements and respective controls in Figure 6, Table 2.

This topology is stress-tested against scenarios of cyber-physical attacks. The following metrics are used to quantify the effect of the attack on the system using four dimensions, influenced by the methodology presented in (Moraitis et al. 2020)

- Temporal dimension: earliest detection time (EDT) – the time delta between the contaminant injection and the first report of a contamination event from the quality sensors in *s*.
- Spatial dimension: ratio of supply nodes affected with lower quality water (NA) – ratio of supply nodes with concentration above 0 *mg/l*Lto the total number of supply nodes.
- Contaminant dimension: total mass consumed (MC) – total consumed mass in *kg* during the simulation period. By consumption we define all interactions with supplied water, not specifically ingestion by customers. Also, we define the total mass consumed before detection (MCBD) as a more representative metric of contaminant consumption, because usually when a contaminant is detected, a 'do-not-use' public warning is issued (not modelled in the scenarios presented here). Related to this dimension is the flushed mass (FM), the contaminant mass in *kg* removed from the system by the activation of flushing units.

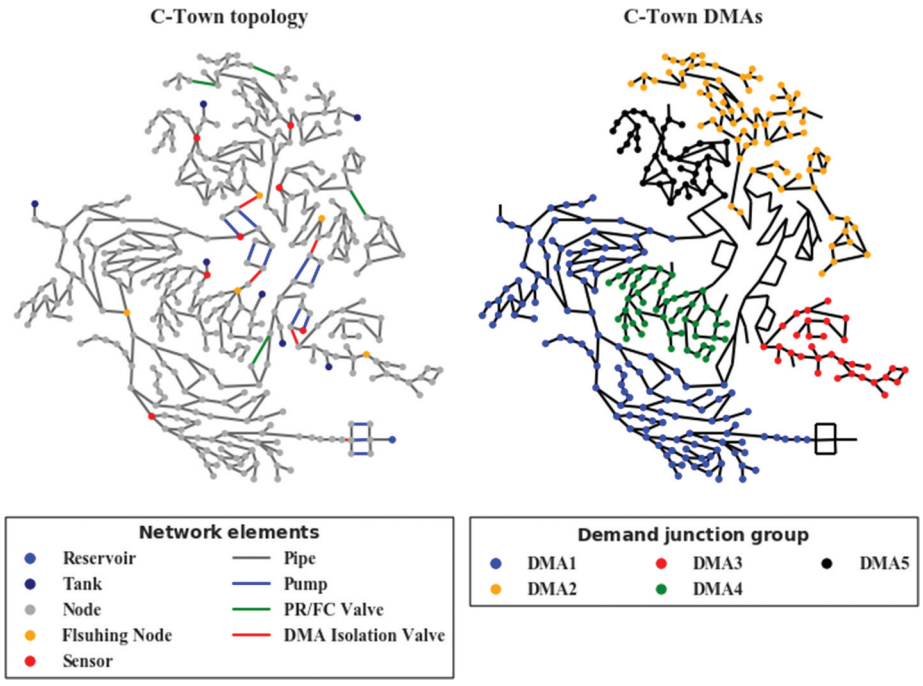

Figure 5. Left: C-Town modified topology, including sensors, DMA isolation valves, flushing units. Right: The five DMAs of C-Town.

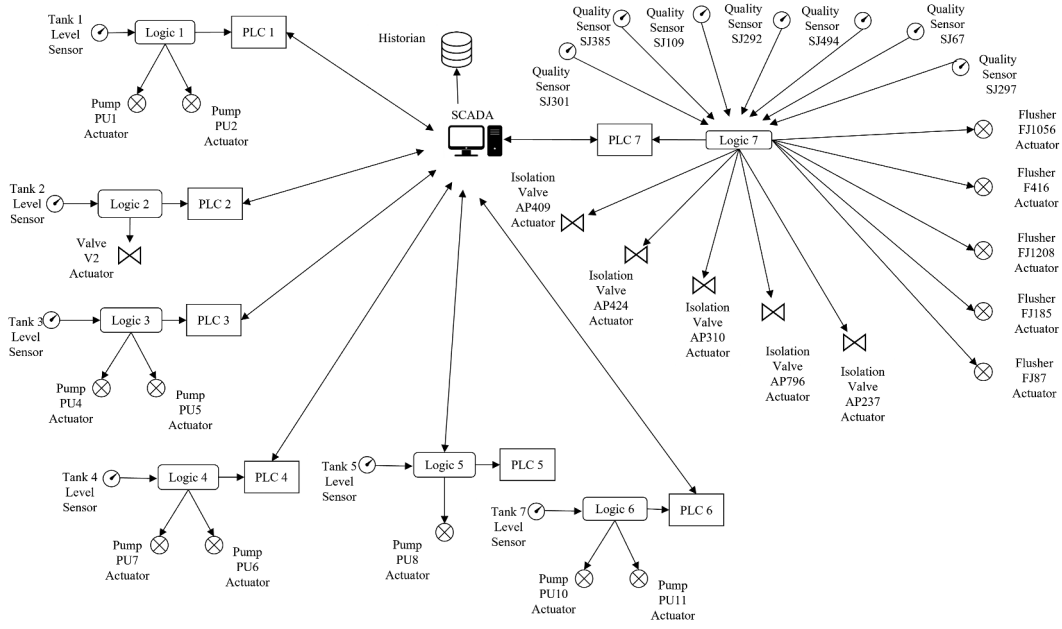

Figure 6. Schematic representation of the cyber layer. The 'logic' components are groups of control logic statements for brevity reasons.

Table 2. Cyber elements and controls for quality monitoring and response strategy (note that the actual controls that adhere to the control logic are 49).

Components	Elements
Sensors	Placed at junctions J301, J385, J109, J292, J494, J67, J297, prefixed with 'S'
DMA isolation valves actuators	Placed at pipes P409, P424, P310, P796, and P237, prefixed with 'A'
DMA isolation valves control logic	'If concentration readings of ANY sensor above 0.001 mg/L close ALL DMA isolation valves'
Flushing units	New nodes adjacent to present nodes J1056, J416, J1208, J185, and J87, Prefixed with 'F'
Flushing unit control logic	'If concentration readings of the DMA's sensor above 0.001 mg/L open the DMA's flushing unit's isolation valve'

- Water supply dimension: unmet demand (UD) – the total volume of water not delivered to customers in m^3, as a result of the attack scenario. Note that high values in this metric is not always detrimental to the service, i.e. when the mitigation measures (flushers) are activated, which is captured by another related metric, flusher outflow (FO) in m^3.

Scenario 0: backflow injection attack

An example backflow injection attack is simulated with both basic EPANET 2.2. i.e. without the quality monitoring and response measures) and with the RISKNOUGHT cyber-physical model, for comparison purposes. The physical attack's injection node is 'J159', from start time 10:00 to end time 11:00, with mass flowrate 0.001 kg s^{-1}, and the contaminant is a conservative species, i.e. there is no bulk/wall reactions and no diffusion. The scenario simulation duration is set to 24 hours with a hydraulics timestep of 10 min and a quality solver timestep of 5 min. In the EPANET simulation, a total of 3.055 kg of contaminant mass is consumed (MC), affecting 92.26% of the nodes (NA). The total unaltered water supply, the growing cumulative mass consumption, and the contamination extents to the whole WDN downstream of node 'J159' are presented in Figure 7. The same physical attack in RISKNOUGHT with the CWS system in operation is detected by sensor SJ109 at time 10:40 (40 min after injection). This means that only 0.054 kg of contaminant mass is consumed before detection and up to 1.213 kg during the event, depending on if and how fast and effectively a do-not use general public warning is issued (the water demands remain currently unchanged in RISKNOUGHT) The contamination extent is lower, as 8.5% of the nodes are affected, while there is an unmet demand volume of 8465.44 m^3. The water supply is reduced as tanks empty, the cumulative mass consumption stops growing early as the contaminant mass is either consumed or contained within isolated DMAs without water supply and the extent of the contamination is reduced, as shown in Figures 7 and 9.

Scenario 1: single sensor manipulation

A perpetrator performs a backflow injection attack that is discussed above but has also hijacked the connection of sensor SJ109. For 4 h, from 10:00 to 14:00 fake normal quality readings are replayed and received from the SCADA. In this hypothetical case, it is assumed that sensors in the CWS are perfect and can measure the concentration of the contaminant, so the replayed values are a timeseries of 0.0 mg/L. Simulation results show that the contaminant spreads from its source past the monitoring point, enters other DMAs, when it is finally detected at the same timestep, at time 11:10 (EDT: 3900 *s*) by two sensors,

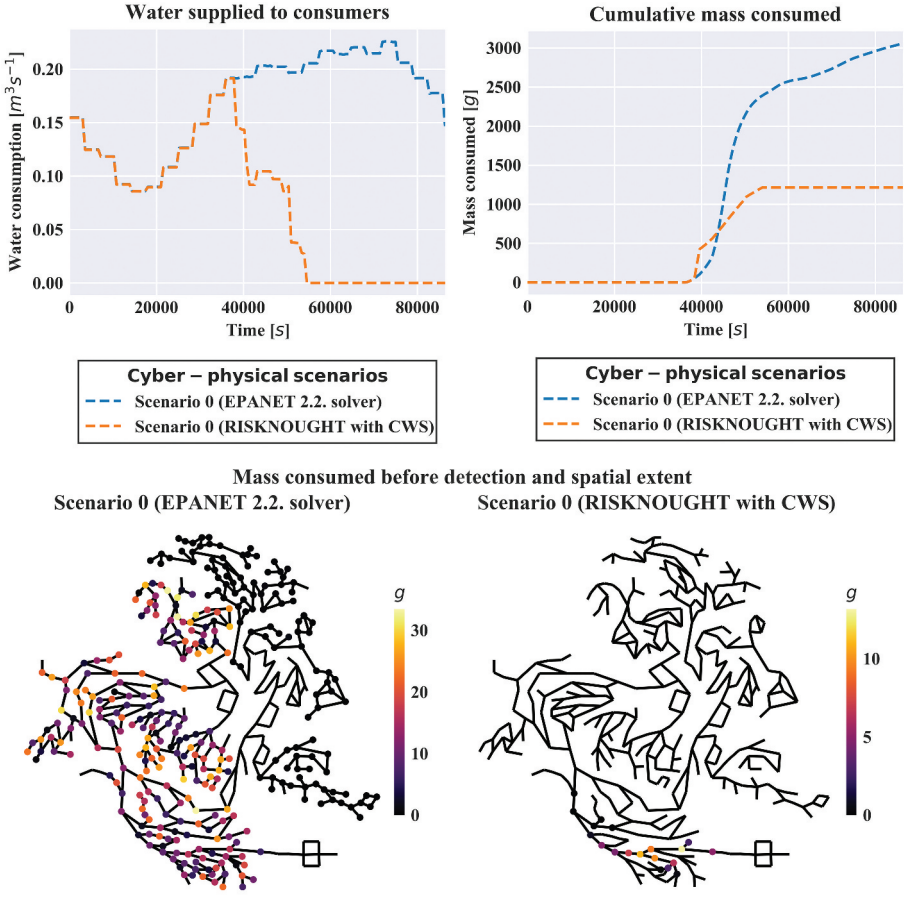

Figure 7. Scenario 0 and comparison with a basic EPANET 2.2 simulation. Top left: Water supply. Top right: contaminant mass consumed. Bottom: Spatial extent of contamination.

SJ385 and SJ494 (both in DMA2). Before detection (MCBD), 0.143 kg of contaminant mass are consumed which is a 265.16% increase compared to the benchmark scenario, and up to (MC) 1.127 kg during the event, assuming no change in water demand due to an issued public warning. The delayed (by 30 min compared to Scenario 0) response and mitigation measures result in FO of 4817.44 m^3, FM is 0.56 kg, NA is 43.56% of the WDN's nodes and UD is 8006.50 m^3.

Scenario 2: manipulation of all sensors

This scenario is a variant of the previous one, but the perpetrator accomplishes the exploitation of all sensors in the CWS for 4 h, so fake normal quality readings are received from all sensors from 10:00 to 14:00. In this case, the attack is detected right after the end of the cyber-attack at 14:10 (note that the discretization step of the simulation is 10 min). The impact of the attack is larger with MCBD of 2.219 kg at 14:10 (EDT: 15000 *s*), with up to MC 2.636 kg in the simulation period. The attack results in most of the WDN's nodes becoming contaminated (NA 92.01%), due to the DMA isolation happening late (just after the cyber-attack's end). The late flushing results in FO of 4657.8 m^3 with FM 0.168 kg, while UD is lower at 5894.32 m^3.

Scenario 3: DoS on the connections to actuators

In this case, the perpetrator performs the same physical part of the attack as scenarios 1 and 2 but changes the cyber-attack type to DoS on the connections to actuators isolating the DMAs. Therefore, the attack is detected by SJ109 at 10:40 (EDT: 2400 *s*) but there is a delay of 1 hour to manually regain control of the isolation valves. The flashing units operate as normal (unaffected by the cyber-attack), so MCBD is 0.054 kg and MC 0.697 kg, while FM is 2.417 kg due to FO of 5754 m^3). The 32.47% of nodes are affected by the contaminant (NA) and UD is 8469.98 m^3.

Scenario 4: sensor manipulation at a targeted DMA

The perpetrator performs a sophisticated targeted cyber-physical, by a) performing a backflow injection rate of 0.001 kgs^{-1} from 13:00 to 14:00 at node J292, with the intent to target specifically the area of the network contained in DMA3, b) hijacking the connection of sensor SJ292 and replaying normal water quality readings from 13:00 to 23:59. The attack goes undetected, as contaminated water cannot flow to other parts of the network, resulting in 2.057 kg of contaminant consumed (the rest resides in the pipes of the DMA and tank T3) in the 11 h time frame. 0

Scenario 5: fake contamination event

In this scenario, the intent of the perpetrator is to cause chaos in the water utility rather than contaminating the water, so the attack consists of only a cyber attack, i.e. hijacking the connection of sensor SJ109. For 14 h, from 10:00 to 23:59 forged quality readings are relayed to the SCADA, indicating a severe contamination event (a timeseries of large concentration values, i.e. 10 mg/L). The result of the cyber attack is that all DMAs are isolated and flushers are activated, disrupting the water supply to consumers as seen in Figure 8. In total, 8932.36 m^3 of water are not delivered (UD) and a total of 4823.96 m^3 are flushed (FO).

Figures 8–10 illustrate the impact of Scenarios 1,2,3,4 and 5 in the water supplied, contamination extent and contaminant mass consumed dimensions.

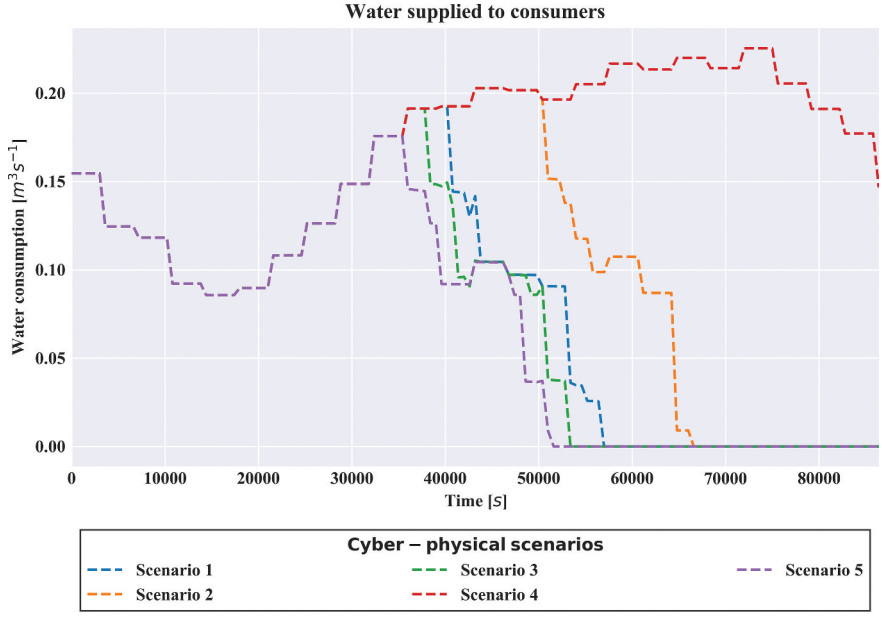

Figure 8. Water supplied to consumers in different scenarios. Note that Scenario 3 curve is the same as the expected consumption, because no response measures are activated.

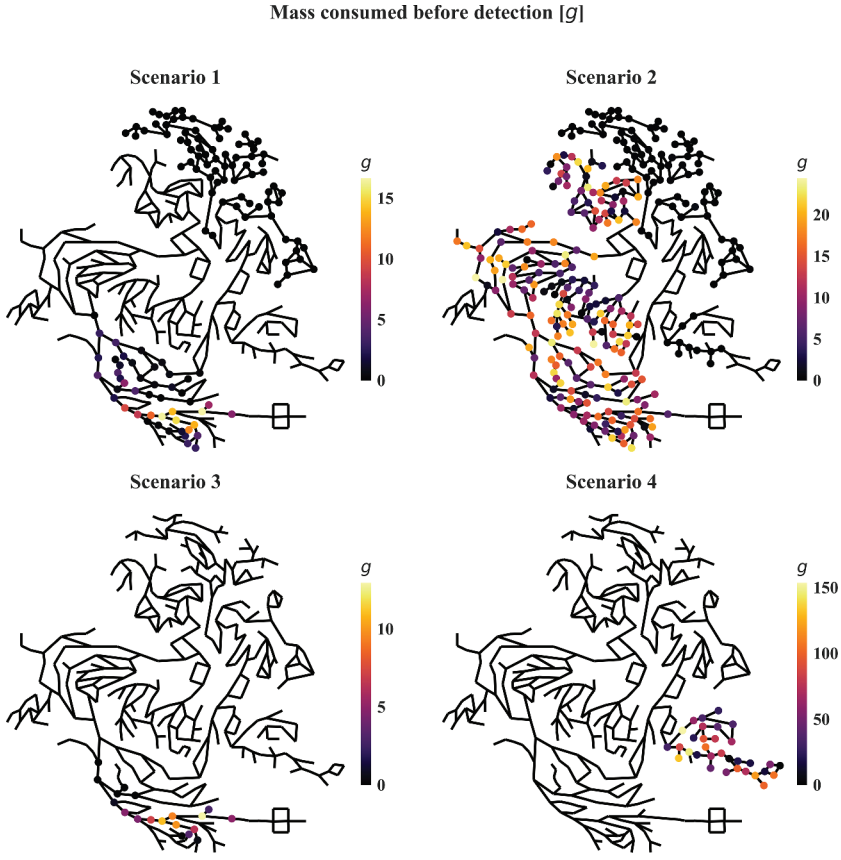

Figure 9. Mass consumed before detection in each node and spatial extent of contamination in each scenario. Note that in Scenario 5 there is no contaminant injection and is not included in the figure.

Discussion

Because C-Town in based on a medium sized real-world city and has a fairly common single water source and branched-DMA network topology, we can gain insights applicable for many water utilities worldwide. Scenario 0 showcases the lessened impact that a physical attack bears when countered with an effective CWS and response measures, as it is evident by comparing with a simulation of the attack without such monitoring and control schemes in EPANET. However, as seen from the scenarios, especially from the Scenario 4, due to complex flow conditions, the temporal and spatial characteristics of any attack are crucial for detection by sensors, along with their placement strategy and number, as it is possible that contaminated water may never reach a (working) quality monitoring location and go totally unnoticed. Case in point, in Scenario 4 sensor SJ292 is rendered useless by a cyber-attack, demoting a significant part of the network (a whole DMA) to an unmonitored area, even though there are six other quality monitor sensors in the network. Large parts of common networks pertaining to branches downstream of sensors, essentially are unmonitored areas, as in the C-Town example. This fact could possibly affect a perpetrator's decision with insider knowledge of the network and its monitoring strategy for purely physical attacks. There are 'blind' spots for quality sensors both in a temporal, as well as a spatial manner and this should be taken into account in water security plans, as dangerous entry points for injection of contaminants. Equally, quality sensors located at the outskirts of the network can be considered critical for cyber-physical protection (e.g. hindering physical access, implementation of cyber-security measures) as their compromise, can be devastating. On the contrary, other 'upstream' (relative to the source, end nodes and other sensors) sensors can be considered less critical, as their compromise by cyber-attacks (or even simple malfunctions) can have a less harmful impact due to the redundancy in detection capability of the overlaps in monitoring capability provided by other sensors. This is demonstrated in Scenario 1, where the cyber-attack on sensor SJ109 has the effect of imposing a considerable lag in detection of the contaminant injection, but the CWS will eventually be alerted. However, there is a significant effect to the risk management of the event, not considered in this case study, which is the tracing of the contamination to identify its origins with one of the sensors being manipulated.

Scenarios 0, 1, 2 and 3 are comparable as the physical attack part is the same, but the cyber-attack part is different. Scenario 0 can be considered the baseline between a cyber-physical water system that employs a working CWS and one that is unmonitored for quality. Scenario 2 contrasts Scenario 1, because even though the cyber attack has the same duration, the attack severity is higher in Scenario 2, as all sensors are compromised, and as expected the impact difference is

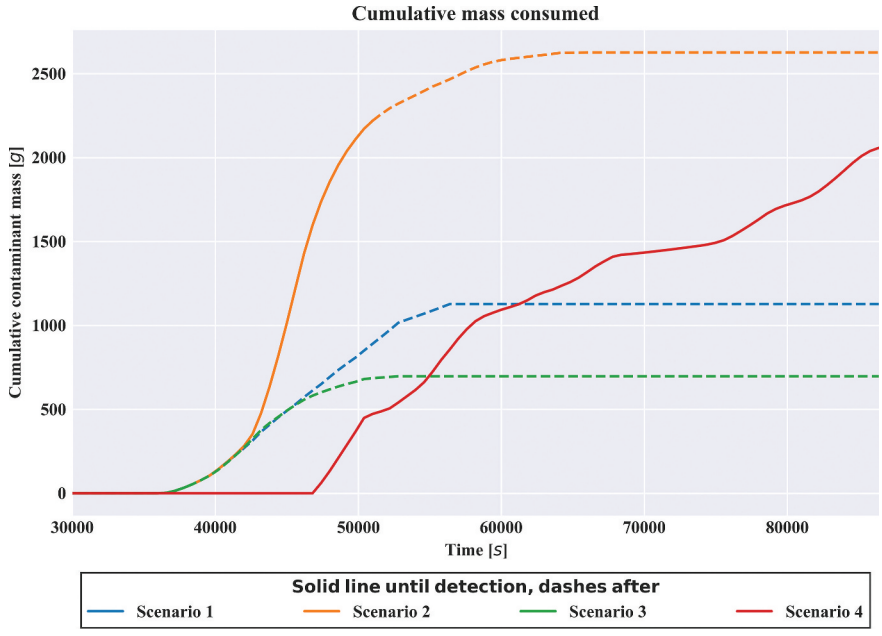

Figure 10. Cumulative mass consumed during the cyber-physical attacks. Scenario 5 is not shown, as there is no real-backflow injection.

significant. The contamination event is detected by the end of the four hour long cyber attack in Scenario 2 while in Scenario 1 the attack is detected after one hour and ten minutes, half an hour later than the baseline detection performance of Scenario 0. As such, there is an increase of 1551.74% and 213.6% in MCBD and NA metrics respectively, illustrating the importance of rapid detection. In Scenario 3, detection is timely, like in Scenario 0, but the type of cyber-attack (DoS on actuators) renders the activation of some of the response and mitigation measures impossible, i.e. the isolation of DMAs. However flushing units are operational and manage to flush out 2.417 kg of the contaminant, with higher FO than the other scenarios due to the continuous water supply from the source. As such, while MCBD is on par with Scenario 0 and 63% lower than Scenario 1, there is the possibility of increased MC up to nearly half that of Scenario 1. In general, for all scenarios MC depends on the efficiency of the public warning issued for avoiding consumption, which may or may be not functional, deployed or even under cyber-attack by the same perpetrator. The upper bounds of MC interestingly are higher in Scenario 0 than Scenario 1, due to the flow conditions generated with the isolation of DMAs in the worst case of not issuing a public warning for consumption and the spread of the contaminant to tanks, pipes etc.

With regards to the impact of cyber-physical attacks to the general public and a water utility, even the faking of a contamination event by manipulating sensor information has devastating impacts, as shown in Scenario 5, where even though there is no contamination and thus no health risks, there is high UD, as well as uncalculated monetary losses to the utility and possible reputation damage.

Another interesting point stems from the Scenario 4, in which there is a targeted attack on a specific targeted area. MC is high and still not totally consumed in the timeframe of the simulation, with a considerable amount still stored in the DMA3's Tank3 and pipes. However, MC is distributed across a smaller extent and population, leading to higher doses to the population than in the other scenarios. The contaminant used in this synthesized case study is a conservative hypothetical substance, with not known properties regarding the health of consumers, and therefore concentrations and actual digestion/inhale doses are not considered. Further research can focus on modelling the interactions of a real substance in the WDN, and the health impacts on consumers according to the received dose. Another consideration for research is the usage of such stress-testing scenarios in water quality sensor placement studies. The seven-sensor design in the example case study of C-Town can monitor only a subset of the nodes (43.8% of the 388 nodes), albeit the most important ones for minimizing the extent of contamination. However, performance changes significantly when considering the possibilities cyber-attacks and more thorough studies in sensor placement optimization (optimizing both the number of sensors and spatial locations) are needed along with resilience assessment (Makropoulos et al. 2018; Nikolopoulos et al. 2019b) of sensor designs (Nikolopoulos et al. 2021), also taking into account the properties and specific vulnerabilities of components to specific types of cyber attacks (e.g. a particular sensor and its connection may be more vulnerable to DoS attacks, than hijacking ad altering the transmitted information) and RISKNOUGHT can be incorporated as the simulation stress-testing tool in such procedures. It is also worth mentioning that cyber-physical WDNs are dynamic systems affected by a multitude of parameters interacting both from a hydraulic and environmental (temporal and spatial characteristics of water supply, quality properties of a contaminant etc.) and a consumer's behavioural (water demand patters etc.) perspective. Thus, in future real-world applications of stress-testing and assessment of performance of cyber-physical attacks the simulation of the stochastic processes (Tsoukalas, Kossieris, and Makropoulos 2020) involved should be considered to be used as input data for the case studies.

Conclusions

We presented the recent expansion of the RISKNOUGTH cyber-physical stress-testing platform to handle quality-related simulations and related cyber-physical attacks. We have also demonstrated the use of the platform through cyber-physical attack scenarios evaluated against several performance metrics, to demonstrate their impact on water distribution networks. With these capabilities, it is suggested that RISKNOUGHT can be utilized to analyze cyber-physical attack events in cyber-aware water utilities, improve risk management practices by providing cyber-physical analysis input to water security plans, prioritize protection measures, and aid in sensor placement methodologies and cyber-layer design.

Acknowledgements

This work was 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.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Horizon 2020 Framework Programme [740610].

References

Albert, Monique, Wim Hijnen, Jojanneke Van Vossen, and Mirjam Blokker. 2017. "Modelling Bacterial Biomass in a Non-Chlorinated Drinking Water Distribution System." *Procedia Engineering* 186: 127–134. doi:10.1016/j.proeng.2017.03.218.

Alfonso, Leonardo, Andreja Jonoski, and Dimitri Solomatine. 2010. "Multiobjective Optimization of Operational Responses for Contaminant Flushing in Water Distribution Networks." *Journal of Water Resources Planning and Management* 136 (1): 48–58. doi:10.1061/(ASCE)0733-9496(2010)136:1(48).

Allmann, Timothy P., and Kenneth H Carlson. 2005. "Modeling Intentional Distribution System Contamination and Detection." *Journal - American Water Works Association* 97 (1): 58–61. doi:10.1002/j.1551-8833.2005.tb10808.x.

Almalawi, Abdulmohsen, Zahir Tari, Ibrahim Khalil, and Adil Fahad. 2013. "SCADAVT-A Framework for SCADA Security Testbed Based on Virtualization Technology." In *38th Annual IEEE Conference on Local Computer Networks, 21-24 October*, 639–646. Sydney, NSW: IEEE. doi:10.1109/LCN.2013.6761301.

Antonioli, Daniele, and Nils Ole Tippenhauer. 2015. "MiniCPS." In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy - CPS-SPC '15*, 91–100. New York, NY: ACM Press. doi:10.1145/2808705.2808715.

Berry, Jonothan, Erik Boman, Lee Ann Riesen, William E. Hart, Cynthia A. Phillips, and Jean-Paul Watson. 2012. *User's Manual: TEVA-SPOT Toolkit 2.5.2*. Cincinnati, OH: U.S. Environmental Protection Agency.

Burkhardt, Jonathan B., Jeff Szabo, Stephen Klosterman, John Hall, and Regan Murray. 2017. "Modeling Fate and Transport of Arsenic in a Chlorinated Distribution System." *Environmental Modelling and Software* 93: 322–331. doi:10.1016/j.envsoft.2017.03.016.

Chang, Ni Bin, Natthaphon P. Pongsanone, and Andrew Ernest. 2013. "A Rule-Based Decision Support System for Sensor Deployment in Small Drinking Water Networks." *Journal of Cleaner Production* 60: 152–162. doi:10.1016/j.jclepro.2012.10.036.

Ciaponi, Carlo, and Enrico Creaco. 2018. "Comparison of Pressure-Driven Formulations for WDN Simulation." *Water* 10 (4): 523. doi:10.3390/w10040523.

Coelho, M., Batlle Ribas, M. and Coimbra, M. 2020. Review of technologies for the rapid detection of chemical and biological contaminants in drinking water, edited by Giannopoulos, G. and Cardarilli, M. Luxembourg: Publications Office of the European Union. doi:10.2760/71247.

Cooper, William J. 2014. "Responding to Crisis: The West Virginia Chemical Spill." *Environmental Science & Technology* 48 (6): 3095. doi:10.1021/es500949g.

Corso, Phaedra S., Michael H. Kramer, Kathleen A. Blair, David G. Addiss, Jeffrey P. Davis, and Anne C. Haddix. 2003. "Cost of Illness in the 1993 Waterborne Cryptosporidium Outbreak, Milwaukee, Wisconsin." *Emerging Infectious Diseases* 9 (4): 426–431. doi:10.3201/eid0904.020417.

Ed, M, and G Ed. 2019. "Guidance on the Production of a Water Security Plan for Drinking Water Supply." doi:10.2760/415051.

Eliades, D. G., T. P. Lambrou, C. G. Panayiotou, and M. M. Polycarpou. 2014. "Contamination Event Detection in Water Distribution Systems Using a Model-Based Approach." *Procedia Engineering* 89: 1089–1096. doi:10.1016/j.proeng.2014.11.229.

Fovino, Igor Nai, Marcelo Masera, Luca Guidi, and Giorgio Carpi. 2010. "An Experimental Platform for Assessing SCADA Vulnerabilities and Countermeasures in Power Plants." In *3rd International Conference on Human System Interaction, HSI'2010 - Conference Proceedings*, 679–686. doi:10.1109/HSI.2010.5514494.

Ginsberg, M. D., and V. F. Hock. 2004. "Terrorism and Security of Water Distribution Systems: A Primer." *Defense and Security Analysis* 20 (4): 373–380. doi:10.1080/1475179042000305822.

Giudicianni, C., M. Herrera, A. Di Nardo, R. Greco, E. Creaco, and A. Scala. 2020. "Topological Placement of Quality Sensors in Water-Distribution Networks without the Recourse to Hydraulic Modeling." *Journal of Water Resources Planning and Management* 146 (6): 04020030. doi:10.1061/(ASCE)WR.1943-5452.0001210.

Gleick, Peter H. 2006. "Water and Terrorism." *Water Policy* 8 (6): 481–503. doi:10.2166/wp.2006.035.

Hagberg, A A, D A Schult, and P J Swart. 2008. "Exploring Network Structure, Dynamics, and Function Using NetworkX." In *7th Python in Science* Conference *(SciPy 2008)*, no. SciPy: 11–15. Pasadena, CA.

Hassanzadeh, Amin, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M. Katherine Banks. 2020. "A Review of Cybersecurity Incidents in the Water Sector." *Journal of Environmental Engineering* 146 (5): 03120003. doi:10.1061/(ASCE)EE.1943-7870.0001686.

Hoxie, N J, J P Davis, J M Vergeront, R D Nashold, and K A Blair. 1997. "Cryptosporidiosis-Associated Mortality following a Massive Waterborne Outbreak in Milwaukee, Wisconsin." *American Journal of Public Health* 87 (12): 2032–2035. doi:10.2105/AJPH.87.12.2032.

Industrial Control Systems Cyber Emergency Response Team. 2016. "ICS-CERT Year in Review." https://www.us-cert.gov/ics/Year-Review-2016

Kenzie, William R., Neil J. Mac, Mary E. Hoxie, M. Proctor, Stephen Gradus, Kathleen A. Blair, Dan E. Peterson, et al. 1994. "A Massive Outbreak in Milwaukee of Cryptosporidium Infection Transmitted through the Public Water Supply." *New England Journal of Medicine* 331 (3): 161–167. doi:10.1056/NEJM199407213310304.

Kessler, Avner, Avi Ostfeld, and Gideon Sinai. 1998. "Detecting Accidental Contaminations in Municipal Water Networks." *Journal of Water Resources Planning and Management* 124 (4): 192–198. doi:10.1061/(ASCE)0733-9496(1998)124:4(192).

Klise, Katherine A., Michael Bynum, Dylan Moriarty, and Regan Murray. 2017. "A Software Framework for Assessing the Resilience of Drinking Water Systems to Disasters with an Example Earthquake Case Study." *Environmental Modelling and Software* 95 (September): 420–431. doi:10.1016/j.envsoft.2017.06.022.

Laird, Carl D., Lorenz T. Biegler, Bart G. van Bloemen Waanders, and Roscoe A. Bartlett. 2005. "Contamination Source Determination for Water Networks." *Journal of Water Resources Planning and Management* 131 (2): 125–134. doi:10.1061/(ASCE)0733-9496(2005)131:2(125).

Lee, E. A. (2008). Cyber Physical Systems: Design Challenges. 200*811th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 363–369. doi:10.1109/ISORC.2008.25

Makropoulos, C., D. Nikolopoulos, L. Palmen, S. Kools, A. Segrave, D. Vries, S. Koop, et al. 2018. "A Resilience Assessment Method for Urban Water Systems." *Urban Water Journal* 15 (4): 316–328. doi:10.1080/1573062X.2018.1457166.

Makropoulos, C., and D. A. Savić. 2019. "Urban Hydroinformatics: Past, Present and Future." *Water* 11 (10): 1959. doi:10.3390/w11101959.

McKinney, W. (2010). *Data Structures for Statistical Computing in Python*, 56–61. doi:10.25080/Majora-92bf1922-00a.

Moraitis, Georgios, Dionysios Nikolopoulos, Dimitrios Bouziotas, Archontia Lykou, George Karavokiros, and Christos Makropoulos. 2020. "Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats." *Journal of Environmental Engineering* 146 (9): 04020108. doi:10.1061/(ASCE)EE.1943-7870.0001765.

Murillo, Andres, Riccardo Taormina, Nils Tippenhauer, and Stefano Galelli. 2020. "Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments." In *Sixth Annual Industrial Control System Security (ICSS) Workshop*, PartF16834:13–20. New York, NY: ACM. doi:10.1145/3442144.3442147.

Nikolopoulos, Dionysios, Avi Ostfeld, Elad Salomons, and Christos Makropoulos. 2021. "Resilience Assessment of Water Quality Sensor Designs under Cyber-Physical Attacks." *Water* 13 (647): 1–23. doi:10.3390/w13050647.

Nikolopoulos, Dionysios, Christos Makropoulos, Dimitrios Kalogeras, Klio Monokrousou, and Ioannis Tsoukalas. 2018. "Developing a Stress-Testing Platform for Cyber-Physical Water Infrastructure." In *2018 International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater), 10-13 April*, 9–11. Porto, Portugal: IEEE. doi:10.1109/CySWater.2018.00009.

Nikolopoulos, Dionysios, Georgios Moraitis, Dimitrios Bouziotas, Archontia Lykou, George Karavokiros, and Christos Makropoulos. 2020. "Cyber-Physical Stress-Testing Platform for Water Distribution Networks." *Journal of Environmental Engineering* 146 (7): 04020061. doi:10.1061/(ASCE)EE.1943-7870.0001722.

Nikolopoulos, Dionysios, Georgios Moraitis, Dimitrios Bouziotas, Archontia Lykou, Georgios Karavokiros, and Christos Makropoulos. 2019a. "RISKNOUGHT: A Cyber-Physical Stress-Testing Platform For Water Distribution Networks." In *11th World Congress on Water Resources and Environment (EWRA 2019) "Managing Water Resources for a Sustainable Future", 2-6 July*. Madrid, Spain.

Nikolopoulos, Dionysios, Henk-Jan van Alphen, Dirk Vries, Luc Palmen, Stef Koop, Peter van Thienen, Gertjan Medema, and Christos Makropoulos. 2019b. "Tackling the 'New Normal': A Resilience Assessment Method Applied to Real-World Urban Water Systems." *Water* 11 (2): 330. doi:10.3390/w11020330.

Ostfeld, Avi, Elad Salomons, Lindell Ormsbee, James G. Uber, Christopher M. Bros, Paul Kalungi, Richard Burd, et al. 2012. "Battle of the Water Calibration Networks." *Journal of Water Resources Planning and Management* 138 (5): 523–532. doi:10.1061/(asce)wr.1943-5452.0000191.

Queiroz, Carlos, Abdun Mahmood, Jiankun Hu, Zahir Tari, and Xinghuo Yu 2009. "Building a SCADA Security Testbed." In *2009 Third International Conference on Network and System Security*, 357–364. IEEE. doi:10.1109/NSS.2009.82.

Queiroz, Carlos, Abdun Mahmood, and Zahir Tari. 2011. "SCADASimA Framework for Building SCADA Simulations." *IEEE Transactions on Smart Grid* 2 (4): 589–597. doi:10.1109/TSG.2011.2162432.

Rasekh, Amin, Amin Hassanzadeh, Shaan Mulchandani, Shimon Modi, and M. Katherine Banks. 2016. "Smart Water Networks and Cyber Security." *Journal of Water Resources Planning and Management* 142 (7): 1–3. doi:10.1061/(ASCE)WR.1943-5452.0000646.

Rasekh, Amin, and Kelly Brumbelow. 2014. "Drinking Water Distribution Systems Contamination Management to Reduce Public Health Impacts and System Service Interruptions." *Environmental Modelling and Software* 51: 12–25. doi:10.1016/j.envsoft.2013.09.019.

Rasekh, Amin, and Kelly Brumbelow. 2015. "A Dynamic Simulation-Optimization Model for Adaptive Management of Urban Water Distribution System Contamination Threats." *Applied Soft Computing Journal* 32: 59–71. doi:10.1016/j.asoc.2015.03.021.

Rossman, Lewis A., Hyoungmin Woo, Michael Tryby, Feng Shang, Robert Janke, and Terranna Haxton. 2020. *"EPANET 2.2 User Manual". 2.2*. Cincinnati, OH: U.S. Environmental Protection Agency.

Salem, Harry. 2003. "Issues in Chemical and Biological Terrorism." *International Journal of Toxicology* 22 (6): 465–471. doi:10.1177/109158180302200607.

Sankary, Nathan, and Avi Ostfeld. 2019. "Bayesian Localization of Water Distribution System Contamination Intrusion Events Using Inline Mobile Sensor Data." *Journal of Water Resources Planning and Management* 145 (8): 04019029. doi:10.1061/(asce)wr.1943-5452.0001086.

Schwartz, Rafi, Ori Lahav, and Avi Ostfeld. 2014. "Integrated Hydraulic and Organophosphate Pesticide Injection Simulations for Enhancing Event Detection in Water Distribution Systems." *Water Research* 63: 271–284. doi:10.1016/j.watres.2014.06.030.

Seth, Arpan, Katherine A. Klise, John D. Siirola, Terranna Haxton, and Carl D. Laird. 2016. "Testing Contamination Source Identification Methods for Water Distribution Networks." *Journal of Water Resources Planning and Management* 142 (4): 1–11. doi:10.1061/(ASCE)WR.1943-5452.0000619.

Seyoum, A. G., & Tanyimboh, T. T. (2014). Pressure-dependent network water quality modelling. *Proceedings of the Institution of Civil Engineers - Water Management* 167(6), 342–355. doi:10.1680/wama.12.00118

Seyoum, A. G., & Tanyimboh, T. T. (2016). Investigation into the Pressure-Driven Extension of the EPANET Hydraulic Simulation Model for Water Distribution Systems. *Water Resources Management* 30(14), 5351–5367. doi:10.1007/s11269-016-1492-6.

Seyoum, Alemtsehay G., and Tiku T. Tanyimboh. 2017. "Integration of Hydraulic and Water Quality Modelling in Distribution Networks: EPANET-PMX." *Water Resources Management* 31 (14): 4485–4503. doi:10.1007/s11269-017-1760-0.

Shafiee, M. Ehsan, and Emily Zechman Berglund. 2017. "Complex Adaptive Systems Framework to Simulate the Performance of Hydrant Flushing Rules and Broadcasts during a Water Distribution System Contamination Event." *Journal of Water Resources Planning and Management* 143 (4): 04017001. doi:10.1061/(ASCE)WR.1943-5452.0000744.

Shang, Feng, James G. Uber, and Lewis A. Rossman. 2008. "Modeling Reaction and Transport of Multiple Species in Water Distribution Systems." *Environmental Science and Technology* 42 (3): 808–814. doi:10.1021/es072011z.

Siaterlis, Christos, Andres Perez Garcia, and Bela Genge. 2013. "On the Use of Emulab Testbeds for Scientifically Rigorous Experiments." *IEEE Communications Surveys and Tutorials* 15 (2): 929–942. doi:10.1109/SURV.2012.0601112.00185.

Siaterlis, Christos, Béla Genge, and Marc Hohenadel. 2013. "EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation." *IEEE Transactions on Emerging Topics in Computing* 1 (2): 319–330. doi:10.1109/TETC.2013.2287188.

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." *Environmental Modelling & Software* 112 (May 2018): 46–51. doi:10.1016/j.envsoft.2018.11.008.

Taormina, Riccardo, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, and Avi Ostfeld. 2017. "Characterizing Cyber-Physical Attacks on Water Distribution Systems." *Journal of Water Resources Planning and Management* 143 (5): 04017009. doi:10.1061/(ASCE)WR.1943-5452.0000749.

Tsoukalas, Ioannis, Panagiotis Kossieris, and Christos Makropoulos. 2020. "Simulation of Non-Gaussian Correlated Random Variables, Stochastic Processes and Random Fields: Introducing the AnySim R-Package for Environmental Applications and Beyond." *Water* 12 (6): 1645. doi:10.3390/w12061645.

Tuptuk, Nilufer, Peter Hazell, Jeremy Watson, and Stephen Hailes. 2021. "A Systematic Review of the State of Cyber-Security in Water Systems." *Water* 13 (1): 81. doi:10.3390/w13010081.

Watson, Jean Paul, Harvey J. Greenberg, and William E. Hart. 2004. "A Multiple-Objective Analysis of Sensor Placement Optimization in Water Networks." In *Proceedings of the 2004 World Water and Environmetal Resources Congress: Critical Transitions in Water and Environmetal Resources Management*, 4609–4618. doi:10.1061/40737(2004)456.

Xing, Lu, and Lina Sela. 2020. "An Overview of the Transient Simulation in Water Distribution Networks (Tsnet)." In *World Environmental and Water Resources Congress 2020*, 282–289. Reston, VA: American Society of Civil Engineers. doi:10.1061/9780784482971.028.

Zechman, Emily M., and S. Ranji Ranjithan. 2009. "Evolutionary Computation-Based Methods for Characterizing Contaminant Sources in a Water Distribution System." *Journal of Water Resources Planning and Management* 135 (5): 334–343. doi:10.1061/(ASCE)0733-9496(2009)135:5(334).