State-of-the-Art Review

Review of Modeling Methodologies for Managing Water Distribution Security

Emily Zechman Berglund, Ph.D., M.ASCE1; Jorge E. Pesantez, S.M.ASCE2; Amin Rasekh, Ph.D.3; M. Ehsan Shafiee, Ph.D.4; Lina Sela, Ph.D., M.ASCE5; and Terranna Haxton, Ph.D., M.ASCE6

Abstract: Water distribution systems are vulnerable to hazards that threaten water delivery, water quality, and physical and cybernetic infrastructure. Water utilities and managers are responsible for assessing and preparing for these hazards, and researchers have developed a range of computational frameworks to explore and identify strategies for what-if scenarios. This manuscript conducts a review of the literature to report on the state of the art in modeling methodologies that have been developed to support the security of water distribution systems. First, the major activities outlined in the emergency management framework are reviewed; the activities include risk assessment, mitigation, emergency preparedness, response, and recovery. Simulation approaches and prototype software tools are reviewed that have been developed by government agencies and researchers for assessing and mitigating four threat modes, including contamination events, physical destruction, interconnected infrastructure cascading failures, and cybernetic attacks. Modeling tools are mapped to emergency management activities, and an analysis of the research is conducted to group studies based on methodologies that are used and developed to support emergency management activities. Recommendations are made for research needs that will contribute to the enhancement of the security of water distribution systems. DOI: 10.1061/(ASCE)WR.1943-5452.0001265. © 2020 American Society of Civil Engineers.

Introduction

Water utilities should deliver water at expected levels of quality, quantity, and pressure, yet water distribution systems (WDSs) are vulnerable to a range of intentional and unintentional threats. Malicious attacks on water distribution systems may release protozoans, bacteria, and toxic chemicals into community WDSs (Kroll and Throckmorton 2005; Janke et al. 2014); disrupt operations through cyberattacks (Rasekh et al. 2016; Ashford 2018); or damage infrastructure through sabotage and vandalism (Winter 2015). Unintentional incidents, such as natural disasters, infrastructure aging, and accidents, can release contaminants (Grigg 2003; Hruday and Hruday 2004; National Research Council 2006; Janke et al. 2014; World Health Organization 2017), break pipes over a widespread area (Kuruoka and Rainer 2010), or create cascading failures in interconnected infrastructure systems, in which damaged power infrastructure causes equipment failure at pump stations and treatment facilities (Wang et al. 2012).

To address the vulnerabilities associated with water distribution, a number of presidential directives, general homeland security laws, and environmental laws have tasked water utilities with recognizing and reducing risks to water infrastructure (US Dept. of Homeland Security and USEPA 2015; US Congress 2018). In response, a wide range of research efforts have been conducted to support emergency management for water distribution infrastructure. Studies have focused largely on risk assessment and risk management, answering research questions, such as “What can go wrong?” and “What can be done?” (Ezell et al. 2000). The use of simulation modeling has been used extensively in creating knowledge about WDS management and security (Janke et al. 2014; Mala-Jetmarova et al. 2018). This is because simulation modeling provides capabilities to explore a wide range of hazards and what-if scenarios for threat events, for which physical experiments are impossible and data are sparse. The nature of worst-case events means that some events, such as intentional attacks, occur with low frequency, and few have been observed and recorded. For events in which natural hazards and accidental intrusion affect water quality, information about the dynamics of an event are rarely available, and at most, community-level impacts are documented (Hruday and Hruday 2004). The scarcity of data is exacerbated by the needs of water utilities to protect their data as part of managing their security. Because of this lack of data, the research community has built up a large body of work around the development of computational modeling tools and frameworks that can provide insight into the potential impacts of hazards and best practices for managing those events. The goal of this manuscript is to provide a comprehensive review of the modeling frameworks that have been developed to assist in the management of emergencies and WDS security. This manuscript provides a review of 263 journal papers, conference proceedings, and technical reports (see Table 1 for major venues). Studies that are reviewed in what follows develop modeling frameworks to assess risk, design early warning systems, detect events, plan mitigation and response actions, and...
Emergency Management Activities

Emergency management frames the practices for managing water distribution security threats as a set of activities to identify and mitigate threats and improve system resilience through response and recovery (Lindell et al. 2007).

Risk assessment, or hazard vulnerability analysis, is conducted to identify the hazards to which a community is exposed, estimate the probability of occurrence of events, and determine the consequences of those events. The following questions should be answered as part of risk assessment (Kaplan 1997; Ezell et al. 2000; Kanakoudis and Tsitsifli 2017): What can go wrong? What is the likelihood that it will go wrong? What are the consequences? The outcome of risk assessment is to rank or select events that require the action of management strategies. In the context of WDS infrastructure, risk assessment can be used to identify system components, such as nodes, pipes, tanks, pumps, sensors, controllers, and communication links that are susceptible to malicious attack or natural hazards and should be protected to improve system security. Example activities for each threat type are provided in Table 3.

Mitigation is a long-term, permanent activity to reduce the actual or potential consequences of a hazardous event. Mitigation actions may focus on the source of the hazard and seek to control it. Mitigation may alternatively focus on the receiving area and seek to limit the impact of the hazard on specific geographic areas or population sectors, reduce the level of urban development in hazard-prone areas, or harden infrastructure against a hazard. For flooding hazards, for example, dams and levees reduce the risk of floods, warning systems enable preventive actions, and limiting development in the floodplain reduces exposure. For WDS security, examples of mitigation actions, as shown in Table 3, include hardening infrastructure components through the use of countermeasures and placing early warning systems to detect contamination or cybernetic attacks.

Because mitigation cannot control all hazards, preparedness activities are taken to reduce the consequences of hazards that do occur. Preimpact activities establish preparedness, or a state of

Table 1. Top literature sources reviewed

<table>
<thead>
<tr>
<th>Title</th>
<th>No. of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal of Water Resources Planning and Management</td>
<td>78</td>
</tr>
<tr>
<td>Water Research</td>
<td>14</td>
</tr>
<tr>
<td>Journal of Hydroinformatics</td>
<td>9</td>
</tr>
<tr>
<td>Environmental Modeling &amp; Software</td>
<td>7</td>
</tr>
<tr>
<td>Journal of Infrastructure Systems</td>
<td>4</td>
</tr>
<tr>
<td>Water Resources Management</td>
<td>4</td>
</tr>
<tr>
<td>Computers and Chemical Engineering</td>
<td>4</td>
</tr>
<tr>
<td>Other journals</td>
<td>84</td>
</tr>
<tr>
<td>Conference proceedings</td>
<td>51</td>
</tr>
<tr>
<td>Technical reports</td>
<td>8</td>
</tr>
</tbody>
</table>

Note: C = contamination; P = physical; II = interconnected infrastructure; and Cy = cybernetic infrastructure.

Table 2. Modeling tools for emergency management of water distribution systems

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
<th>Threat type</th>
<th>Hydraulic simulation</th>
<th>Risk assessment</th>
<th>Mitigation</th>
<th>Response and recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPANET</td>
<td>Hydraulic and quality modeling</td>
<td>C, P</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>EPANET-MSX</td>
<td>Multispecies modeling</td>
<td>C</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>EPANET-RTX</td>
<td>Integration with SCADA</td>
<td>C</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>TEVA-SPOT</td>
<td>Contamination simulation and sensor placement</td>
<td>C</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td>WST</td>
<td>Response actions to contamination</td>
<td>C</td>
<td>✓</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CANARY</td>
<td>Event detection</td>
<td>C</td>
<td>—</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WNTR</td>
<td>Disaster events and network resilience</td>
<td>P, II</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Giraffe</td>
<td>Disaster events and network resilience</td>
<td>P, II</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>REVAS.NET</td>
<td>Disaster events and network resilience</td>
<td>P, II</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>epanetCPA</td>
<td>Cyber-physical attacks</td>
<td>Cy, II</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

Note: C = contamination; P = physical; II = interconnected infrastructure; and Cy = cybernetic infrastructure.
readiness, for a community through planning, training, equipping, and exercising emergency responders and special facilities. Preparedness activities identify and acquire the facilities, equipment, and materials needed for responding to an emergency. These resources may include, for example, emergency operations centers, detection systems, siren systems, traffic barricades, and chemical detection kits. Personnel should be trained and drilled to respond, and plans for response should be tested through emergency exercises. For example, water utilities can conduct tabletop exercises (Moyer 2005), in which emergency scenarios are developed to present staff and emergency response officials with fabricated events. A preparedness plan that is developed and tested through these activities gives specific instructions about the chain of command during emergencies, delineates procedures for reacting to events, and centralizes important management and operation procedures in one location. To assist water utilities in their response to emergencies, FEMA developed the Homeland Security Exercise and Evaluation Program (US Department of Homeland Security 2013), which provides protocols for executing for tabletop exercise programs.

Emergency response activities begin once an event is detected and continue as the situation evolves. Response activities have four functions: emergency assessment, hazard operations, population protection, and incident management (Lindell et al. 2007). Emergency assessment actions provide an assessment of the extent or impact of the hazard and are intended to generate intelligence about the behavior of the hazard and the affected people and property. Emergency assessment activities include threat detection, emergency classification, hazard and environmental monitoring, population monitoring and assessment, and damage assessment. Hazard operations have the same purpose as mitigation actions but are differentiated by their time of implementation. Whereas mitigation actions are implemented preimpact and provide passive protection, hazard operations are implemented rapidly when the need arises. Hazard operations can be preventive and avoid a release of a hazard to the environment, and they are corrective if they act to reduce the magnitude or terminate a release. For example, hazard operations include flushing a contaminant through manipulating hydrants and isolating a contaminant by closing valves or pressurizing a subsection of the network (Table 3). Population protection actions prevent people from being exposed to hazards through activities such as evacuation and warning the affected population. Orders to boil water are an example of population protection (Table 3). Finally, incident management focuses on the management required to execute emergency response by organizing across multiple

Table 3. Emergency management activities for WDS security that have been evaluated through the use of modeling frameworks, as reviewed here

<table>
<thead>
<tr>
<th>Emergency management activity</th>
<th>Contamination threats</th>
<th>Physical threats</th>
<th>Interconnected infrastructure threats</th>
<th>Cybernetic threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>• Rank vulnerable nodes</td>
<td>• Assess network serviceability for threat scenarios</td>
<td>• Assess network serviceability for threat scenarios</td>
<td>• Characterize potential attack scenarios</td>
</tr>
<tr>
<td></td>
<td>• Conduct QMRA</td>
<td>• Identify vulnerable infrastructure assets</td>
<td></td>
<td>• Conduct modified contingency analysis</td>
</tr>
<tr>
<td></td>
<td>• Develop design basis threats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigation</td>
<td>• Implement countermeasures</td>
<td>• Install backup power sources</td>
<td>• Install temporary bypass pipes</td>
<td>• Design redundancy, diversity, and hardening in cyber networks</td>
</tr>
<tr>
<td></td>
<td>• Install water quality sensors</td>
<td>• Harden electrical substations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Design network sectors for isolation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Install chlorine boosters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Maintain disinfectant residuals</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Control valves and pumps for pressure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Response</td>
<td>• Event detection</td>
<td>• Open emergency storage reservoirs</td>
<td>• Change WDS operations</td>
<td>• Event detection</td>
</tr>
<tr>
<td></td>
<td>• Source identification</td>
<td>• Isolate or pressurize network sectors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Adaptive sampling</td>
<td>• Ration water or prioritize nodes for continued service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Flush hydrants</td>
<td>• Install temporary bypass pipes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Warn consumers to change water use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Isolate network sectors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Boost disinfection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td>• None identified</td>
<td>• Schedule and allocate crews for repairs</td>
<td>• Restore power system elements</td>
<td>• None identified</td>
</tr>
</tbody>
</table>


QMRA = quantitative microbial risk assessment.
Contamination Threats

Hazardous chemical and biological agents can threaten public health in the event of exposure through drinking water (National Research Council 2006; Janke et al. 2014). Chemical contaminants include organic chemicals such as benzene, polychlorinated biphenyls, and pesticides; inorganic chemicals such as arsenic and nitrates; and radioactive compounds. For example, an insecticide, chlordane, was intentionally released into the Pittsburgh water system in 1980 (Welter et al. 2009), and in 2014, organic chemicals (primarily 4-methylecyclohexanemethanol) spilled into the Elk River, which serves as the water supply for Charleston, West Virginia (Schade et al. 2015). Enteric microbial pathogens, such as noroviruses, *Escherichia coli* O157:H7, and *Cryptosporidium*, may be introduced through contact of source water or infrastructure components with human or animal feces. Aquatic microorganisms, including nontuberculous mycobacteria, *Legionella*, and toxins from aquatic microorganisms exist in natural waters and may bypass treatment facilities. For example, in Gideon, Missouri, an unintentional outbreak of *Salmonella typhimurium* caused illnesses and deaths when the hatches on the city’s largest water tank deteriorated, leaving the surface of the water open to contamination by bird droppings (Clark et al. 1996). Another example is when members of a religious cult cultured a highly toxic bacterium in their own laboratory to intentionally contaminate the water supply for The Dalles, Oregon, causing a salmonellosis outbreak (Janke et al. 2014). Microbial intrusion may also be introduced through pressure transient events. In these events, an abrupt change in the velocity of water can be caused by valve closure, pipe fracture, or shutting off of pumps, leading to low or negative pressures in the network. Microbial pathogens can infiltrate the system if three conditions are met: the system loses pressure, pathogens are present at WDS pipes through contaminated groundwater or flows from leaking sewers, and pipe integrity is compromised through deterioration or breaks (Besner et al. 2011; Viñas et al. 2019).

The sections that follow describe modeling studies that support emergency management activities to identify and reduce risk of WDS contamination by biological and chemical agents. The distribution of contamination threat studies across emergency management activities is shown in Fig. 3. Many of the studies described in what follows use the EPANET toolkit (Rossman 2000) (Table 2), which solves equations representing hydraulic flows and includes several generic fate methods (e.g., first-order bulk decay, exponential growth to a limiting value, and conservative substances). A few studies that did not use EPANET used hydraulic calculations developed in-house. EPANET-MSX was developed to simulate the interaction of multiple species (e.g., contaminants with disinfectants and disinfection byproducts) in the system (Shang et al. 2008a, b) (Table 2). This enables a more realistic estimation of the consequences of a contamination incident.

Risk Assessment

A few risk assessment studies calculated the outcome of contamination events based on contaminant concentration in the WDS, where risk is calculated as a characteristic of the infrastructure. A set of studies defined hazardous nodes as those nodes that deliver contaminant to other nodes when breached and vulnerable nodes as nodes that receive contaminant when it is injected at upstream nodes (Xin et al. 2012; Mansour-Rezaei et al. 2013, 2014). These studies applied hydraulic modeling to simulate a range of contamination events and identify the most hazardous and vulnerable junctions in a WDS.
Other risk assessment studies quantified the risk of a population to exposure due to a contaminated WDS. Fifteen studies were found that adopted the procedure developed through quantitative microbial risk assessment (QMRA), which uses explicit quantification of model inputs and health impacts (Pettersson and Ashbolt 2016). QMRA requires four components of the exposure pathway: the pathogen loading in the water source, which may or may not be reduced by mitigation; exposure or pathogen dose due to water consumption behaviors; a dose-response relationship to quantify the probability of infection; and the exposure frequency (Pettersson and Ashbolt 2016). Besner et al. (2011) developed a conceptual model to conduct QMRA for low-pressure events that allow the intrusion of microbes into a water network. QMRA was applied for pressure transients using probabilistic representations of each component of the exposure pathway (Gibson et al. 2019). This work uses a probabilistic approach without the use of hydraulic simulation and quantifies changes in the risk of infection to *Giardia, Cryptosporidium*, and rotavirus with aging pipes. Flow patterns in the network and chemical reactions of contaminants with the constituents in the bulk water and at the pipe wall create nonuniform exposure across a population; however, Besner et al. (2011) and McInnis (2007) simulated a low-pressure event using EPANET to model the transport, dilution, and die-off of microorganisms within a QMRA framework. Other QMRA frameworks coupled EPANET-MSX with Monte Carlo simulation to capture the complexities of pathogen reactions with disinfectants and the effects on exposure (Propato and Uber 2004; Tennis et al. 2010; Yang et al. 2011).

When calculating the exposure of a population, the behaviors of individual consumers can affect the exposure frequency and dose. Research has improved the representation of these behaviors in quantitative risk assessments for both chemical and biological incidents. Van Abel et al. (2014) coupled EPANET and the SIMulation of water Demand and End-Use Model (SIMDEUM) to model a short-term contamination event where sewage is pumped into the system and evaluate the risk of exposure to *Campylobacter jejuni*. This study evaluates assumptions about the number of ingestion events per day and their effect on risk assessments. Other studies evaluated population exposure through ingestion (Davis and Janke 2008; Davis et al. 2014) and inhalation (Davis et al. 2016) and evaluated the effects of ingestion timing and volume, showering frequency and duration, and humidifier use on health outcomes. Further, the sensitivity of consequences was tested for event characteristics, population distribution, ingestion patterns, and exposure thresholds through the simulation of exposures across a range of events for 12 realistic systems (Davis et al. 2010; Davis and Janke 2011; Davis et al. 2014). Results show that the spatial extent of consequences depends on the interactions between the dose level required for adverse effects and the population density near the injection site. Another simulation study found that uncertainty in model parameters affect predictions of plume propagation, and contamination source location can have the greatest effect on the uncertainty in the number of exposed persons (Hart et al. 2019). In addition to consumption and exposure, other behaviors that can affect exposure during a contamination event are travel within a network, communication within social networks about the water event, and reduction of water uses. A sociotechnical simulation framework was developed that tightly couples agent-based modeling with EPANET to capture feedback to the water network when consumers stop consuming water after having become sick (Zechman 2011; Shafiee and Zechman 2013).

Another set of risk assessment studies focused on characterizing likely scenarios and assessing risk associated with these scenarios. A cross-entropy approach was coupled with EPANET to sample characteristics of contamination scenarios for extreme events (Perelman and Ostfeld 2010b, 2012). Rasekh and Brumbelow (2013) created probability distributions for contamination event scenarios and used Monte Carlo simulation to generate probabilistic distributions of human exposure. They coupled EPANET with a genetic algorithm approach to identify critical scenarios, or design-basis threats. Instead of using the product of probability and consequence to represent risk, they explored tradeoffs between the two risk factors using the nondominated sorting genetic algorithm II (NSGA-II). Rasekh et al. (2013) built on the agent-based modeling framework to identify design-basis threats and reassess system risk as it is affected by the behaviors, interactions, and adaptations of consumers.

**Mitigation**

Research in mitigation focuses on reducing the likelihood of the occurrence of contamination events or the magnitude of consequences. Modeling frameworks are described in what follows based on their contribution to designing sensor networks, mitigating pressure transients, and mitigating intentional attack by placing countermeasures.

**Designing Sensor Networks**

Online water quality sensors that are placed strategically in a WDS can be used to detect the occurrence of a contamination event. Online sensors can generate an informative data set in short time increments about the location of a contaminant over a wide geographical area, and some water quality parameters can be monitored at relatively low expense. Sensor placement is a significant mitigation activity since placing an early warning system is critical to identifying that water quality has been compromised. Contamination early warning systems can integrate data from various sources (e.g., online sensors, surveillance cameras, customer complaints
centers, and routine sampling and inspection programs), perform expert-based and analytical-based analyses of information, and raise appropriate alarms to facilitate a response. An early warning system contributes to preparedness and enables response. Because it entails preimpact installation and maintenance of a sensor network, it is classified as a mitigation activity.

The sensor placement problem can be generally stated as follows: given a limited number of sensors, find the optimal sensor locations such that some performance and impact measures are optimized. The sensor placement problem has been widely studied in connection with detecting contamination events, as evident from the many papers reviewed herein (Figs. 2 and 3) and previously published reviews (Hart and Murray 2010; Rathi and Gupta 2014; Hu et al. 2018), starting from early warning event detection systems (Lee and Deininger 1992; Kessler et al. 1998) to the more recent applications for sensor placement (Zhao et al. 2016; Sela and Amin 2018). Because this research has been reviewed by others in previously published reviews, the following discussion does not explicitly list every paper described in those reviews. Related papers that are not described in the following discussion are included in an analysis of trends presented in figures and tables. The complete list of references that is used to create figures and tables is provided in the supplementary data file.

The underlying process of determining the optimal sensor locations involves three stages: (1) modeling and simulation, (2) solution approach and methods, and (3) testing and validation. Modeling and simulation involve specifying the WDS model (e.g., steady or extended period simulation), contamination dynamics (e.g., single- or multispecies analysis), and sensing model (e.g., perfect or imperfect readings). There is no consensus on what should be the appropriate design conditions for the contamination incidence, and the majority of prior works followed the guidelines established in the Battle of Water Sensor Networks (BWSN) (Ostfeld et al. 2009), relying on Monte Carlo sampling to generate potential contamination events and relying on well-calibrated hydraulic models for extended-period simulations. Three distinct solution approaches to solving the sensor placement problem are found in the literature: engineering principles and expert opinion (e.g., Chang et al. 2011), distance-connectivity network-based decision-making (e.g., Diao and Rauch 2013), and model-driven optimization (e.g., Ostfeld and Salomons 2004). While the majority of researchers have considered minimizing the average impact of contamination scenarios, including detection likelihood, time to detection, volume of contaminated water, and affected population, additional performance measures that reduce the impact of high-impact contamination events have been suggested including value at risk, tail-conditional expectation, and worst-case events (Rasekh and Brumbelow 2013; Watson et al. 2009; Perelman and Ostfeld 2010a). Mixed-integer optimization (e.g., Berry et al. 2006; Propato 2006), greedy approximation (e.g., Krause and Guestrin 2009; Sela and Amin 2018), evolutionary algorithms (e.g., Ostfeld and Salomons 2005; Eliades and Polycarpou 2010), and heuristic approaches (e.g., Dorini et al. 2006; Rathi et al. 2016) have been developed specifically for the sensor placement problem using a combination of optimization methods.

Notably, advances in modern optimization solvers and hardware speedup have enabled the consideration of more realistic assumptions, such as imperfect sensors (e.g., Berry et al. 2009), data uncertainties (e.g., Carr et al. 2006), and high-consequence contamination events (e.g., Watson et al. 2009). Despite the extensive literature, the application of continuous monitoring of water quality within WDSs has been extremely limited in practice owing to the high level of investment required, operation and management costs, and low level of reliability of the generated data (Aisopou et al. 2012).

**Mitigating Pressure Transient Events**

Pressure transient events, which allow microbial intrusion, can be mitigated by controlling pressures and maintaining disinfectant residuals. EPANET is used to simulate the intrusion of contaminants during a pump shut-down operation and evaluate the effects of closing valves in the network and adding a flywheel at a pump motor to cause it to slow down gradually (McInnis 2007). Yang et al. (2011) builds on the framework demonstrated by Propato and Uber (2004) that couples EPANET-MSX with Monte Carlo simulation. The framework is applied to test the effect of maintaining disinfectant residuals in the network to reduce the risk of exposure to norovirus.

**Mitigating Intentional Attacks by Placing Countermeasures**

Intentional attacks that introduce contaminants to a WDS can be mitigated through the use of countermeasures. Skolicki et al. (2008) develop a coevolutionary computation modeling framework to develop strategies for implementing countermeasures. An evolutionary computation-based approach is coupled with EPANET to evolve the decisions of defenders in selecting hydrants to guard and the decisions of attackers in selecting hydrants as locations for injecting contaminant. Actors learn improved strategies over many iterations of an evolutionary algorithm. An agent-based modeling framework, also coupled with EPANET, extends this work to simulate attackers and defenders as agents (Monroe et al. 2018). Attacker agents use multattribute theory to select nodes to inject a contaminant, and defender agents implement countermeasures, including security equipment and security personnel, at critical nodes.

**Response**

Response activities can be grouped as emergency assessment, hazard operations, population protection, and incident management, as described by Lindell et al. (2007). Emergency assessment models focus on event detection, source identification, and adaptive deployment of sensors. Hazard operations and population protection are supported through modeling studies that simulate and optimize hydrant flushing, valve closure, disinfectant boosts, and consumer warning systems.

**Emergency Assessment: Event Detection**

Data from online water quality observations can be analyzed to detect events, but several challenges limit this approach (Spence et al. 2013). Sensors are needed to observe parameters that experience changes when a meaningful event occurs, because it is not realistic to expect a sensor to detect any contaminant that can be introduced into a water system. Parameters that are used to detect events should also be readily and cheaply monitored. For example, common water quality parameters, including chlorine residual, alkaline, pH, turbidity, total organic carbon, oxidation reduction potential, UV254, nitrate-nitrogen, phosphate, and specific conductance, can be monitored using off-the-shelf commercial sensors, and laboratory experiments found that these parameters can be sensed to detect pesticides, heavy metals, and other chemical and biological contaminants (Byer and Carlson 2005; Hall et al. 2007; Liu et al. 2014). Building on this knowledge, modeling studies have identified the signature of changes in water quality parameters that can be used to detect the presence of contaminants. Chlorine is easily and routinely monitored, and EPANET-MSX simulations are developed to explore the use of chlorine sensors for event detection by simulating the interaction of chlorine with pesticides.
(Schwartz et al. 2014) and microbial contaminants (Helbling and VanBriesen 2009). Yang et al. (2008) tested the response of chlorine to nonreactive sodium fluoride and reactive pesticide aldicarb within a lab-scale drinking water pipe network and developed a convection dispersion reaction model to simulate interactions.

Once a set of parameters has been identified for monitoring, an event detection algorithm should positively identify anomalies in water quality time series that are caused by contamination. Event detection algorithms have been developed to detect contamination events in streaming data from multiple water quality sensors. An artificial neural network has been constructed for a measured parameter to estimate the target parameter in the next time step, and a set of detection rules is applied to determine whether an observation is an outlier or an expected value (Perelman et al. 2012; Arad et al. 2013). Other multivariate detection algorithms have been developed using support vector machine models (Oliker and Ostfeld 2014a) and an unsupervised classifier (Oliker and Ostfeld 2014b) to detect events. Other methods fuse readings among water quality sensors to detect events using a logit discrete model (Housh and Ostfeld 2015), calculation of Pearson correlation coefficients (Liu et al. 2015b), a multisensor data fusion model based on time series prediction and Dempster-Shafer evidence theory (Hou et al. 2013), a pattern-matching application using artificial neural networks (Mounce et al. 2014), and data-mining and clustering techniques (Raciti et al. 2012). The CANARY event detection algorithm (Table 2) uses signal-processing and statistical tools to analyze real-time water quality sensor data and identify anomalies within a WDS (USEPA 2012). Multivariate models report increased accuracy and detection ratios compared with univariate models (Arad et al. 2013).

One challenge associated with developing and using event detection algorithms is the process of defining a baseline (Spence et al. 2013). Dynamic threshold models update the threshold for detecting anomalies based on the current and recent state of water quality parameters (Arad et al. 2013; Oliker et al. 2016; Williamson et al. 2014). Eliades et al. (2015) developed a model with multilevel thresholds to accommodate for the natural fluctuations in water quality parameters due to factors such as demand variability.

Event detection methods are susceptible to false positives, and the chances of receiving false alarms increase significantly as the number of sensors in a network increases. Liu et al. (2015a) explored the tradeoffs in false negatives and false positives in training a simple rule-based event detection algorithm through the use of NSGA-II. While most event detection methods are based on a single sensor, multispecies, multisensor simulation models have been developed to reduce false positives by exploiting spatial data. A data fusion model reduces the number of false alarms by at least three orders of magnitude by considering the spatiotemporal characteristics of contamination events (Koch and McKenna 2010). Murray et al. (2012) used a Bayesian belief network model to process data from multiple water quality sensors to address the issue of false positives. Many signal-processing event detection algorithms do not account for operational data signals, such as tank levels, pressures, and pumps status. A Monte Carlo simulation-based approach was developed that computes the bounds of expected chlorine concentrations by running multiple randomized simulations using EPANET-MSX, and an event detection algorithm was created to determine whether the concentration is outside of the expected bounds (Eliades et al. 2014). A data-driven model (Oliker and Ostfeld 2014b) was coupled with a simulation-based model to improve the detection of water quality events (Oliker and Ostfeld 2015; Oliker et al. 2016). Housh and Ohar (2017) extended existing models to include hydraulic characteristics in event detection, and results demonstrated that including pressure, flow, and velocities improved detection performance for two benchmark WDSs. The hydraulic model in this study was used to confirm the consistency of outputs of a data-driven model and was not tightly coupled with the data-driven model.

**Emergency Assessment: Adaptive Sampling**

In response to perceived or actual contamination events, a utility may seek to obtain additional information about the event to improve response actions. Additional information can be obtained through collecting grab samples and releasing mobile sensors to enhance the resolution and accuracy of the observations from an existing sparse network of fixed sensors. During the 2010 water emergency, for example, hundreds of samples of water were taken by the Massachusetts Water Resources Authority to guide their response and decisions about the extent and duration of the order (Daley and Gil 2010; LCRA Water Quality Advisory Committee 2019). This sampling and reporting is required by law in some states (Massachusetts Water Resources Authority 2010; Weber and McGillichy 2018).

A key research question associated with adaptive sampling concerns the best location in a network to gather additional measurements. Eliades and Polycarpou (2012) use a decision tree approach to determine a sequence of nodes that should be sampled in a network. Wang and Harrison (2013a) use a Markov chain Monte Carlo approach to release mobile sensors to strategically maximize the reduction in source uncertainty. Perelman and Ostfeld (2013b) explored the benefits of augmenting fixed sensors for event detection with mobile sensors. Mobile sensors are assumed to be carried by the flow traversing the network and collecting hydraulic and water quality measurements. A cross-entropy heuristic optimization approach was implemented to find the optimal location and time to release mobile sensors in a WDS to improve detection likelihood and time to detection. Although initial results demonstrated the benefit of using mobile sensors to increase detection likelihood and reduce expected time to detection, the researchers also found that similar benefits may be achieved by adding extra fixed sensors. Suresh et al. (2015) presented a comprehensive architectural design, algorithms, and communication protocols for optimal WDS surveying with mobile sensor networks. Gong et al. (2016) proposed a mixed-integer nonlinear programming framework for mobile sensor operation to optimize the sensors’ leak and backflow detection and localization performance. To support these and several other computational modeling efforts (Suresh et al. 2013; Oliker and Ostfeld 2016), there has been significant progress in the design and manufacture of hardware for mobile sensors [Wu 2014; Banks et al. 2014; Sankary et al. 2015; Chatzigeorgiou et al. 2016a].

**Emergency Assessment: Source Identification**

Source identification is typically posed as an inverse problem, in which the system state or water quality parameters at specified points in the network are given, and a methodology identifies model parameters and boundary conditions, which are the location, concentration, and release history of the source. The source identification algorithm seeks to minimize the error between the set of water quality observations collected at sensors and the set of water quality predictions simulated by a hydraulic model. Similar to many inverse problems, the source identification problem is ill-posed and difficult to solve. Given that sensor data are spatially sparse and the number of source variables is extremely large (the source could be introduced at any node and at any time), there exists a set of multiple nonunique solutions that solve the problem equally well or nearly equally well. The source identification problem has been solved using methods that are grouped in what
follows as nonlinear and backtracking methods, statistical modeling methods, and simulation-optimization methods.

An early study solved the source identification problem through a nonlinear programming approach that minimizes the error between calculated and target concentrations at sensors (van Bloemen Waanders et al. 2003). The optimization problem was solved using direct successive quadratic programming coupled with EPANET but posed an impractical computational burden for larger networks. In subsequent work, an origin tracking algorithm was developed to reformulate partial differential pipe equations into a set of algebraic constraints, and a simultaneous nonlinear programming approach was used to solve the new formation (Laird et al. 2005). A backtracking approach was used in a related study to identify the probability density functions of possible prior times when the observed contamination was at any up-gradient node (Neupauer et al. 2010). The method was extended to account for the effects of complex, transient WDSs with storage tanks and assess how flow paths through the storage tank dilute the information content of sensor observations in identifying source characteristics (Wagner et al. 2015). A simulation-based approach reverses hydraulic simulation results to model source nodes as demand nodes and, similarly, demand nodes as source nodes (Salomons and Ostfeld 2010). Using the reverse hydraulic model, water quality readings become sources of contamination, which can be traced back to the actual sources of contamination.

Probabilistic and statistical models determine the probability that a node was the site of contamination, based on observations at sensors. A data mining approach was developed that constructs a large database containing simulated contamination scenario characteristics to identify the source (Huang and McBean 2009). Logistic regression was demonstrated as a prescreening approach to estimate the probability that each node will be a candidate source node (Liu et al. 2011b). Approaches based on Bayesian statistics were used in several applications to assign probabilities to potential source locations and update probabilities using observed data (Dawsey et al. 2006; Wang and Harrison 2013b; Wang and Zhou 2017).

Other approaches explore simulation-optimization frameworks to solve the inverse problem of source identification. Simulation-optimization approaches provide a way to solve complex formulations of the source identification problem. These methods allow changes in flow directions due to diurnal flow patterns and search for time-varying release histories without assuming constant release concentrations. Methods were developed using model trees and linear programming (Preis and Ostfeld 2006), an impact coefficient approach (Di Cristo and Leopardi 2008), a reduced gradient method (Guan et al. 2006), and evolutionary algorithms (Preis and Ostfeld 2007; Zechman and Ranjithan 2009). Sun et al. (2019) employed a deep-learning algorithm to use consumer complaint information, rather than online water quality data, in identifying a source. Subsequent studies addressed the complexities of using source identification methods for realistic water contamination scenarios. A major limitation of source identification methods is the existence of nonunique solutions because the presence of other potential solutions undercut a decision maker’s confidence in the effectiveness of response actions. Laird et al. (2006) demonstrated the use of mathematical regularization, which is a traditional approach that can be used to address ill-posed problems. Propato et al. (2010) developed probability distributions associated with the identification of a source. Kumar et al. (2012) use a multipopulation evolution strategy search to identify a set of sources that match sensor observations equally well.

Uncertainty in demands can also create errors in the identification of sources, and methods to account for this uncertainty in source identification were developed through a Markov chain Monte Carlo implementation of Bayesian analysis (Wang and Harrison 2014) and a noisy genetic algorithm (Vankayala et al. 2009). Similarly, many source identification approaches assume that perfect sensors are placed in a network to observe precise levels of concentration for a broad class of chemical or microbial contaminants. These sensors do not exist yet, and a more realistic expectation of sensors is the detection of the presence or absence of a contaminant. Source identification methods were adapted to use only binary signals at sensors (Wagner et al. 2015; Yang and Boccelli 2013; Preis and Ostfeld 2011; Kumar et al. 2012). Research has demonstrated that, as expected, nonuniqueness in a problem solution increases with less precise information.

During the course of an event, new information may become available as sensors continue to detect contaminants. A few source identification methods have been extended to incorporate new information as it emerges. An evolutionary algorithm was used to conduct a dynamic adaptive search to identify a contaminant source using streaming data (Liu et al. 2011a), and backtracking methods were modified to update source location based on new information from binary sensors (Costa et al. 2013; De Sanctis et al. 2010).

Finally, many source identification algorithms are limited in their realistic implementation by the time required to execute them. Approaches to reduce computation time include parallel computing (Shen and McBean 2011), statistical and machine learning methods (as opposed to simulation-optimization approaches) (Perelman and Ostfeld 2013a; Liu et al. 2012a; Wang and Harrison 2013b; Wang and Zhou 2017), and approaches that use prescreening and postscreening combined with simulation-optimization (Liu et al. 2012b).

Hazard Operations

Hazard operations seek to control the sources of hazards or the receiving area to limit the impacts on sectors of the population. One hazard operation is to treat a contaminant in situ. Disinfectant can be released in a network to treat and deactivate microbial contaminants. In contrast to mitigation actions that place chlorine boosters in a network to provide continuous low-level protection (Yang et al. 2011; Propato and Uber 2004), Parks and VanBriesen (2009) examined how responding to a contamination event with disinfection boosts, as releases of disinfectant in the system, could reduce the impact of a contaminant.

A second approach to controlling contaminant transport in a network is through isolating contaminated sections. Valves can be closed to prevent contaminated water from reaching uncontaminated areas of the network. Poulin et al. (2008) developed simple heuristic rules to define isolation strategies by delineating the area of contamination and identifying adjacent pipes to close. Palleti et al. (2018) solved a graph partitioning problem to install valves that can be used to close pipes in a contamination incident. Di Nardo et al. (2013) identify district metered areas (DMAs) as an approach to designing response strategies that isolate contaminants and reduce their spread to nodes. This approach entails evaluating different designs for network sectorization based on a reduction in event consequences.

Another hazard operation involves flushing contaminated water through hydrant flows or increasing demand at terminal nodes. Baranowski and LeBoeuf (2006) coupled commonly used optimization methodologies, a first-order reliability method (FORM), and parameter estimation (PEST) with hydraulic simulation models to explore the tradeoffs between minimizing contamination concentration in the network and minimizing the excess demand needed to reduce contaminant concentration at nodes. Zechman (2011) simulated the opening of hydrants near a contaminant injection site.
and evaluated the effectiveness of the method using an agent-based modeling approach that calculates the number of consumers who are exposed. The agent-based modeling approach was coupled with evolution strategies and genetic algorithms to identify optimal hydrant flushing strategies that reduce population exposure (Zechman 2013).

Additional reduction in consequences may be achieved by strategically combining hydrant flushing strategies with valve closures. Unidirectional flushing successively isolates pipe sections and unidirectionally flushes contaminated water by closing valves and opening hydrants located at the termination of pipe sections. Unidirectional flushing was evaluated as a response by simulating the procedure using EPANET (Poulin et al. 2010). Optimization models, described in what follows, have been developed to identify a combination of valves and hydrants that minimize the spread of contamination, which can be represented as the number of nodes that are contaminated, the volume of contaminated water that is consumed, or the number of exposed individuals, for a specified intrusion event. A genetic algorithm–based approach was solved for a single-objective formulation to minimize contamination consequences (Baranowski and LeBoeuf 2008). Several studies address complexities associated with operating multiple components across a network. Operating valves and hydrants requires time and resources, which may become intractable if a large number of operations is required. For example, Baranowski and LeBoeuf (2008) evaluated loss in performance due to delays associated with confirmation of the contaminant in the network through multiple sensor triggers, identification of the contaminant in the system, location of the injection site, and operation of valve closures. Multiobjective approaches minimize both the extent of the contamination and the number of devices that should be operated in a flushing and isolation strategy (Preis and Ostfeld 2008; Alfonso et al. 2010; Rasekh and Brumbelow 2014; Bashi-Azghadi et al. 2017; Zafari et al. 2017). Alvisi et al. (2012) and Gavanelli et al. (2015) developed an optimization problem to schedule the order for operating devices based on the limitations of the travel time required to reach each point in the distribution system. Other studies have evaluated the tradeoffs between minimizing consequences and the cost or inconvenience of solutions, represented as the pipe length that is isolated (Poulin et al. 2008), service interruptions (Rasekh and Brumbelow 2014), and increases in demand required to flush the contaminant (Baranowski and LeBoeuf 2006). Finally, a few studies have shown that the demand-driven analysis approach provided by EPANET can misrepresent flows and pressures under conditions of extreme demand, and they explored the use of pressure-driven analysis to simulate hydrant flushing (Alfonso et al. 2010; Rasekh and Brumbelow 2014; Afshar and Najafi 2014; Bashi-Azghadi et al. 2017; Zafari et al. 2017).

The approaches just described assume that a specific contamination event has occurred and that the location and timing of injection are known. In an actual event, however, identifying source characteristics can be challenging, and, as described, there may be nonuniqueness in the solution, where any one of multiple events could have triggered the same set of activated sensors. Afshar and Najafi (2014) addressed the problem of nonuniqueness in developing hydrant flushing strategies. They coupled an colony optimization and EPANET with a pressure-driven analysis to minimize the regret associated with implementing hydrant flushing and valve closure strategies, which are evaluated for a set of nonunique sources leading to a similar activation of sensors. Guidorzi et al. (2009) and Shafiee and Berglund (2015) identify flushing and isolation strategies that rely on an activated sensor rather than the exact location of release and the release signature or a specific event. One dynamic optimization approach couples a specialized evolutionary algorithm and EPANET to update response operations as information about the event unfolds and the characteristics of the source become more certain through new sensor information (Rasekh and Brumbelow 2015). This approach can be used in coordination with adaptive sampling procedures and adaptive source identification approaches.

The Water Security Toolkit (WST) (Table 1) is a comprehensive planning tool that was developed to assist in the evaluation of multiple response actions to select the most beneficial consequence-management strategy. WST includes the functionality of EPANET and TEVA-SPOT and optimization methodologies to identify: (1) the best locations to place water quality sensors in a system to detect contamination, (2) locations that could be the source of contamination in the system, (3) the best hydrant locations to flush out contaminated water from the system, (4) the best locations in the system to inject chlorine to inactivate contaminants, and (5) the best grab sample locations to help identify the extent of contamination in the system (USEPA 2014; Seth et al. 2016).

### Population Protection

Population protection measures focus on warning a population or moving the population away from a hazard. A few studies developed modeling frameworks to evaluate how warning a population reduces exposure in a water contamination event. These approaches build on the agent-based modeling approach (Zechman 2011; Shafiee and Zechman 2013) to simulate how water consumers comply with advisories based on the source of information, such as peers, family, or water utility officials (Shafiee et al. 2018b). A modeling framework couples the agent-based modeling framework with evolutionary algorithm-based approaches to route siren vehicles to disseminate warnings as the plume moves through the network (Shafiee and Berglund 2016). A comprehensive model was built to compare the effectiveness of hydrant flushing and warning consumers for reducing community exposure to a contaminant (Shafiee and Berglund 2017). Rasekh and Brumbelow (2015) developed a dynamic optimization approach to explore how injecting food-grade dye into a network can be used as a warning to consumers. In this approach, the population would be expected to respond to discolored water and stop consumption for drinking and eating. A multigoal approach is applied to determine where to inject dye in a network as information about the event unfolds.

### Physical Threats

Physical threats include pipe bursts, equipment failure, malevolent destruction of system components, and natural disasters, including earthquakes, hurricanes, tornadoes, freezing temperatures, and fire. Intentional damage to infrastructure constitutes a potential attack scenario because explosive materials are readily available, and high levels of expertise are not required to cause physical destruction (Burns et al. 2002). Earthquakes also cause widespread damage to WDSs. The 1994 Northridge earthquake in California disrupted water supply for 450,000 people in the state (Grigg 2003), and the 1995 Hyogo-ken Nanbu earthquake in Japan led to a disruption in water supplies for a million people in the city of Kobe (Kuraoka and Rainer 2010).

In physical damage scenarios, serviceability is an important performance indicator and represents the ability of a damaged system to supply water. It is calculated as the ratio of the available demand to the total required demand (Adachi and Ellingwood 2008; Romero et al. 2010; Tabucchi et al. 2010; Brink et al. 2012; Yoo et al. 2016; Choi et al. 2018). Estimates of serviceability are useful to map a timeline showing which pipes are damaged and where customers are located who do not receive water.
tools have been developed to assist in calculating serviceability specifically in the context of earthquake damage (Table 2). The USEPA developed the open-source Python package WNTR (Table 2). It includes the capabilities to (1) create and modify distribution system hydraulic models, (2) assign system components to different survival and fragility curves, (3) simulate disruptive events (e.g., power outages, pipe breaks, contamination incidents, and earthquakes) to the system, (4) simulate a variety of response and repair strategies to reduce the consequences of the emergency, and (5) analyze simulation results to calculate system resilience metrics. The capabilities of EPANET are extended in WNTR to enable hydraulic simulations using pressure-dependent demands, simulations of different sized leaks/breaks through the addition of leak nodes, stopping and restarting of simulations to alter system components and operations, and additional enhancements to create a more robust distribution system model (Krizek et al. 2017a). The Graphical Iterative Response Analysis of Flow Following Earthquakes (GIRAFFE) (Tabucchi et al. 2010) and Reliability Evaluation Model for Seismic Hazard for Water Supply Network (REVAS.NET) (Yoo et al. 2016) calculate the extent of earthquake damage to water supply networks and quantify system serviceability. GIRAFFE estimates multiple realizations of the initial postearthquake damage and creates a profile of damaged pipes. This framework couples the simulation of earthquakes through a physics-based simulation of strong motion and ground deformation with a graphical analysis of flows in the network. An iterative approach is used to simulate a situation in which nodes in damaged areas with negative pressures are disconnected from the water supply source, and serviceability can be calculated. This modeling approach can be time-consuming because of the iterative process. REVAS.NET couples a hypothetical earthquake generator with a hydraulic simulator to calculate hydraulic conditions in a network immediately following an earthquake. The seismic simulation module generates stochastic seismic events with random magnitudes and locations and models seismic wave attenuation.

### Risk Assessment

One activity within risk assessment identifies vulnerable components of a WDS or ranks components based on their vulnerabilities. Tidwell et al. (2005) used Markov latent effects modeling to assess and rank the security of WDS assets for a set of attack scenarios, including contamination and physical destruction. Markov latent effects modeling provides an approach to quantify subjective factors, such as cultural and environmental factors that contribute to breaches of security, and risk is calculated as the product of the probability of attack, probability of system effectiveness, and consequences. Multiattribute utility theory was applied to rank WDS components by identifying assets that should be protected, based on vulnerability to malevolent threats and the consequences of successful attacks (Michaud and Apostolakis 2006; Patterson and Apostolakis 2007). Shuang et al. (2014) assessed the vulnerability of pipes by simulating the intentional attack and destruction of nodes in a WDS, followed by cascading failures within the WDS. Pressure-driven analysis was used to simulate the effects of broken links and pressure transients.

A few studies have quantified the serviceability of a network due to pipe breaks that result from earthquake scenarios (Selcuki and Yucemen 2000; Adachi and Ellingwood 2009; Romero et al. 2010; Yoo et al. 2016; Krizek et al. 2017b; Koc et al. 2019). For example, Shi and O’Rourke (2006) developed a comprehensive model for simulating the earthquake performance of a WDS in conjunction with the water system operated by the Los Angeles Department of Water and Power and validated it on the 1994 Northridge earthquake. These approaches couple Monte Carlo simulation with the simulation of pipe breaks and simulate loss of service using graph theory concepts or hydraulic conditions through the frameworks GIRAFFE, REVAS.NET, and WNTR described earlier. These studies report the probability distribution of serviceability due to pipe breaks and leaks that result from earthquake scenarios. Yoo et al. (2019) updated the procedures for estimating postearthquake WDS serviceability by replacing demand-driven pressure-dependent hydraulic calculations.

Design-basis threats are identified as scenarios that should be used to plan responses and mitigation. To locate high-impact failures in a system during a fire event, Kanta and Brumbelow (2013) maximized risk, defined as the product of consequences or damage and the probability of an event occurring. They used dynamic programming to search for the highest-risk scenarios and identify the most vulnerable pipes to deterioration, earthquake, and malevolent actions. Laucelli and Giustolisi (2015) used a multiobjective genetic algorithm to find a set of risky scenarios, based on the volume of unmet demands, maximum probability of occurrence, and number of failed segments. They identified worst-case scenarios of pipe failure while taking into account the existing system of isolation valves, which can reduce cascading effects among segments of a network.

### Mitigation

Mitigation policies focus on minimizing the consequences of physical hazards and possible component failures. Implementing countermeasures or hardening network components can reduce the success of intentional attacks by protecting infrastructure components. An evolutionary algorithm was coupled with EPANET to implement countermeasures at vulnerable pipes and calculate the consequences of worst-case attack scenarios (Skolicki et al. 2006, 2008). Qiao et al. (2007) use a similar approach and couple a genetic algorithm with EPANET to identify which pipes should be protected.

To mitigate natural hazards, pipes can be hardened or sized to reduce impacts. Kanta and Brumbelow (2013) selected susceptible pipes for hardening to reduce risk, which is calculated as the product of probability of failure and consequence of failure, based on the fire flow at a node. Shahandashti and Pudasaini (2019) created a simulated annealing-based optimization method to identify critical pipes that should be hardened proactively. Yoo et al. (2017) coupled a multiobjective harmony search with REVAS.NET to explore the tradeoffs between the cost of pipes and serviceability in evaluating pipe hardening strategies.

### Response

An approach to responding to physical failure is to identify strategies for continuing to provide water while the network is damaged. Genetic algorithm–based approaches were developed to select which nodes could continue to receive water when system capacity is limited by the destruction of a water source (Jeong et al. 2006; Jeong and Abraham 2006), and an extension of this work developed dynamic water rationing strategies, where alternative nodes receive water at different times during the day (Jeong and Abraham 2009).

Another response strategy to mitigate the consequences of physical damage is to isolate damaged sections of a network. A mixed-integer linear programming problem was formulated and solved to identify undamaged subnetworks that could be pressurized by manipulating valves (Turner et al. 2012). Demands are met through the reconfigured system or by trucks hauling water from pressurized...
points in the system. Mahmoud et al. (2018) specify strategies to isolate and provide water to the affected part of the network by manipulating boundary valves, resetting pressure-reducing valves, and installing temporary overland bypasses between fire hydrants. The researchers used a multiobjective optimization approach, NSGA-II, to explore the tradeoffs between negative impacts on consumers and the number of operations needed, which represents cost. Shuang et al. (2017) also explore isolation strategies in the context of attack scenarios, in which multiple pipes are destroyed through cascading failures in the water network.

Finally, new water sources may be identified and deployed if existing storage facilities are destroyed. Romero et al. (2010) apply GIRAFFE to assess system effects of opening additional reservoirs to augment flows in the system in a postearthquake scenario. A discrete event simulation framework was coupled with GIRAFFE to simulate response actions, including augmenting the existing water supply through groundwater and emergency storage reservoirs and rationing water (Brink et al. 2012).

Recovery

Recovery, rehabilitation, and restoration activities work to restore networks to pre-event levels of service. The 2019 Battle of Post-Disaster Response and Restoration formulated an optimization problem for restoring a WDS after an earthquake by allocating crews to isolate, repair, and replace visible and nonvisible damage to optimize a set of multiple objectives (Paez et al. 2018). A number of teams participated in the battle and developed approaches that used algorithms to rank or prioritize pipes (Balut et al. 2018; Balut et al. 2019; Santonastaso et al. 2018) and optimization approaches, including evolutionary optimization, engineering judgment, greedy algorithms, and heuristic approaches (Zhang et al. 2018; Deuerlein et al. 2018; Castro-Gama et al. 2018; Li et al. 2018; Sweetapple et al. 2018). Similar research used a neural network to prioritize pipes for repair (Ho et al. 2009). Klise et al. (2017b) simulated the performance of repair strategies that allocate crews to fight fires and fix pipes, tanks, and pumps. Luna et al. (2011) used discrete event simulation coupled with a graphical representation of a network to simulate the restoration process and map the return of serviceability to the system. A related study used GIRAFFE to simulate damage due to earthquakes and applied discrete event simulation to simulate recovery strategies, including inspection, rerouting, isolating, and repairing system damage (Tabucchi et al. 2010). Choi et al. (2018) simulated damage to tanks and pipes in earthquake scenarios and developed recovery strategies that allocate crews to repair prioritized pipes. Alternative strategies are evaluated for their ability to quickly restore system serviceability. One study focused on recovery as the set of tasks to restore normal modes of operation for a system (Nayak and Turnquist 2016). This framework used a simulated annealing approach to schedule the order of tasks needed to bring infrastructure components, such as destroyed pumps and pipes, back online and minimize the cost of restoration.

Interconnected Infrastructure Threats

Another set of physical threats is created not just from vulnerabilities in a water network but on the network’s dependence on other infrastructures. Loss of electricity can result in the failure of pumps, water treatment facilities, and firefighting capabilities. Negative pressures that may result can allow the intrusion of contaminants and a loss of service at nodes. The importance of interconnections on water supply serviceability was demonstrated in 2003, when a widespread power outage in the northeastern US and Canada was caused by a software bug that slowed utility response when a power line dropped into foliage (Janke et al. 2014). During the power outage, the Cleveland, Ohio, water system lost serviceability, and 500,000 people were without water for several hours (Cascos et al. 2004). The Detroit water supply system, on the other hand, was equipped with backup generators at some pumping stations, and the utility was able to maintain flows in the network. A simultaneous fire at an oil refinery, however, required the diversion of flows, and some consumers were without water supplies for more than 24 h (Klein et al. 2005). Several smaller communities that buy wholesale water from Detroit relied on stored water during the event (Cascos et al. 2004).

Natural disasters can also indirectly interrupt the serviceability of water networks when the power network is damaged. The 1994 Northridge earthquake in California caused disruptions to water delivery, water quantity, water quality, fire protection, and functionality of the Los Angeles water network (Davis et al. 2012). The causes of the damage were identified as power loss and structural collapse. The restoration effort extended for nearly 12 days to bring network performance to preimpact levels, and the water network functionality failed to reach 60% of preimpact levels 13 days after the event. Earthquakes often lead to urban fires, and water supply systems that are in a damaged state may not be able to provide the flows needed for firefighting (Kuraoka and Rainer 2010; Bristow and Brumbelow 2012). A large number of research studies have explored interconnected infrastructures and the effects of cascading failures (Ouyang 2014; Gao et al. 2014). This review includes studies that focus specifically on vulnerabilities in WDSs that are introduced by interconnected infrastructure failures.

Risk Assessment

Several studies in risk assessment focus on characterizing the interconnection between WDSs and the power system, and a set of models were developed that represent connections using graph theory concepts (e.g., Kameda 2000). Dueñas-Osorio et al. (2007) represented a water network and power network as graphs, and the interdependencies between nodes were determined based on geographic immediacy. Seismic hazards and intentional destruction of both water and electrical system nodes were simulated to assess the probability of connectivity loss for a water system through the use of fragility curves. Adachi and Ellingwood (2008) also represented water and electrical systems as graphs to calculate the serviceability of a system in an earthquake scenario. They conducted risk assessment using Monte Carlo simulation to calculate the probability of serviceability under various seismic events in which both water infrastructure and power infrastructure are damaged. Kim et al. (2007) developed a graph-based algorithm and assessed connectivity loss and service flow reduction to quantify the performance of a water network damaged by an earthquake. A few studies have sought to determine the effects of power loss on a water network using hydraulic simulation. In a comprehensive study by Javanbarg and Takada (2010), a reliability model was developed to assess the serviceability of a water network by coupling a hydraulic model with a probabilistic model and Monte Carlo simulation to measure the water loss due to leakages after the event. The model was validated for the Osaka city water network during the 1995 Kobe earthquake, and comparison of simulated and actual pressure data demonstrated that the reliability model accurately predicted the serviceability of water networks after a seismic event. Guidotti et al. (2016) used a damage evaluation model to simulate the cascading effects of power network failure on a water network and simulate losses using the emitter function in EPANET. Grolinger et al. (2011) did not specify a threat mode but coupled infrastructure domain simulators, including EPANET for a WDS,
PSCAD for power systems, and I2Sim for infrastructure interdependency, to enable mapping and information exchange between models and infrastructure domains. Pournaras et al. (2019) studied how power cascading failures could spread and coevolve in a water network using epanetCPA (Table 2) and found a strong dependency, especially for heavily loaded power networks.

Other studies have included infrastructure interconnections beyond the power system. Apostolakis and Lemon (2005) modeled gas, water, and power networks on a university campus using a graph approach and deployed a cut-set method to identify vulnerable locations for terrorist attack scenarios. The connection to fire services was explored in a study that evaluated the consequences of damage to water distribution infrastructure after an earthquake, where damage was assessed as the ability of the supply system to mitigate fires (Bristow and Brumbelow 2012). In this work, EPANET was coupled with HAZUS-MH, which calculates urban fire spread to create earthquake and fire scenarios. By simulating conflagration, the number of persons displaced due to destroyed buildings can be evaluated for different damage scenarios.

**Mitigation**

Mitigation actions for interconnected power failures focus on hardening the electrical system. Dueñas-Osorio et al. (2007) tested mitigation actions that modified an electrical system by adding bypass lines at congested nodes and hardening electrical substations. Nodes in the electrical system are ranked and selected for mitigation based on their ability to maintain interdependent network performance. Mitigation was also simulated as strategies that use backup power (Adachi and Ellingwood 2008) and redundancy in the power system (Kameda 2000) to improve the expected serviceability of pump stations and nodes. Zhang et al. (2016) used numerical simulation to model cascading failures in interdependent power-water networks and to explore power system topologies that reduce failure.

Mitigation actions for interconnections between firefighting, power, and water distribution were explored (Bristow and Brumbelow 2012). Using a coupled hydraulic and urban fire spread model, mitigation actions, such as pipe replacement and increasing tank storage, are evaluated to improve the response of water distribution infrastructure after an earthquake and urban conflagration. Coar et al. (2019) investigated the effects of water network design, seismic hazard, and electric network dependency on WDS post-earthquake fire suppression capability and showed that ignoring the dependencies may lead to unconservative predictions of available water pressure. Shypanski et al. (2011) modeled the interdependency of steam plants and municipal water supplies during winter operations and used this model to design mitigation measures.

**Response**

One approach to responding to cascading failures is to change operations in the WDS to continue to supply water during power outages. A genetic algorithm was coupled with EPANET to identify pump and valve operations (Khatavkar and Mays 2018, 2019).

**Recovery**

Guidotti et al. (2016) adopted a recovery model based on American Lifelines Alliance guidelines (American Lifelines Alliance 2001), which are implemented in the HAZUS-MH model (FEMA 2003). Damage to a water network was represented as leakages and power outages at pump stations, and recovery was estimated using restoration functions. The model was illustrated for the virtual city of Centerville (Ellingwood et al. 2016).

**Cybernetic Infrastructure Threats**

Cyberattacks are deployed by nation-states, groups, organizations, and individuals to achieve objectives for political, ransom, and terrorist purposes. Cybernetic attacks provide unauthorized access to control software through human access or virus infections on the host machine. Perpetrators may gain access to network segments hosting supervisory control and data acquisition (SCADA) devices with the intent of gaining access to private data or disrupting facility operations (Janke et al. 2014). Two notable examples of cybernetic attacks are the Stuxnet virus and an attack on the Maroochy Shire sewer control system in Queensland, Australia. The Stuxnet virus was transferred to Iran’s nuclear enrichment facilities on a flash drive and ordered centrifuges to rotate and decelerate abnormally fast, causing damage to facility equipment (Langner 2011; Farwell and Rohozinski 2011). In the Maroochy Shire, a cyberattack was executed on a SCADA system, and a disgruntled employee opened sewage valves to release sewage into a nearby park and drainage ditch (Brenner 2013). As advanced sensors and information and communication technology (ICT) systems are used in automating the operation of water networks, it is expected that the occurrence of cyberattacks on water infrastructures will increase. Cyberattacks do not necessarily require a large investment by governments, and, with the rise of cryptocurrency, there is incentive for hackers to gain monetary benefits by disturbing the daily operation of utilities. So-called cryptojacking involves the hijacking and repurposing of computational resources used by utility systems, such as SCADA networks, for mining cryptocurrency (Newman 2018). A critical review of cybersecurity incidents in the water sector was presented by Hassanzadeh et al. (2020), together with a comprehensive description of industrial control system architectures, cyber layers, and attack-defense models.

In light of recent cybersecurity incidents in critical infrastructure system sectors, it is imperative that utilities have a cybernetic infrastructure threat management strategy in place. Publications that have used hydraulic modeling for cyber-physical threat management are compiled in this article. An analysis of this compilation suggests that the use of hydraulic modeling for cybernetic threat management has been steadily on the rise, though their distribution across emergency management activities is disproportionate. Fig. 1 shows the trend of the number of publications over time, and Fig. 2 illustrates their distribution over the five threat management categories.

**Risk Assessment**

Risk assessment involves evaluating the level of cyber risk to an entity, where risk may be characterized by triplets of attack scenario, probability, and consequence (Kaplan and Garrick 1981). A few studies have assessed scenario and consequence as part of risk. Taormina et al. (2017) introduced a toolbox named epanetCPA to characterize a broad array of attack scenarios and their consequences on the hydraulic behavior of WDSs. Douglas et al. (2019) and Taormina et al. (2019) extended the capabilities of the epanetCPA toolbox to simulate pressure-driven simulations of cyber-physical attacks for more realistic modeling of the impacts on system hydraulics. Yeung et al. (2017) developed an approach to estimate the impacts of a large contingency scenario on WDSs without conducting an exhaustive contingency analysis, which is combinatorially prohibitive. Ahmed et al. (2017b) presented the architecture of a cyber-physical water distribution testbed, called WADI, to analyze the cascading effects of attacks.
**Mitigation**

Risk mitigation is any sustained action implemented to reduce or eliminate long-term risk (FEMA 1999). Mitigation is typically achieved through proactive measures that look at securing the operation technology (OT) networks used to monitor and control WDSs. The ongoing convergence of information technology (IT) and OT in the water sector demands a fundamental shift in mitigation and water security (Rasekh et al. 2016). A synergistic study by Laszka et al. (2017) introduced a methodology for eliminating potential vulnerabilities through redundancy, diversity, and hardening. This study has a special focus on cyberattacks launched to cause harm by contaminating a WDS with harmful chemicals.

**Response**

Cyberattack detection is a response activity that detects the presence of an attack and characterizes the attack. This activity has been explored by 75% of the publications in cybernetic threats. The earliest study was conducted by Almalawi et al. (2014), in which a data-driven anomaly detection model was developed using a k-nearest neighbor method and was applied to synthetic WDS data sets generated by EPANET for a simple network. Do et al. (2014) formulated the problem of attack detection as detecting transient changes in the state of a stochastic-dynamical system and demonstrated a threshold-based methodology for detecting a covert attack to steal water from a reservoir. Pasqualetti et al. (2015) developed a model-based framework for the detection of cyberattacks and also focused on attacks that steal water. As with event detection for contamination, detection threshold setting is a critical task. Laszka et al. (2016) formulated the problem as an attacker-defender security game and studied the complexity of finding thresholds. Ahmed et al. (2017a) designed a model-based attack detection procedure using a linear time-invariant model, Kalman filter, and dynamic cumulative sum change detection.

The BATtle of the Attack Detection ALgorithms (BATADAL), which took place in 2017, catalyzed the research in this area (Taormina et al. 2018). The design challenge was set for the C-Town network, and the data were generated using the epanetCPA MATLAB toolbox. BATADAL resulted in several innovative data-driven and model-driven detection frameworks. These include autoencoders (Taormina and Galelli 2018; Chandy et al. 2019), deep learning models (Abokifa et al. 2019), and a model-based methodology based on WDS hydraulics (Housh and Ohar 2018).

**Discussion**

**Emergency Management Activities**

The studies reviewed here are grouped based on their contribution to four emergency management activities within each type of threat. Threat characteristics drive the need for more focus on some activities, as shown by the number of papers across emergency management activities and threats. For example, a physical threat is the only threat for which studies have explored recovery activities, which plan and optimize actions for bringing a damaged WDS back online. In physical scenarios, it is expected that a large set of system components may not be operational, and strategies that account for the timing and order of repairing components are needed. The majority of the studies within contamination threats focus on mitigation activities that include sensor placement and response activities, which include event detection and source identification (Fig. 2). Cybernetic studies focus mainly on response activities, including event detection, to establish the first line of defense against breaches in security.

While emergency preparedness is a critical step in emergency management and required by regulations, this review did not classify modeling approaches that have been applied or developed for use in emergency preparedness. Operators, inspectors, and other personnel run and monitor water systems, and the need for continuous training has increased, due to the importance of stringent regulations, complex chemical and biological processes, infrastructure operations, and infrastructure interconnections. The National Research Council (2006) identified the importance of operator training and called for new attention and investment in training facilities, instructors, and programs. Modeling frameworks to date have not played a major role in developing these capabilities. Some studies reviewed here could be applied to assist in the development of emergency preparedness plans, such as risk assessment tools that focus activities on likely threats and response strategy tools that develop a library of strategies based on hazard characteristics. Further research could investigate how these tools could be used in emergency preparedness activities. For example, Curnin and Heumüller (2016) demonstrated a tabletop exercise for utility response to failure of a dam and developed a methodology to evaluate tasks that were completed as part of the exercise.

**Threat Modes**

Threats modes explored in the literature include, for example, intentional and accidental events and biological and chemical contaminants. Fifty-four studies have explored physical and interconnected infrastructure threats, and the majority of these studies simulated earthquakes, with fewer papers focused on intentional attack and equipment failure. The studies that explored interconnected infrastructure failures focused on failures caused by earthquakes that caused power systems to fail. Cybernetic events only occur through intentional acts.

Studies in contamination events do not always specify the type of threat. For example, many sensor placement, event detection, and source identification studies do not specify whether contamination should have been intentionally or accidentally injected, and some methodologies are also independent of chemical or biological contaminants. Among risk assessment studies, 15 papers developed methods to conduct QMRA for biological threats, and 6 of those papers focused on pressure transient events. As demonstrated by Rasekh and Brumbelow (2013), risk is affected by the threat mode since the probabilities associated with intentional and accidental events vary. Accidental events have been well documented, and probabilistic data associated with their occurrence can be constructed. Intentional events are infrequent, and data are not available to construct probabilistic information about their occurrence. Mechanistic models of the intent of terrorists have been constructed to explain decision-making (e.g., Michaud and Apostolakis 2006; Patterson and Apostolakis 2007; Skolicki et al. 2008; Monroe et al. 2018), but further research is needed to provide information about the frequency that should be associated with intentional attacks.

**Modeling Approaches**

Regardless of the threat mode, the selected solution approach, or the specific technique applied, hydraulic simulation undoubtedly plays a key role in emergency management activities. Of the research studies reviewed here, 222 used hydraulic simulation and 207 used EPANET as the hydraulic simulation engine. Only 12 studies...
used EPANET-MSX to model more realistic reaction dynamics (e.g., Schwartz et al. 2014; Ohar et al. 2015; Mukherjee et al. 2017). Advanced applications using EPANET-MSX require detailed, well-calibrated, and well-maintained hydraulic and water quality models, which are generally uncommon for many WDSs. For example, Zhao et al. (2014) provided a review of event detection algorithms and identified the need to incorporate diverse types of contaminants.

It follows that there is a gap between the available network models used by water utilities for design and planning and the network models required for security applications in WDSs. Furthermore, no common set of standards have been adopted by the research and industry communities that specify the detail required for hydraulic models, water quality dynamics, and design conditions for modeling contamination events. Eighteen papers reviewed here use pressure-driven analysis [shown as EPANET (PDA) in the supplementary materials]. The use of pressure-driven analysis has increased for application in studies that simulate changes in hydrant flows, and model results show a significant difference compared with demand-driven analysis (Bashi-Azghadi et al. 2017; Zafari et al. 2017).

The studies reviewed here use a large number of modeling approaches beyond hydraulic simulation (Table 4). The research conducted here highlights that the development of water security tools has advanced to address additional complexities of infrastructure management. Evolutionary computation methods are the most widely used, and of the 58 studies that implemented an evolutionary computation approach, 25% of those studies used NSGA-II, which is the leading multiobjective algorithm for evolutionary algorithms. Monte Carlo simulation and quasi-Monte Carlo simulation are used in 34 studies. The widespread application of these approaches in supporting emergency management can lend insight into the types of software that may be most useful in developing tools for utility use. Human behaviors, including those of decision makers and water consumers, as they affect the outcome of events and affect exposure through consumption behaviors are captured through discrete event simulation, agent-based modeling, demand modeling, and QMRA approaches. Research has explored the development of tools beyond theoretical models to frameworks that can be implemented by utilities for use in real-time deployment. Adaptive procedures have been developed to assist decision-making as an event unfolds and to select the next steps in responding to the event based on evolving conditions. Further research can also explore the development of a comprehensive approach to event detection that would tightly couple a data-driven and hydraulic model to identify deviations in predictions for event detection.

### Network Applications

Many emergency management activities rely on hydraulic modeling for decision-making, and new models have been demonstrated using realistic, test, and network models (Fig. 4). Test networks (e.g., EPANET tutorial network models) represent simplistic water networks with a small number of pipes and nodes, and virtual networks are hypothetical networks that are constructed to represent a realistic water system. Test and virtual water networks may fail to adequately represent the complexity of water flows in actual networks or accurately predict flows and operations, and efforts to develop hydraulic models using data taken from realistic systems are needed to ensure that methods accurately represent the normal operating conditions of water networks. Realistic networks have been used primarily for physical threats and, in increasing numbers, for contamination threats in the last 10 years. Models in new and emerging research in cybernetic threats and adaptive mobile sensing networks have been verified using test and virtual networks to date.

### Adoption of Modeling Frameworks within Water Industry

Although a multitude of optimization, simulation, and management tools for managing WDS security have been developed, more effort is needed to make these advances accessible to practitioners.

---

**Table 4. Modeling methodologies used in reviewed studies**

<table>
<thead>
<tr>
<th>Methodologies</th>
<th>Examples</th>
<th>No. of papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evolutionary computation (EC)</td>
<td>Genetic algorithm, ant colony optimization, evolution strategies, simulated annealing, NSGA-II</td>
<td>58</td>
</tr>
<tr>
<td>Classical optimization (CLA)</td>
<td>Nonlinear programming, integer programming, gradient-based searches, dynamic programming, branch and bound, depth-first search, gradient search</td>
<td>48</td>
</tr>
<tr>
<td>Other computational methods (OCM)</td>
<td>Agent-based modeling, discrete event simulation, Monte Carlo simulation, Quasi-Monte Carlo Simulation, multiattribute theory, backtracking, game theory</td>
<td>41</td>
</tr>
<tr>
<td>Heuristic approach (HEU)</td>
<td>Heuristic rules, cross-entropy</td>
<td>40</td>
</tr>
<tr>
<td>Statistical modeling (STA)</td>
<td>Probability distribution, Bayesian statistics, Bayesian belief network, logistic regression</td>
<td>25</td>
</tr>
<tr>
<td>Machine learning (ML)</td>
<td>Artificial neural networks, support vector machine</td>
<td>14</td>
</tr>
<tr>
<td>Greedy approach (GRD)</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Graph theory (GT)</td>
<td></td>
<td>11</td>
</tr>
</tbody>
</table>

Note: Abbreviations listed in the table correspond to labels provided for studies in supplementary data.

---

Studies are typically limited to the domain of their developers and are not being widely used. Most of these tools are published in journals without distributing and documenting the code and are rarely used by the scientific community even if the code is available in a public repository. The continuing challenges in bridging the gap between research and practice have motivated several important initiatives in the WDS analysis community. The first is an effort by the Open Water Analytics (OWA) community that is developing an updated version of EPANET’s computational engine using an object-oriented paradigm. Notably, code development and management are hosted using the GitHub open-source development platform, which is open for the exchange of information and ideas related to computing and analysis of WDSs. A second initiative is by the EPA to reengineer and design a modular and extensible architecture for the EPANET user interface (UI). The major functionalities of the new UI are modular software design, scripting, and plugin support using an open-source platform. Although still under development, the first version of the new EPANET UI was released in March 2016. A third initiative was launched by the National Center for Infrastructure Modeling and Management (NCIMM), led by the University of Texas at Austin and initiated primarily by the EPA in 2016, for the purpose of coordinating the development of next-generation water infrastructure simulation models.

Some of the described tools were developed by the EPA, and efforts have been made to implement these tools to make them available to utilities (Janke et al. 2016). Since drinking water utilities have SCADA systems, geographic information systems (GIS), and distribution system infrastructure models, these systems can be combined to support improved utility decision-making. Real-time sensor data for pressure, flow, tank level, pump and valve status, and water quality can be used to produce an accurate and reliable distribution system infrastructure model. To facilitate this, EPA began researching and developing EPANET-RTX to enable the integration of SCADA data with the WDS infrastructure model. This more realistic model can assist water utilities with daily operational activities and emergency situations as well as planning exercises (Janke et al. 2011; Uber et al. 2014; USEPA 2015). CANARY can also be integrated with real-time WDS modeling software to alert users when the modeled results diverge from the collected SCADA data (e.g., flow, pressures, and tank levels). Beyond this, additional effort is needed to minimize the differences between simulation and reality by calibrating network models. Using water security models does not guarantee that applicable solutions to manage water networks will be generated because the discrepancies between models and realities create barriers when uncalibrated hydraulic models are used. New efforts are required to standardize the process of acquiring SCADA and demand data to calibrate hydraulic models with minimum engineering interventions. Polaris, for example, was developed by Citilogics (2020) as a real-time analytics tool that provides a workbench data integration environment to prepare data for the EPANET-RTX model (Janke et al. 2011; Janke 2018). Further research is needed to develop standard processes that enable streaming of SCADA and meter data directly into hydraulic models (Shafiee et al. 2018a). Real-time models that are developed for daily operation and management can be extended for real-time deployment of water security models to improve emergency management.

Conclusions

The analysis conducted here is based on a review of 263 sources that have developed modeling methodologies for the management of WDS threats. This review used an emergency management framework to organize studies within the activities of risk assessment, mitigation, response, and recovery. Studies were grouped based on their contribution to contamination, physical, interconnected infrastructure, and cybernetic threats.

This review found that the majority of studies are focused on contamination threats and that the sensor placement problem has been studied more than other problems in threat management. Research has extended far beyond the first set of studies that developed mathematical formulations of sensor placement in networks to address the realities of real-time response to contamination. Newly developed models address limitations in sensor technology, computational speed, consumer behaviors, and mathematical formulations as they affect event detection, source identification, and response planning. Recent work has developed new methods that support real-time automated response to threats, enabled by real-time hydraulic modeling, emerging data, and adaptive sampling.

Research on physical threats has addressed relevant problems in the event of widespread destruction of system components and developed approaches to continue to supply water as quickly as possible to critical nodes. The majority of these studies focused on loss of service due to earthquakes, and multiple studies developed approaches to plan recovery and restoration of water delivery, which was the focus of a recent design competition, the 2019 Battle of Post-Disaster Response and Restoration (Pacz et al. 2018).

Cybernetic threats have recently emerged due to new capabilities for water utilities to manage infrastructure through ICT and connected systems. Studies in cybernetic threats have investigated vulnerabilities and methods for event detection with application to cybernetic threats (e.g., Taormina et al. 2018). Further work is needed to develop the tools to harden connected WDS components to thwart cybernetic sabotage.

Research in WDS security has also developed new insight about the vulnerabilities of WDSs to interconnected infrastructure threats. Loss of power due to heat waves, for example, can create extensive loss for WDSs. Further interconnected infrastructure research is needed on risk assessment to prioritize vulnerable nodes, on mitigation to develop strategies to install back-up generators, and on response to emergencies to develop adaptive procedures to ensure water is supplied at prioritized nodes.

Evolutionary computation and Monte Carlo simulation are used widely in studies to sample random scenarios and to optimize response and recovery strategies. New software tools to easily enable these solution procedures may advance the application of methodologies, as demonstrated in the published literature. EPANET was used in the majority of the studies, and recent work aimed at including pressure-driven hydraulic has expanded applications to disasters that result in pipe breaks and substantial loss of pressure. Further research is needed to improve the simulation of multispecies interactions, for example, through the use of EPANET-MSX (Shang et al. 2008a, b).

Research and practice can move beyond planning models to use methodological tools in real-time response during an emergency, but this transition will require the development and adoption of realistic and real-time water models. New research is needed to incorporate real-time hydraulic modeling into management protocols, and further research is needed on coupling sensor data with hydraulic models and calibrating models for real-time simulation. Reliable and secure network connectivity is required to connect sensor data with real-time simulation and response methodologies to assess emergencies and identify hazard operations and population protection. Sequential computation of multiple methods using multiple runs of complex hydraulic and mathematical models creates a large computational burden that is not practical for most utilities. Real-time computation facilities that are made available...
through the cloud should be developed for WDS applications to enable fast and thorough insight about evolving threats. Other alternatives are the use of surrogate models that can run more quickly than hydraulic simulations or libraries of response actions that provide a set of rules for selecting actions. The further development of advanced real-time models and computation facilities will reveal new frontiers in managing WDS security.

One limitation of the review conducted here is that many of the models that were developed have not been implemented by utilities or the water industry. As shown earlier in this article, emerging research is focusing on bridging this gap to improve the usefulness of new methods for solving practical problems. Two recently published editorials encourage the community to engage in more open and collaborative research and software development, which will facilitate knowledge transfer and integration of the different tools developed in the water system modeling community to benefit researchers and practitioners and make these tools accessible to a wider community of users for WDS security (Uber et al. 2018; Sela and Housh 2019). The review conducted here identified important directions that should be explored as the community moves forward to improve modeling tools to support WDS security and emergency management.

Data Availability Statement
All data, models, and code generated or used during the study appear in the published article.

Acknowledgments
This publication was developed under Cooperative Agreement No. 83595001 awarded by the US Environmental Protection Agency to The University of Texas at Austin. It has been subjected to the Agency’s review and has been approved for publication. The views expressed in this document are solely those of the authors and do not necessarily reflect those of the Agency. EPA does not endorse any products or commercial services mentioned in this publication.

Supplemental Materials
Data including all references used to generate figures and tables are available online in the ASCE Library (www.ascelibrary.org).

References


© ASCE
03120001-16 J. Water Resour. Plann. Manage.


