Chapter 2
Protecting Water Supply Critical Infrastructure: An Overview

Robert Janke, Michael E. Tryby and Robert M. Clark

Technical Terms and Definitions

CANARY Contamination event detection system
CMMS Computerized maintenance management systems
CWS Contamination warning system
DHS Department of Homeland Security
DSL Digital subscriber lines
EDS Event detection system
EPA U.S. Environmental Protection Agency
GA Genetic algorithm
GAO Government Accountability Office
h Hours
HMI Human–machine interface
ICS Industrial control system
IT Information technology
LIMS Laboratory information management system
LAN Local area network
MCMC Marko chain Monte Carlo
MILP Mixed integer linear program
2.1 Introduction

Government planners have long been aware that urban water systems are vulnerable to threats and disasters, both manmade and natural, including water shortages and droughts, earthquakes, and storms with high winds and flooding. Since the attacks of September 11, 2001, government planners in the United States have been forced to also consider the vulnerability of the nation’s critical infrastructure, including water systems, to terrorism. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (U.S. Congress 2002) intensified the focus on water security (WS) research in the United States. Homeland Security Presidential Directive 7 (HSPD-7), signed on December 17, 2003, established a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. HSPD-7 established the Environmental Protection Agency (EPA) as the lead agency for the Water Sector’s critical infrastructure protection activities. Consequently, the EPA developed a Homeland Security Strategy, which is regularly updated (U.S. EPA 2013). The intent of the act was to enhance national security and protect human health and the environment.
Natural threats from water shortages and droughts have led to political, humanitarian, and environmental crises throughout history and in many parts of the world. Drought may affect both developing and developed countries and, according to the United Nation’s Office of Foreign Disaster Assistance, no other natural disaster has caused as many displaced persons in the twentieth century. Water played an important role in the Peace Treaty that Israel and Jordan signed on October 26, 1994 and to this point the worst case scenarios have not materialized over water disputes in the Middle East. There is concern, however, that water scarcity might become the basis for future wars.

Unlike droughts, which are described as a creeping phenomenon, the damage associated with earthquakes is concentrated in time and space. In 1906, an earthquake in San Francisco caused numerous pipes to rupture and caused dozens of residents drowning when water from broken pipes flooded the Valencia hotel. It was impossible to control the fires that spread through the area and entire buildings exploded in a huge firestorm during which temperatures were reported to reach 2000 °F (1093.2 °C). In 1995, a major earthquake hit the city of Kobe, Japan. The quake lasted 20 s and 4,069 people died, 14,679 were injured, and 222,127 people were moved into evacuation shelters. There were 67,421 fully collapsed structures of which 6,985 were burned to the ground, and there was a city-wide power failure and a nearly city-wide water supply failure (Clark and Deininger 2001). Also in Japan, on Monday, April 11, 2011, in the Hamadōri region of Fukushima, Japan an earthquake of 9.0 triggered tsunami waves that reached heights of up to 40.5 m (133 ft) in Miyako and traveled up to 10 km (6 mi) inland in the Sendai area. At least 1.5 million households were reported to have lost access to water supplies after the tsunami (Samuels et al. Chap. 6 this volume).

Rapid proliferation of computer systems and telecommunication networks compounds the vulnerability of the nation’s critical infrastructure to terrorist attacks (Clark and Deininger 2000). This chapter will discuss the general principles and characteristics of water and wastewater system security and will summarize current research as it relates to system security focusing on intentional threats to water systems.

2.2 U.S. Drinking Water Infrastructure

Most water supply systems in the United States consist of the common elements of a source(s), a treatment facility and a distribution system. Distribution system infrastructure is generally the major asset of a water utility, even though most of the components are either buried or located inconspicuously. Water is transported from its source or sources to various consumers and the system is designed to operate both consistently and economically, and to deliver water in sufficient quantity, of acceptable quality, and at appropriate pressure (Jung et al. 2007). In general, to continuously and reliably move water between a source and a customer,
the system would require storage reservoirs or tanks, and a network of pipes, pumps, valves, and other appurtenances. This infrastructure is collectively referred to as the drinking water distribution system (WDS) (Walski et al. 2003).

2.2.1 System Design and Operation

The branch, grid, or loop represents the three basic configurations for most WDSs. A branch system is similar to that of a tree branch with smaller pipes branching off larger pipes throughout the service area. This type of system is most frequently used in rural areas, and the water has only one possible pathway from the source to the consumer. Grid and loop systems are similar, except that a loop system typically contains a larger diameter primary transmission mains that surround the distribution area, contributing water supply within the grid from different directions. Grid and loop systems are the most widely used configurations in large municipal systems and consists of interconnected pipe loops throughout the area to be served. In this type of system, there are several pathways that the water can follow from the source to the consumer. Transmission water mains are typically 20 (7.9 cm) to 24 (9.4 cm) inches in diameter or larger. Dual-service mains that serve both transmission and distribution purposes are normally 12–20 inches (30.48–50.8 cm) in diameter. Distribution mains are usually 6–12 inches (15.25–30.48 cm) in diameter and located in every street. Service lines are typically 1 inch (2.54 cm) in diameter. Single family residences are commonly served by 3/4 inches (19 mm) service lines; While apartment buildings are large residences can have service lines larger than 1 inch (2.54 cm). Specific pipe sizes can vary depending on the extent of the distribution system and the magnitude of demand. Looped systems provide a high degree of reliability should a line break occur, because the break can be isolated with little impact on consumers outside the immediate area (Clark and Tippen 1990; Clark et al. 2004).

Key infrastructure components in a WDS include the following:

- Storage tanks or reservoirs
- Pipe network
- Valves
- Pumps
- Hydrants
- Other appurtenances, e.g., pits, manholes, blow-offs, and meters.

2.2.1.1 Basic Design and Operational Philosophies

A detailed understanding of “how water is used” is critical to understanding WDS design and operation. Almost universally, the manner in which industrial and residential customers use water drives the overall design and operation of a WDS. Generally, water use varies both spatially and temporally. Besides customer
consumption, a major function of most distribution systems is to provide adequate standby fire-flow capacity (Fair and Geyer 1971). For this purpose, fire hydrants are installed in areas that are easily accessible to fire fighters and are not obstacles to pedestrians and vehicles. The ready-to-serve requirements for firefighting are governed by the National Fire Protection Association (NFPA), which establishes standards for fire-fighting capacity of distribution systems (NFPA 2003). In order to satisfy this need for adequate standby capacity and pressure (as mentioned earlier), most distribution systems use standpipes, elevated tanks, and large storage reservoirs. Additionally, most large distribution systems are “zoned.” Zones are areas or sections of a distribution system of relatively constant elevation. Zones can be used to maintain relatively constant pressures in the system over a range of ground elevations. Sometimes, zone development occurs as a result of the manner in which the system has expanded. Supervisory Control and Data Acquisition (SCADA) systems are key components in operating water distribution networks and have become standard for all medium to large drinking water utilities.

2.2.1.2 SCADA Systems

As with society in general, the use of computer technology in water and waste water technology has become increasingly prevalent. The computer systems for most medium to large water utilities typically include the financial system, the Human Resource system, Laboratory Information Management Systems (LIMS), SCADA systems, and Computerized Maintenance Management Systems (CMMS). The financial, human resources, LIMS, and CMMS are considered to be part of the utilities information technology program and are generally a part of an individual utility or a local governmental information technology (IT) group and are only available 8–10 h a day. SCADA systems are generally run by the utility itself and are available on a 24 h a day, 7 days a week basis. SCADA systems are a computer-controlled type of industrial control system (ICS) that monitors and controls physical industrial processes. SCADA systems historically distinguish themselves from other ICS systems by being integrated into large-scale processes that can include multiple sites and large distances. These processes include industrial, infrastructure, and facility-based processes.

According to Panguluri et al. (2004), a water utility SCADA system usually consists of:

- A human–machine interface (HMI) through which the human operator monitors and controls the process
- A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process
- Remote terminal units (RTUs) connecting to sensors in the process, and sending digital data to the supervisory system
- Programmable logic controllers (PLCs), which are more economical, versatile, flexible, and configurable than special-purpose RTUs
• Communication infrastructure connecting the supervisory system to the RTUs
• Various process and analytical instrumentation

Data acquisition begins at the RTU or PLC level, which includes meter readings and equipment status reports that are communicated to SCADA systems as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU or PLC controls.

A HMI presents process data to a human operator, and the human operator then controls the process through the HMI. HMIs are usually linked to the SCADA system’s databases and software programs to provide trending, diagnostic data, and management information such as scheduled maintenance procedures, logistics information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides. An important part of most SCADA implementations is alarm processing, i.e., determining when alarms should be activated. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken such as the generation of e-mail or text messages to inform management or remote SCADA operators.

The RTU connects to physical equipment. Typically, an RTU converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage, or current. By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.

The term supervisory station refers to the servers and software responsible for communicating with the field equipment (RTUs, PLCs, etc.), and then to the HMI software running on workstations in the control room, or elsewhere. In smaller SCADA systems, the master station may be composed of a single personal computer (PC). In larger SCADA systems, the master station may include multiple servers, distributed software applications, and disaster recovery sites. To increase the integrity of the system, the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server failure.

SCADA systems have traditionally used combinations of radio and direct wired connections (Panguluri et al. 2011). The remote management or monitoring function of a SCADA system is often referred to as telemetry. It is reasonable to consider SCADA as having evolved through three stages. In the first stage, computing was done by mainframe computers. Networks did not exist at the time SCADA was developed. Thus, SCADA systems were independent systems with no connectivity to other systems. Wide area networks were later designed by RTU vendors to communicate with the RTU. In the second stage, processing was distributed across multiple stations that were connected through a local area network
and they shared information in real time. Each station was responsible for a particular task thus making the size and cost of each station less than the one used in the first generation. The third stage might be classified as “networked.” Due to the usage of standard protocols and the fact that many networked SCADA systems are accessible from the Internet, the systems are potentially vulnerable to remote attack. All three of these stages exist in the water industry today.

2.3 Size and Distribution of U.S. Drinking Water Utilities

Water utilities in the United States vary greatly in size, ownership, and type of operation. The Safe Drinking Water Act (SDWA 1974) defines public water systems as consisting of community water supply systems; transient, noncommunity water supply (TNCWS) systems; and nontransient, noncommunity water supply (NTNCWS) systems. A community water supply system serves year-round residents and ranges in size from those that serve as few as 25 people to those that serve several million. A TNCWS system serves areas such as campgrounds or gas stations where people do not remain for a long period of time. A NTNCWS system serves primarily nonresidential customers but must serve at least 25 of the same people for at least 6 months of the year (such as schools, hospitals, and factories that have their own water supply). There are over 162,000 water systems in the United States that meet the federal definition of a public water system (U.S. EPA 2011). Thirty-three percent (52,838) of these systems are categorized as community water supply systems, 55% are categorized as TNCWS, and 12% (19,375) are NTNCWS (U.S. EPA 2011). Overall, public water systems serve 297 million residential and commercial customers. Although the vast majority (98%) of systems serves less than 10,000 people, almost three quarters of all Americans get their water from community water supplies serving more than 10,000 people (U.S. EPA 2011). Not all water suppliers deliver water directly to consumers; some deliver water to other suppliers. Community water supply systems are defined as “consecutive systems” if they receive their water from another community water supply through one or more interconnections (Fujiwara et al. 1995).

Some utilities rely primarily on surface water supplies while others rely primarily on groundwater. Surface water is the primary source for 22% of the community water supply systems, while groundwater is used by 78% of community water supply systems. Of the noncommunity water supply systems (both transient and nontransient), 97% are served by groundwater. Many systems serve communities using multiple sources of supply such as a combination of groundwater and surface water sources. In a grid/looped system, the mixing of water from different sources can have a detrimental influence on water quality, including taste and odor, in the distribution system (Clark et al. 1988, 1991a, b). Table 2.1 provides a snapshot of the size, and the population served for public water systems in the United States (U.S. EPA 2011).
Table 2.1  Public water system inventory data (U.S. EPA 2011)

<table>
<thead>
<tr>
<th>Water system population size category</th>
<th>Very small 500 or less</th>
<th>Small 501–3,300</th>
<th>Medium 3,301–10,000</th>
<th>Large 10,001–100,000</th>
<th>Very large &gt;100,000</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Water Supply # Systems</td>
<td>28,346 2</td>
<td>13,737</td>
<td>4,936</td>
<td>3,802</td>
<td>419</td>
<td>51,356</td>
</tr>
<tr>
<td>Pop. Served</td>
<td>4,763,672</td>
<td>19,661,787</td>
<td>28,737,564</td>
<td>108,770,014</td>
<td>137,283,104</td>
<td>299,216,141</td>
</tr>
<tr>
<td>% of Systems</td>
<td>55 %</td>
<td>27 %</td>
<td>10 %</td>
<td>7 %</td>
<td>1 %</td>
<td>100 %</td>
</tr>
<tr>
<td>% of Pop.</td>
<td>2 %</td>
<td>7 %</td>
<td>10 %</td>
<td>36 %</td>
<td>46 %</td>
<td>100 %</td>
</tr>
<tr>
<td>NTNCWS # Systems</td>
<td>15,461</td>
<td>2,566</td>
<td>132</td>
<td>18</td>
<td>1</td>
<td>18,178</td>
</tr>
<tr>
<td>Pop. Served</td>
<td>2,164,594</td>
<td>2,674,694</td>
<td>705,320</td>
<td>441,827</td>
<td>203,000</td>
<td>6,189,435</td>
</tr>
<tr>
<td>% of Systems</td>
<td>85 %</td>
<td>14 %</td>
<td>1 %</td>
<td>0 %</td>
<td>0 %</td>
<td>100 %</td>
</tr>
<tr>
<td>% of Pop.</td>
<td>35 %</td>
<td>43 %</td>
<td>11 %</td>
<td>7 %</td>
<td>3 %</td>
<td>100 %</td>
</tr>
<tr>
<td>TNCWS # Systems</td>
<td>80,347</td>
<td>2,726</td>
<td>92</td>
<td>13</td>
<td>1</td>
<td>83,179</td>
</tr>
<tr>
<td>Pop. Served</td>
<td>7,171,054</td>
<td>2,630,931</td>
<td>514,925</td>
<td>334,715</td>
<td>2,000,000</td>
<td>12,651,625</td>
</tr>
<tr>
<td>% of Systems</td>
<td>97 %</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>% of Pop.</td>
<td>57%</td>
<td>21%</td>
<td>4%</td>
<td>3%</td>
<td>16%</td>
<td>100%</td>
</tr>
<tr>
<td>Total # of systems</td>
<td>124,270</td>
<td>19,029</td>
<td>5,160</td>
<td>3,833</td>
<td>421</td>
<td>152,713</td>
</tr>
</tbody>
</table>

Source U.S. EPA (2011), “Fiscal Year 2011 drinking water and ground water statistics.” CWS community water supply; NTNCWS nontransient, non-community water supply; TNCWS transient, noncommunity water supply
2.4 Vulnerable Characteristics of U.S. Water Supply Systems to Intentional Threats

Water systems are vulnerable to a range of intentional threats including physical disruption, contamination, and cyber attack. *Vulnerable* implies the existence of a threat and Haimes and Horowitz (2004) characterize threat, in the context of a terrorism scenario, as “a potential adversarial intent to cause harm or damage by adversely changing the states of the system.” Willis et al. (2005) expanded the definition of threat to include intent and capability of the perpetrators. Similarly, again in the context of terrorism, vulnerability is defined by Haimes and Horowitz (2004) to be the “manifestation of the inherent states of a system (e.g., physical, technical, organizational, and cultural) that can be exploited by an adversary to cause harm or damage.” As Haimes and Horowitz (2004) point out “Threats exploit vulnerabilities.”

Vulnerable characteristics of water systems include their physical attributes, e.g., reservoirs, tanks, and pump stations. The distribution system itself may be vulnerable to sabotage or intentional contamination. The “trusted insider” is a potential threat because he or she has presumably extensive knowledge of the water system and its operation, and, therefore, capability (Porco et al. 2006). The largest water systems, i.e., those supporting the largest populations, are believed to be the most vulnerable water systems to attack (Copeland 2010).

In addition to physical attributes, a water utility’s SCADA could be vulnerable to cyber attack, for example, turning pumps on or off, filling or emptying tanks inappropriately, or causing water hammer events. Cyber attacks could also affect the administrative side of the water system business or operation creating confusion by straining already-strained resources and possibly leading to denial of service for some or possibly leading to compromised water quality (Weiss, Chap. 3 this volume).

An examination of published papers, reports, and studies over the past 10–15 years illustrates the range of threats and vulnerabilities to water systems that have been identified by government agencies, researchers, and commercial sectors of the water community. Some specific threats and vulnerabilities are common in many of the studies examined. For example, contaminant threats are generally identified as the primary threat to water systems. While disruption of water service due to some type of physical destruction is often identified, most studies rank such denial of service or disruption-based attacks below those of contamination, both in terms of magnitude of impact (cost and public health) and the length in time of the disruption. From a vulnerability perspective, many studies cite post treatment storage facilities and the distribution system as being the most vulnerable components (Hickman 1999; Brosnan 1999; Allmann and Carlson 2005; Nuzzo 2006; Porco et al. 2006; Copeland 2010; Tularam and Properjohn 2011).
In the following sections, specific vulnerable characteristic of WDSs are discussed including physical disruption scenarios, intentional contamination, unintentional contamination, and cyber security issues.

### 2.4.1 Physical Disruption Scenarios

The President’s Commission on Critical Infrastructure Protection (PDD 63 1998; PCCIP 1997) identified several features of U.S. drinking water systems that are particularly vulnerable to terrorist attack. For example, community water supplies in the USA are designed to deliver water under pressure and generally supply most of the water for fire-fighting purposes. Loss of water or a substantial loss of pressure could disable fire-fighting capability, interrupt service, and disrupt public confidence (Clark and Deininger 2000). This loss might result from a number of different causes. Many of the major pumps and power sources in water systems have custom-designed equipment and in case of a physical attack it could take months or longer to replace them. Sabotaging pumps that maintain flow and pressure or disabling electric power sources could cause long-term disruption (Clark and Deininger 2001). Many urban water systems are reliant on an aging infrastructure. Temperature variations, large swings in water pressure, vibration from traffic or industrial processes, and accidents often result in broken water mains. Planning for main breaks is usually based on historical experience; however, breaks can be induced by a system-wide hammer effect, which could be caused by opening or closing major control valves too rapidly. This could result in simultaneous main breaks that might exceed the community’s capability to respond in a timely manner, causing widespread outages. Recognizing this vulnerability, water systems have been incorporating valves that cannot be opened or closed rapidly. However, many urban systems still have valves that could cause severe water hammer effects. Interrupting the water flow to agricultural and industrial users could have large economic consequences. For example, the California aqueduct, which carries water from northern parts of the state to the Los Angeles/San Diego area, also serves to irrigate the agricultural areas in mid-state. Pumping stations are used to maintain the flow of water. Loss of irrigation water for a growing season, even in years of normal rainfall, would likely result in billions of dollars of loss to California and significant losses to U.S. agricultural exports. Another problem associated with many community water systems is the potential for release of chlorine to the air. Most water systems use gaseous chlorine as a disinfectant, which is normally delivered and stored in railway tank cars. Generally, there is only minimal protection against access to these cars. The release of chlorine gas, whether intentional or unintentional, could injure nearby populations.
2.4.2 Examples of Unintentional Contamination

2.4.2.1 Pressure Transients

Pressure transient regimes are inevitable because all systems will, at some time, be started up, switched off, or undergo rapid flow changes such as those caused by hydrant flushing. They will also likely experience the effects of human errors, equipment breakdowns, earthquakes, or other risky disturbances (Boulos et al. 2005, 2006; Wood et al. 2005). LeChevallier et al. (2003) reported the existence of low and negative pressure transients in a number of distribution systems. Gullick et al. (2004) studied intrusion occurrences in live distribution systems and observed 15 surge events that resulted in a negative pressure. Friedman et al. (2004) confirmed that negative pressure transients can occur in the distribution system and that the intruded water can travel downstream from the site of entry. In fact, soil and water samples were collected adjacent to drinking water pipelines and then tested for occurrence of total and fecal coliforms, *Clostridium perfringens*, *Bacillus subtilis*, coliphage, and enteric viruses (Karim et al. 2003). The study found that indicator microorganisms and enteric viruses were detected in more than 50% of the samples examined.

2.4.2.2 Milwaukee, Wisconsin, USA

In 1993, Milwaukee, Wisconsin, experienced the largest waterborne disease outbreak in documented United States history. The etiological agent was determined to be the *Cryptosporidium* protozoan. In combination with the simultaneous occurrence of frozen ground conditions, recent storms resulted in high levels of surface water runoff while changes in the normal treatment protocols were being introduced were the probable causes of the outbreak. The source of the organism was never officially identified but it was suspected to be caused by the cattle genotype due to runoff from pastures or possibly discharges from a sewage treatment plant outlet two miles upstream in Lake Michigan. Fox and Lytle (1996) and the Centers for Disease Control and Prevention (CDC) showed that this outbreak was caused by *Cryptosporidium* oocysts that passed through the filtration system of one of the city’s water-treatment plants. Over the span of approximately 2 weeks, 403,000 of an estimated 1.61 million residents in the Milwaukee area (of which 880,000 were served by the malfunctioning treatment plant) became ill with the stomach cramps, fever, diarrhea, and dehydration caused by the pathogen. At least 104 deaths have been attributed to this outbreak, mostly among elderly and immuno-compromised people, such as AIDS patients (MacKenzie et al. 1994).
2.4.2.3 Cabool, Missouri, USA

Cabool, Missouri, a town of approximately 2,100 people, located in the South-eastern corner of Missouri, experienced a large outbreak of *Escherichia coli* O157:H7 during the winter of 1989–1990 (Geldreich et al. 1992). The waterborne disease outbreak resulted in 243 cases, with 32 hospitalizations and 4 deaths. This was the largest waterborne outbreak of *E. coli* O157:H7 that had been reported in the United States at the time. A precursor model to EPANET WDS modeling software package was applied to examine the movement of water and contaminants in the system. (EPANET is a public sector model that can simulate hydraulic and water quality transport of drinking water networks.) The modeling effort revealed that the pattern of illness occurrence was consistent with water movement patterns in the distribution system assuming two water line breaks. It was concluded, therefore, that some disturbance in the system, possibly the two line breaks and simultaneous meter replacements, allowed contamination to enter the water system. Analysis showed that the simulated contaminant movement covered 85% of the infected population.

2.4.2.4 Gideon Missouri, USA

In 1993, the town of Gideon, Missouri, located in a rural, agricultural area, suffered an outbreak of salmonellosis that ultimately affected more than 650 people and caused 7 deaths (Hrudey and Hrudey 2004). At the time of the outbreak, Gideon had a population of 1,100. In early November, the town water system had experienced a major taste and odor event. In response, the water system was systematically flushed on November 10. The first cases of acute gastroenteritis were reported on November 29 and diagnosed as *Salmonella typhimurium*. However, the outbreak investigation later revealed that diarrhea cases in Gideon started around November 12 with a peak incidence around November 20. By early December, there was a 250% increase in absenteeism in the Gideon schools and a 600% increase in anti-diarrheal medication sales. Over 40% of nursing home residents suffered from diarrhea and seven people died (Angulo et al. 1997). The U.S. EPA was requested to conduct a field study by the Missouri Department of Health (MDOH) and the CDC (Clark et al. 1996) in early January of 1994. The study utilized water quality modeling to reach the conclusion that the contamination source was bird droppings in the city’s largest municipal tank. The tank’s hatches had severely deteriorated leaving the surface of the water open to contamination by roosting birds.

2.4.2.5 Walkerton Ontario, Canada

The first documented outbreak of *Escherichia coli* O157:H7 and *Campylobacter* spp. bacterial gastroenteritis associated with a municipal water supply in Canada
occurred in the small rural town of Walkerton, Ontario (population 1261) in May 2000 (Grayman et al. 2004). At the time of the outbreak, the town’s drinking water was supplied by three wells (Wells 5, 6, and 7), which fed a common distribution system.

In order to understand the factors that caused the outbreak, a water quality model of the Walkerton WDS was developed. Using a cross-sectional study, it was demonstrated that during the outbreak, residents living in homes connected to the municipal water supply and consuming Walkerton water were 11.7 times more likely to have developed gastroenteritis than those not exposed to Walkerton water.

Modeling of the Walkerton water system required estimations of the following parameters for use in the water quality model:

- Pipe diameter and length, location, age, and composition of all water pipes
- Size, storage capacity, and active volumes of the two stand pipes (water towers) in the system
- Well pump specifications (including pump curves)
- Pipe friction

The results of this study clearly supported the hypothesis that Well 5 was likely the only well involved in the Walkerton E. coli/Campylobacter waterborne outbreak. The results also suggested that an extreme rainfall event, which occurred just prior to the peak of the outbreak, may have played a significant role in the propagation of the contaminants. The primary cause of the contamination event, however, was human negligence. The Well 5 chlorinator was not working prior to the outbreak and the responsible operator knew it, but did not report nor correct the problem.

### 2.4.3 Examples of Intentional Contamination

According to Gleick (2006), attacks on water supply systems have been recorded as long as 4,500 years ago. Hickman (1999) showed that significant harm to public health could be caused by introducing chemical or biological agents into drinking water supplies and the distribution system. Hickman concluded that, “Any adversary with access to basic chemical, petrochemical, pharmaceutical, biotechnological or related industry can produce chemical or biological weapons” (Hickman 1999). Thus, the internet and a small amount of money are sufficient for capability. Hickman identified tanks, reservoirs, and the distribution system as key vulnerabilities. Burrows and Renner (1999) identified a list of biological agents that could be used to efficiently contaminate water supplies. Clark and Deininger (2001) effectively combined the work of Hickman, and Burrows and Renner to highlight how the release of biological organisms into the distribution system could significantly affect public health. Allmann and Carlson (2005) showed how
commercially available distribution system modeling tools could be used to study intentional contamination events and demonstrated that service connections and fire hydrants were likely the most vulnerable components of the water system.

The following two case studies are examples of intentional contamination events in a water system. It is noteworthy that in the first example the perpetrators were able to culture the bacterium in their own laboratory. The second example illustrates that a small amount of a pesticide can be strategically placed to cause a significant amount of damage and loss of service.

2.4.3.1 The Dalles, Oregon, USA

In 1984, the Rajneeshee religious cult, using vials of the highly toxic bacterium *S. typhimurium* [*S. enterica* serovar Typhimurium], attempted to contaminate a water supply tank and salad bars in a number of area restaurants in The Dalles, Oregon. Their intent was to cause massive causalities or widespread panic. The attack resulted in a community outbreak of salmonellosis in which at least 751 cases were documented in a county that typically reports fewer than 5 cases per year. It is not clear if the WDS was chlorinated or what role, if any, disinfectant played in possibly mitigating the consequences from the contamination event. The cult apparently cultured the organisms in their own laboratories (Clark and Deininger 2000; Gleick 2006).

2.4.3.2 Pittsburgh, Pennsylvania, USA

In 1980 in Pittsburgh, Pennsylvania, an unknown perpetrator introduced chlordane into the Pittsburgh distribution system. The insecticide was injected at an isolated valve location on a large distribution main feeding, an area of the distribution system of Pittsburgh. This case study has been reported on in several articles but the most comprehensive discussion seems to be by Welter et al. (2009). The contamination event affected an area of the distribution system serving approximately 10,500 people (Welter et al. 2009). It was thought that eight or more gallons of commercial grade chlordane were introduced into the system. The highest measured concentrations of chlordane were 144,000 ug/L and the estimated average concentration across the 2,000 plus customers was estimated to be about 100 ug/L, which was about 50 times the maximum contaminant level (MCL) permitted for chlordane in drinking water (Welter et al. 2009).

The event was first discovered and reported to the utility by customers experiencing taste and odor problems with their tap water (Welter et al. 2009). The utility quickly recognized that there was a water contamination problem due to the number and location of the complaints and, as a result, dispatched personnel to investigate. Utility personnel quickly confirmed (odor was easy to confirm) that there was a contamination event and the likely contaminant was a pesticide. Public health and water utility officials issued a warning through various outlets, i.e.,
radio, television, and newspaper, to water customers, “do not drink or cook with water until further notice” (Welter et al. 2009). Subsequent sampling and analysis found chlordane concentrations at or above 1 mg/L in many locations (Welter et al. 2009). The utility sought to quickly contain the event, closing valves in order to prevent the contamination from reaching a storage tank. The utility requested and received permission from public health and regulatory officials to initiate hydrant flushing of the pesticide contaminated water to storm sewers in the identified area (Welter et al. 2009). After the contamination was believed to be contained, restoration plans were developed and implemented. Water usage was restored in 1 month, but 9 months of flushing and monitoring were required prior to the release of the water for unrestricted use and some residential appliances and selected pipes had to be replaced (Welter et al. 2009).

The utility and public health officials initially considered shutting down the water system instead of issuing the “do not use for drinking or cooking” order, but the problems associated with no water for sanitation or fire fighting were deemed too critical (Welter et al. 2009). Alternative drinking water was brought in and administered from various locations throughout the contaminated area, especially for residences experiencing high concentrations of chlordane. Additionally, people with sensitive skin were offered the opportunity to bathe nearby but outside the contaminated area. The first action level established was to allow bathing when chlordane concentration dropped sufficiently (below 10 ug/L). Chlordane concentration of 10 ug/L was identified as the odor detection limit for chlordane in heated water. Public health officials allowed drinking and cooking when chlordane concentration dropped below 3 ug/L. However, 3 ug/L was only allowed for 1 month in order to minimize exposure. Additional target action levels were set as the system was flushed and restored, specifically 1 ug/L a month after establishing the 3 ug/L action level, 0.2 ug/L within 2 months, and no greater than the 0.05 ug/L within about 7 months from the start of the event (Welter et al. 2009).

The chlordane incident in Pittsburgh is noteworthy in that extended flushing and intensive monitoring do not tell the whole story. In some cases, customer plumbing was replaced. Such decisions seemed to be based on cost-benefit calculations. Health authorities established progressively lower action levels during the course of the restoration to ensure that customer exposure was minimized. Monitoring continued for months after the system had been restored to unrestricted use (Welter et al. 2009).

2.4.4 Cybersecurity

Growth in the use of the Internet throughout the world has dramatically changed the way that both private and public sectors organizations communicate and conduct business (Clark et al. 2011). Although it was originally developed by the U.S. Department of Defense, the vast majority of the Internet is owned and operated by various entities in the public and private sectors. It is becoming
increasingly recognized that all countries need to prepare for the potential of debilitating Internet disruptions. Therefore in the USA, the Department of Homeland Security (DHS) at the Federal level has been assigned to develop an integrated public/private plan for Internet recovery, should it be impaired. The U.S. Government Accountability Office (GAO) was asked to (1) identify examples of major disruptions to the Internet, (2) identify the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluate DHS plans for facilitating recovery from Internet disruptions, and (4) assess challenges to such efforts (U.S. GAO 2006).

GAO found that a major disruption to the Internet could be caused by:

- A cyber incident (such as a software malfunction or a malicious virus)
- A physical incident (such as a natural disaster or an attack that affects key facilities)
- A combination of both cyber and physical incidents.

Recent cyber and physical incidents have, in fact, caused localized or regional disruptions but have not caused a catastrophic Internet failure. The GAO report presents several examples of major interruptions of the Internet, which are summarized briefly in this chapter.

The move from proprietary technologies to more standardized and open software solutions together with the increased number of connections between SCADA systems and office networks has made SCADA systems more vulnerable to attacks (Panguluri et al. 2011). The security of some SCADA-based systems has come into question as they are seen as potentially vulnerable to cyber attacks.

In particular, security researchers are concerned about:

- Lack of concern about security and authentication in the design, deployment, and operation of some existing SCADA networks
- Believing that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces
- Believing that SCADA networks are secure because they are physically secured
- Believing that SCADA networks are secure because they are disconnected from the Internet.

There are two distinct threats to a modern SCADA system. First is the threat of unauthorized access to the control software, whether it be human access or changes induced intentionally or unintentionally by virus infections and other software threats residing on the control host machine. Second is the threat of packet access to the network segments hosting SCADA devices and one’s ability to control or interrupt critical facility operations. In many cases, there is rudimentary or no security on the actual packet control protocol, so anyone who can send packets to the SCADA device could potentially control it.

The Department of Homeland Security has begun efforts to develop an integrated public/private plan for Internet recovery, but, according to GAO, these efforts are not complete or comprehensive. Specifically, DHS has developed high-
level plans for infrastructure protection and incident response. The GAO has provided five examples to illustrate the breadth and depth of both natural and manmade disasters that could have a major effect of electronic communications (U.S. GAO 2006). Clarke and Knake (2010) have explored the potential for cyber attacks from unnamed adversaries on institutions in the United States. They cite an example of a power failure in combination with a programming glitch in a widely used SCADA system; the glitch slowed utility responses to a falling tree, which created a power surge in Ohio. The surge resulted in a power outage that encompassed 8 states, 2 Canadian provinces, and 50 million people. The Cleveland water system was left without electricity causing their pumps to fail and placing the utility in a near crisis. A hacker attack was launched against an electrical system in Brazil with similar results. A more extreme example is the Stuxnet virus that attacks SCADA systems through vulnerability in Microsoft Windows (AWWA Streamlines 2010), which is discussed below.

2.4.4.1 The “Stuxnet” Virus

The “Stuxnet” virus was apparently designed to jump from computer to computer until it found its specific target that, in this case, was Iran’s nuclear enrichment program. The virus was apparently successful in finding its targets, which were both of Iran’s nuclear enrichment facilities. It entered the operating systems at both facilities and then modified itself when it was discovered. What is especially interesting is that the nuclear facilities in Iran run an “air gap” security system, meaning they have no connections to the Web, making them secure from outside penetration. Stuxnet was apparently designed on the assumption that someone working in the plant would take work home on a flash drive, acquire the worm, and then bring it back to the plant. After defeating the security systems, the worm ordered centrifuges to rotate extremely fast, and then to slow down precipitously damaging the converter, the centrifuges and the bearings, and corrupting the uranium in the tubes. At the same time, it confused Iran’s nuclear engineers and left them wondering what was wrong, because computer checks showed no malfunctions in the operating system. It is estimated that this penetration went on for more than a year, leaving the Iranian program in chaos and that the worm grew and adapted throughout the system (Panguluri et al. 2011).

2.4.4.2 Maroochy Shire Council

An attack that threatened public health and safety was carried out in on Maroochy Shire Council’s sewage control system in Queensland, Australia (Weiss, Chap. 3 this volume). Shortly after a contractor installed a SCADA system in January 2000, system components began to function erratically. Pumps did not run when needed and alarms were not reported. Sewage flooded a nearby park and contaminated an open surface-water drainage ditch and flowed into a tidal canal. The
SCADA system was directing sewage valves to open when the design protocol should have kept them closed. Monitoring of the system logs revealed the malfunctions was the result of cyber attacks. It was found that the attacks were made by a disgruntled employee of the company that had installed the SCADA system.

2.5 The Threat of Terrorism to Urban Water Systems

As discussed previously, it has become generally accepted that water systems and their customers are vulnerable to terrorist attacks. The President’s Commission on Critical Infrastructure (PDD 63 1998) was formed to evaluate the vulnerability of the nation’s critical infrastructure to internal and external terrorism and has highlighted this issue. There are a wide range of vulnerabilities associated with municipal water systems including the expansive and spatially distributed infrastructure that can easily be damaged or sabotaged through physical destruction, cyber attack or control, or through the introduction of contamination.

As Beering (2002) points out, “Threats must be analyzed ‘in perspective’.” The utility must assess its weakest points, and then consider what actions a potential attacker might employ against them. Further, it has been noted that we need to analyze consequences to prioritize responses, identify critical components, harden or secure those that can reasonably be better protected, and develop response plans (Beering 2002; Gleick 2006).

Here we start with a brief discussion on threats to water systems. Broadly, we categorize threats to water systems as either internal or external in origin. Next, we provide some rationale as to why we believe the security emphasis in the water community should be focused on water contamination threats. Next, we discuss water contamination events from the perspective of what is known from selected published papers and reports that have examined the nature and consequences of intentional contamination events. Specifically, we discuss contamination from the perspective of: (1) contaminant quantity, method, and location selection within the water system for contamination injection or release, (2) water contaminants, and (3) magnitude of possible consequences. Finally, we talk about countermeasures that could be employed to defend against possible threats and water system vulnerabilities.

2.5.1 Internal and External Threats

Threats or perpetrators can generally be categorized as either internal or external to the water utility or its community. Porco et al. (2006) suggests the “trusted insider” is perhaps the greatest vulnerability. Copeland (2010) identifies the most likely “vulnerable” water systems to be the relatively small number of water systems serving the largest populated cities in the country.
Internal threats might include disgruntled employees who may or may not be currently employed at the organization. For example, as discussed earlier, in Pittsburgh, some believe the unknown perpetrator was a disgruntled employee (Tucker 2000). Other insider attacks might include a scenario where pipelines from drinking WDS were deliberately cross-connected with a wastewater collection pipeline. Insiders, including current employees, former employees, contractors and vendors, pose a particularly dangerous threat since they have specific knowledge of the utilities’ weaknesses.

External threats may range from simple vandals to nation-sponsored terrorist threats. Critical infrastructure is an attractive target for terrorists due to the potential consequences and ripple effects of a successful attack. The distribution components of a water system are especially at risk due to the potentially large number of illness and death that could result from an attack. DHS has issued advisories to water utilities indicating that al-Qaida has shown interest in using cyanide, Botulinum toxin (Botox), Salmonella typhi (the causative agent of typhoid fever), and Bacillus anthracis (the causative agent of the disease anthrax) to attack U.S. water systems (U.S. DHS 2003). Terrorist organizations such as al-Qaida are not the only external sources with motives to use chemical or biological weapons to attack a water system.

### 2.5.2 Intentional Water Contamination Events

Hickman (1999); Clark and Deininger (2000, 2001), provided some of the earliest papers raising the awareness of the vulnerability of WDSs to contaminant threats. Hickman (1999), Brosnan (1999), and Clark and Deininger (2000, 2001) have shown that the distributed nature of the distribution system makes it particularly vulnerable to contamination attacks. Clark and Deininger (2000, 2001) specifically highlighted the distribution system as the most vulnerable component of a water system.

Disruption of water service due to some type of physical destruction is often considered in the identification of water threats, but most studies rank such denial of service or disruption based attacks below those of contaminant introduction, both in terms of magnitude of impact (cost or public health consequences) and the length of time of the disruption. Contamination threats represent the greatest risk to water systems and the communities they serve.

Numerous papers have analyzed and reported on the types of contaminant threats that would be of concern to water systems. Prior to the plethora of post-9/11 research studies on the threats and consequences of chemical and biological agents on water systems, Hickman (1999) identified and qualitatively characterized the magnitude of public health impacts that could result given the deliberate introduction of chemical or biological contaminants into a water system to be significant. Hickman (1999) noted from his analysis that “it is not expensive to wage an unsophisticated attack on a community water system.”
In 2005, American Water Works Association (AWWA) hosted and led a water utility forum to raise awareness of contamination threats to water systems and identify key research questions that needed to be answered in order to design effective contamination warning systems (CWSs) and response capabilities (Roberson and Morley 2005). In 2007, EPA launched the WS Initiative (WSi), a pilot program to deploy and evaluate CWSs as demonstration projects at four major cities across the country (U.S. EPA 2007). These efforts and others demonstrate the need to focus on water contamination threats to water systems.

In the following sections, the intentional threat is discussed from the perspective of (1) approach, (2) contaminant, and (3) magnitude of potential consequences. Current research work is cited to frame the magnitude of possible public health consequences that could occur given a terrorist attack on an urban water system.

2.5.2.1 Approach

Contamination of a distribution system could occur through contaminant release (e.g., dumping chemicals or pesticides into a water tank) or injection (pressurized back flow of a chemical solution into the distribution system through a service connection). Fire hydrants, tanks, reservoirs, or pump stations are vulnerable to both contaminant release and contaminant injection. Pressurized backflow could theoretically occur anywhere in the distribution system and simply requires a pump with the necessary power to overcome the distribution system line pressure where the injection is to occur.

The amount of material needed to deliberately contaminate a water source (such as a reservoir or aquifer) is large and generally exceeds what an individual or small group of terrorists could easily acquire, produce, or transport. However, contaminants introduced into a tank or directly into the distribution system would be diluted less and would reside in the system for shorter times prior to public exposure and ingestion, thus diminishing the effects of disinfectants and chemical decomposition and oxidation.

A number of researchers have investigated intentional contamination events in WDSs. The objectives of these studies varied from performing threat and consequence studies to developing algorithms and methodologies for designing CWSs. Early work by Hickman (1999), Uber et al. (2004), and Allmann and Carlson (2005) demonstrated the feasibility and shed light on the magnitude of consequences that could result due to intentional contamination of WDSs. Hickman observed that such consequences would be significant. Uber et al. (2004) estimated the consequences that could range from 6% to above 50% of the population being exposed to lethal concentrations of a toxic contaminant. Allmann and Carlson (2005) estimated that a single pressure zone (an area of four square miles) could be contaminated at a concentration corresponding to a lethal dose for the chemical agent VX (Allmann and Carlson 2005). However, Davis et al. (2013) describe how less toxic contaminants could be used to contaminate even larger
areas at lethal dose concentrations. Grayman et al. (2008) demonstrated the application of hydraulic modeling to a better understanding of possible high-rise building contamination, noting that contamination can originate from outside or from within the building and the extent of contamination is “most sensitive to the operational aspects of the internal water system.”

Generally, early studies analyzed a small number of contamination scenarios and later studies have analyzed ensembles or collections of contamination scenarios to provide a statistical analysis of the consequences by injection location. Probabilistic approaches have been applied to the study of contamination events to understand how water usage influences exposure and consequences (Khanal et al. 2006) or better predict the timing of when people drink to better assess dose (Davis and Janke 2008, 2009).

Davis and Janke (2011) and Davis et al. (2010) quantified the consequences from contamination events for a diverse set of 12 real distribution systems. Their modeling and simulation work showed that significant (those similar to worst case) consequences from intentional contamination events would likely only occur at a minority of release or injection locations. These studies also demonstrated that the size of the area exhibiting certain public health consequences was relatively small for less toxic contaminants compared to the size of the area for very toxic contaminants with the relationship being proportional to the quantity of contaminant released or injected.

Grayman et al. (2008) constructed EPANET-based hydraulic models to examine the movement of contaminants within high-rise buildings. Their work showed that contamination movement within residential buildings were very sensitive to the water usage patterns at the fixture level, toilets, faucets, showers, etc. In high-rise buildings, contamination entering the building from the municipal distribution system along with its movement through the high-rise building was found to be most sensitive to the operational practices of the building’s water system, i.e., pump operation in filling and draining the building’s tanks. Janke et al. (2009) and collaborators later applied the high-rise building model to study consequences and sensor monitoring location performance in two real, but artificially modified system models. These papers along with others illustrated the influence of model detail on estimating consequences.

The nature of the contamination event can be described, generally, by three aspects: (1) type and quantity of the contaminant released as well as the behavior of the contaminant once released into the system, (2) location or locations in the water system where the contaminant is introduced, and (3) the type and distribution of the population downstream of the contaminant introduction and their behavior as the contamination progresses through the water system.

2.5.2.2 Water Threat Contaminants

The President’s Commission on Critical Infrastructure Protection (PCCIP 1997) concluded that there is a credible threat to the nation’s water supply system from
certain known biological agents. Certain chemical agents have also been identified that might constitute a credible threat against water supply systems. The U.S. Army Combined Arms Support Command evaluated 27 agents for the potential for weaponization. Seven of twenty-seven agents are listed as having the potential for being “weaponized” and 14 others are listed as either possible or probable weapons. A number of these organisms are listed as definite or probable threats in water (Clark and Deininger 2000; Burrows and Renner 1999). In addition, newly discovered or emerging pathogens may pose a threat to water supply systems. One such pathogen was isolated during an EPA study (Clark and Deininger 2000) in Peru. Several chemical agents have also been identified that might constitute a credible threat against water supply systems. Although much is known about chemical and biological agents dispersed in air, less is known about these agents in potable water.

Allman and Carlson (2005) conducted a study utilizing a commercial distribution system modeling software program to show how a drinking water system could be impacted by the intentional introduction of chemical contaminants. They examined four highly toxic chemicals such as c-parathion, VX, sodium monofluoroacetate and cyanide, along with a WDS considering water quality models under various scenarios to determine the influence of feed methodology, location, and the contaminant on the effect of contamination. Their results showed that it was possible to accomplish large-scale contamination of a drinking water system through backflow into major network water supply lines.

Most modeling and simulation studies examined do not specify a contaminant but generally refer only to the contaminant as being toxic or harmful, or as being of chemical or biological in nature. Often researchers will specify whether the analysis treats the contaminant as a conservative tracer or considers some form of decay or loss. Most studies to date have generally not considered contaminant decay or loss. Propato and Uber (2004) examined the vulnerability of WDSs to pathogen intrusion to understand how effective a system’s disinfectant residual would be. Their findings indicated that disinfectant residual is generally not very effective at reducing the risk of disease from pathogen intrusion.

Davis et al. (2013) consider influence of contaminant decay or loss in their analysis of the consequences of intentional WDS contamination in 12 diverse, real water systems. The extension to EPANET allowing the user to evaluate more sophisticated contaminant interactions in a WDS has been available since 2008 with the release of the multispecies version of EPANET (Shang et al. 2008). The ability to consider the influence of multispecies interactions on estimating consequences was provided with the update of Threat Ensemble Vulnerability Assessment Sensor Placement Optimization Tool (TEVA-SPOT) to include the EPANET-MSX capability in 2011 (U.S. EPA 2013).

Davis and Janke (2011) and Davis et al. (2010) showed that consequences are dependent on the contaminant, where it is released or injected into the distribution system, and the quantity released. The work of Davis and Janke (2011) and Davis et al. (2010) supported the earlier findings of Allman and Carlson (2005). However, the approach used by Davis and Janke (2011) and Davis et al. (2010)
consisted of a flexible approach that was noncontaminant-specific but could be applied to any contaminant for which health effects information was available. Davis and Janke (2011) and Davis et al. (2010) defined “impacts” to be the number of people who receive a dose (mg of some chemical or number of organisms ingested through contaminated tap water) above a certain level. This “impacts”-based approach was extended in Davis et al. (2013).

Davis et al. (2013) expanded on earlier work by examining the consequences from intentional contamination events given contaminant decay or loss as a result of transport in the WDS. A flexible analysis framework for estimating the magnitude of consequences is presented for any system provided the population is specified along with the contaminant and its behavior (decay/loss rate) in the WDS. Specifically, upper bounds on the magnitude of adverse effects are developed for a wide range of water systems, possible contaminants (based on toxicity), and a wide range of contaminant decay/loss rates.

The magnitude of adverse consequences given the release of a contaminant into a WDS is a function of the contaminant: (1) toxicity, (2) quantity released, and (3) behavior in WDS. The behavior of the contaminant is dependent on its interaction with any available disinfectant and naturally occurring biological materials present in WDSs. Adverse health effects are dependent on contaminant solubility and organoleptic properties, which influence exposure and dose.

2.5.2.3 Magnitude of Potential Consequences

Consequences of a water contamination event can be significant. A contamination event in a water system can adversely affect the people, the businesses, and the community it serves due to fear, loss of water service, significant economic costs for decontamination and recovery, and the magnitude of adverse public health effects. Public health consequences can be described and estimated as (1) exposures (i.e., people through their places of residence and business witness contamination in their tap water) (2) doses (i.e., people within the community served by the water system ingest contaminated water or somehow accumulate some measurable quantity of the contaminant or contaminants in their bodies), or (3) health effects, i.e., given some ingested mass of contaminant a health effect can be estimated. Health effects can occur within the short term, i.e., within days or weeks of exposure, or in the long term, i.e., within months or years. Within the short term, health effects could include sickness, incapacitation, or death. In the long term (i.e., Yrs), health effects could include increased cancer risk, although such health effects may be difficult to link to WDS contamination.

Numerous researchers have characterized the magnitude of the consequences that could result from an intentional contamination event in a water system. Most of the research work to describe and estimate the consequences from intentional contamination events have been in the support of WS tools. For instance, Ostfeld et al. (2008), Berry et al. (2005a, b), and Krause et al. (2008) have developed tools to determine where best to place sensor monitoring equipment in support of a
CWS. These researchers, as well as others, used extended period simulation models to predict the consequences of contamination events. Consequences were generally estimated by quantifying (1) tap water contamination concentrations, (2) quantity of pipe experiencing contamination, (3) quantity of contaminant removed at each model node (e.g., gallons of polluted water), (4) population exposed, fraction of population at risk, or number of people who receive a certain dose of contamination, and (5) population sickened or killed, using exposure, dose, and dose response models. Since these studies were intended to develop optimization algorithms, little effort was devoted to accurately estimating public health consequences or infrastructure consequences or even understanding the uncertainties in the process.

A historical evaluation of unintentional contamination events in water systems can provide some insight on the magnitude of adverse public health effects that can occur from contamination events in water systems. Approximately 690,000–1,790,000 *Salmonella typhi* cases, 20,000 hospitalizations, and 400 deaths occur annually in the USA, costing approximately $2.6 billion dollars (US) (Economic Research Service 2008; Scallan et al. 2011). *Salmonella* causes 35% of all foodborne hospitalizations, 10% of waterborne disease deaths, and 28% of foodborne disease deaths (Craun et al. 2006; Scallan et al. 2011). Unintentional *Salmonella* outbreaks can infect large numbers of people. The intentional introduction of *Salmonella* into a WDS could affect a far greater number of people. *Salmonella* was used as a biological terror agent in The Dalles, Oregon in 1984 (Torok et al. 1997).

*Salmonella* incidence in WDSs and the cost of the associated consequences are difficult to quantify. Incidence, morbidity, mortality, and duration of many historical outbreaks are uncertain (Craun et al. 2006). Current methods fit three categories: (1) incidence models; (2) national illness burden models; and (3) economic impact models. Numerous general or *Salmonella*-specific incidence models exist. Murray et al. (2006) proposed a general susceptible, infected, and recovered population model of the spatial and temporal disease distribution in a WDS. Chandrasekaran (2006) modeled *Salmonella* incidence from contaminated water storage tanks, Danyluk et al. (2006) estimated the risks of consuming raw almonds and Mena et al. (2008) estimated the risks from pipe cross connections. Murray et al. (2006) estimated mortality while the others only estimated incidence.

Herrick et al. (2011) developed a Markov chain Monte Carlo (MCMC) model to estimate illness duration, physician, and emergency room visits, inpatient hospitalizations, mortality, and resultant costs for the Gideon, Missouri *Salmonella* waterborne disease outbreak. Most existing models estimate morbidity, mortality, and cost solely from incidence data but do not estimate illness duration as an independent cost predictor. As a result, such models may underestimate physician visits, hospitalizations, deaths, and associated costs. In the Herrick et al.’s (2011) study, transition probabilities for the Markov analysis were based on a meta-analysis of 53 *Salmonella* studies. His model resulted in an accurate prediction of the public health consequences from the Gideon, Missouri outbreak (Clark et al. 1996).
Predicting the consequences from intentional contamination can be difficult. Most modeling and simulation studies have examined intentional contamination events from the perspective of a single contamination event. Further, actual intentional contamination events have resulted in fairly localized consequences. Little, if any, has been published estimating the consequences from multiple, concurrent contamination events in WDS. Most studies have only varied the location of the contaminant release in the WDS and the various parameters describing the contaminant and how the contaminant is released or injected into the WDS. A few researchers have studied the behavior of potential receptors downstream of the contamination event. Davis and Janke (2011) studied the magnitude of potential consequences, termed “impacts,” given a range of dose thresholds or levels (representing a range of contaminant toxicities), location of contaminant release in the WDS, size of population served by the water system, and quantity of contaminant (mass) released. In Davis et al. (2010), the authors examined the nature of the consequences or “impacts” for 12 real and diverse water systems while looking at the sensitivity of the consequences to (1) mass of contaminant injected, (2) time of contaminant injection, (3) duration (hr) of contaminant injection, (4) distribution of population within the WDS model, (5) tap water ingestion pattern, i.e., time of day when people drink and how much. In Davis et al. (2013), consequences were estimated while considering contaminant decay or loss.

In each of these studies, an ensemble of contamination events, described by a contaminant injection at each nonzero demand node in the model, were simulated to determine each location’s percentile ranking based on consequences. Generally, only nonzero demand nodes were used as injection locations because they were believed to be most representative of actual service connections. Injection or release of contamination directly into utility facilities, e.g., tanks, was not evaluated.

These studies showed that the magnitude of public health consequences are most influenced by (1) size and nature of the particular WDS, (2) toxicity, quantity of contamination injected, and behavior of the contamination within the WDS, and (3) location of the contamination injection. Given no prior knowledge of the particular WDS, the results further indicated that a random selection of a particular contamination injection location could result in consequences that approach between one-thousandth and one-tenth of the particular system’s worst case consequences (Davis et al. 2010), ranging from only a few people to many thousands, which could represent a significant fraction of the population served by the water system. Their work also showed that public health consequences from very toxic contaminans can vary substantially between water systems and is largely a function of the population served. However, for less toxic contaminants, public health consequences can be similar across a wide range and size of water systems. For less toxic contaminants, network population does not significantly influence the magnitude of consequences and increasing the quantity of contaminant injected will have a significant influence on the magnitude of consequences (Davis et al. 2010).
2.6 Countermeasures Against Terrorism

The authors believe that there are several steps that a water utility can take to protect against terrorist threats. These steps will be discussed in terms of physical countermeasures and the CWSs, which include chemical countermeasures and institutional countermeasures.

2.6.1 Physical Countermeasures

Access to a free water surface such as exists in a water reservoir should be eliminated. For example, the ventilation devices in a reservoir must be constructed in such a way as to prevent contamination of the reservoir. The intakes, pumping stations, treatment plants, tanks, and reservoirs should be fenced to secure them against casual vandalism. Beyond that, intrusion alarms should be installed to notify the operator that an individual has entered a restricted area. An immediate response might be to shut down a part of the pumping system until the appropriate authorities determine that there is no threat to the system.

An important extension of the security concept against terrorist attack would be the planning and construction of separate water lines that are fed from a protected water supply-source, which would only be activated during an emergency. Many of the older cities in the United States have separate water lines that have been installed for fire protection in heavily developed downtown areas. These water lines might be upgraded for possible use to supply the population with safe water during emergency conditions. Such proactive planning for WS, including the continuous maintenance and monitoring of chlorine residual in the water, would help to ensure the safety of most water supply systems. Nevertheless, it is of vital importance that system planners and managers be constantly on the alert to prohibit deliberate sabotage of municipal water supply systems.

2.6.2 Contamination Warning System

Among the different threats to a WDS a deliberate chemical or biological contaminant injection is the most difficult to address, both because of the uncertainty of the type of the injected contaminant and its consequences, and the uncertainty of the location and injection time. In principle, a pollutant can be injected at any WDS connection (node) using a pump or a mobile pressurized tank. Although backflow preventers provide an obstacle to such actions, they do not exist at all connections (i.e., generally very rare), they are not always functional at all connections, and they can be overcome.
Online contaminant monitoring systems or simple CWS have been considered for some time (ASCE 2004; AWWA 2004) as a tool to reduce the consequences of a deliberate contamination attack from either a chemical or biological intrusion. A CWS should be designed to detect contamination events and to provide information on the location of the contaminants within the system, including an estimation of the injection characteristics (i.e., contaminant type, injection time and duration, concentration, and injected mass flow rate). Once the type and the characteristics of the contaminant are discovered, a containment strategy can be implemented to minimize the contamination spread throughout the system and to determine which parts of the system need to be contained and/or flushed.

CWSs have been envisioned to include multiple approaches to monitoring. For instance, water quality sensors located throughout the distribution system combined with a public health surveillance system and a customer complaint monitoring program are believed to be capable of detecting a wide range of contaminants in water systems. However, the concept of using a water quality sensor-based CWS has only been piloted within the last decade and little experience exists to demonstrate performance. Also, CWSs are expensive to purchase, install, and maintain. To make them a viable option, there is a clear need to maximize the benefits that a CWS can provide beyond those of security.

EPA is piloting the deployment of test CWSs through the Office of Water’s Water Security initiative (WSi), formerly called WaterSentinel, at five large drinking water utilities across the nation (U.S. EPA 2007, 2008). (The WSi program was developed by EPA in close partnership with drinking water utilities and other key stakeholders involving the design, deployment, and evaluation of a CWS for drinking water systems.) Design includes the selection of water quality sensors and their strategic placement in the WDS.

The WSi promotes a comprehensive CWS that is capable of detecting a wide range of contaminants, covering a large spatial area of the distribution system, and hopefully providing early detection to mitigate impacts (U.S. EPA 2005, 2007). Components of the comprehensive CWS being piloted through WSi include chemical countermeasures (online water quality monitoring) and institutional countermeasures such as consumer complaint surveillance, public health surveillance, enhanced security monitoring, and routine sampling and analysis. These components are described below (U.S. EPA 2007).

### 2.6.2.1 Online Water Quality Monitoring

Continuous online monitors for water quality parameters, such as chlorine residual, total organic carbon (TOC), electrical conductivity, pH, temperature, oxidation reduction potential (ORP), and turbidity help to establish expected baselines for these parameters in a given distribution system. Hall et al. (2007) found that free chlorine (in chlorinated water) and TOC were the most useful parameters for observing a changed water quality baseline condition due to a contaminant injection. Event detection systems, such as CANARY (Hart et al. 2007) or Hach
Corporation’s Guardian Blue (Kroll 2006), can detect anomalous changes from the baseline to provide an indication of potential contamination. (CANARY is software that can help detect a wide variety of chemical and biological contaminants in drinking water.) The system can also use other monitoring technologies, such as contaminant-specific monitors. The goal is to detect a wide range of possible contaminants.

2.6.2.2 Consumer Complaint Surveillance

Water utilities track consumer complaints regarding unusual taste, odor, or appearance of the water, and they record what steps they took to address these water quality problems. The WSi is developing a process to automate the compilation and tracking of information provided by consumers. Such a system, coupled with anomaly detection software, might be able to rapidly identify unusual trends that indicate a potential contamination incident.

2.6.2.3 Public Health Surveillance

Syndromic surveillance conducted by the public health sector might serve as a warning of a potential drinking water contamination incident. This surveillance includes information such as unusual trends in over-the-counter sales of medication, and reports from emergency medical service logs, 911 call centers, and poison control hotlines. Information from these sources can be integrated into a CWS by developing a reliable and an automated link between the public health sector and drinking water utilities.

2.6.2.4 Enhanced Security Monitoring

Security breaches can be monitored and documented through enhanced security practices that detect anomalous conditions. A tampering event can potentially be detected in progress and thus possibly preventing the introduction of a harmful contaminant into the drinking water system.

2.6.2.5 Routine Sampling and Analysis

Utilities can collect and analyze water samples at a predetermined frequency to establish a baseline for contaminants of concern. This provides a baseline for comparison during the response to detection of a contamination incident. Laboratory staff can engage in regular drills simulating the sampling and analysis of potential contaminants so that they will be better prepared for an actual incident.
Procedures can be periodically reviewed by qualified personnel to ensure that they remain up-to-date and implementable.

Simply placing a collection of monitors and equipment throughout a water system is not enough to effectively detect contamination incidents. To be effective, a CWS must also manage large volumes of data and provide actionable information to decision-makers. Different information streams must be captured, managed, analyzed, and interpreted in time to recognize potential incidents and mitigate the impacts. Each component of a comprehensive CWS provides useful information; however, if the data from these several components were integrated and used to evaluate a potential contamination incident, the credibility of the incident could be established more quickly and reliably than if any single information stream were used.

Many utilities currently implement monitoring and surveillance activities, but few are operating in such a way as to meet the primary objective of a CWS – timely detection of a contamination incident. For example, although many utilities currently track consumer complaint calls, a CWS requires a robust, spatially based system that, when integrated with multiple data streams (from public health surveillance, online water quality monitoring, and enhanced security monitoring), can provide specific, reliable, and timely information for decision-makers to design an effective and timely response. Consequence management plans and advanced laboratory capabilities are also required in order to respond to contamination incidents in a timely and appropriate manner. The utility, public health agencies, local government officials, law enforcement, and emergency responders, and others, must coordinate to develop an effective consequence management plan that ensures appropriate response to detection by different components. An advanced and integrated laboratory infrastructure is needed to support baseline monitoring and analysis of samples collected in response to initial detections. Still, the challenge in applying a CWS is to reliably integrate the multiple information streams in order to decide if a contamination incident has occurred. While the primary purpose of a CWS is to detect contamination incidents, dual-use benefits, such as better monitoring of water age (a surrogate for water quality) under routine circumstances, will likely help to ensure the sustainability of a CWS within a utility.

2.6.3 Cyber Security Countermeasures

Water utility SCADA systems present a major vulnerability to terrorist attacks. As the importance of SCADA systems grow this vulnerability will grow as well (Clark et al. 2011; Weiss, Chap. 3 this volume). DHS established the National Cyber Security Division (NCSD) as a public–private partnership to serve as the flagship for cyber security coordination and preparedness. The NCSD established the U.S. Computer Emergency Readiness Team (U.S. CERT) and the Control Systems Security Program (CSSP).
U.S. CERT provides the operational component of NCSD for advancing cyber security protection across the federal government. Specifically, U.S. CERT is responsible for providing response support and defense against cyber attacks for the U.S. government (nonmilitary). U.S. CERT coordinates with federal agencies, industry, the research community, state and local governments, and others to provide actionable guidance and information on cyber security to the public. CSSP’s role is to reduce SCADA and industrial control system risks across all critical infrastructures. The CSSP coordinates activities to reduce the likelihood of cyber attack success and the magnitude of their possible impact against critical infrastructure control systems through risk-mitigation activities. The Cyber Security Evaluation Tool (CSET) is a software tool that assists organizations in protecting their IT assets. CSET guides users through a step-by-step process to assess their network security practices against industry standards. CSET provides a prioritized list of recommendations for improving the cyber security of water utility’s SCADA system.

Panguluri et al. (2004) lists 10 vulnerabilities which are common to SCADA system infrastructure as follows:

- Operators are logged-on to the system even when the operator is not present at the workstation, thereby rendering the authentication process useless.
- Easy physical access to the SCADA equipment.
- Unprotected SCADA network access from remote locations via digital subscriber lines (DSL) and/or dial-up modem lines.
- Insecure wireless access points on the network.
- Most SCADA networks are connected directly or indirectly to the internet.
- No firewalls are installed or the firewall configuration is weak or unverified.
- System event logs are not monitored.
- Intrusion detection systems are not used.
- Operating and SCADA system software patches are not routinely applied.
- Network and/or router configuration insecure; passwords are not changed from the manufacturer defaults.

All utilities should periodically review and examine these vulnerabilities. Panguluri et al. (2011) suggest some positive steps that utilities should consider to enhance their cyber security and in particular protect their SCADA systems against cyber threats. It is recommended that utilities take the following six steps to protect cyber system:

- Be proactive in testing software by testing source and binary application code using security scanners with assessments and certifications.
- Employ a variety of network-based intrusion prevention and detection systems combined with network behavior analysis, firewalls, enterprise antivirus, and threat management devices (secure gateways, application firewalls, and managed security services).
• Implement a variety of host-based security measures such as endpoint security, network access control, and system integrity checking tools, application control, and configuration hardening tools.
• Establish vulnerability management by employing penetration testing and ethical hacking techniques, followed by patch and security configuration management and compliance measures.
• Implementing measures such as identity and access management, mobile data protection and storage and backup encryption, content monitoring/data leak prevention, and virtual private networks (VPNs).
• Initiate the use of tools and measures such as log management, event management, media sanitization, mobile device recovery and erasure, security skills development, security awareness training, forensics tools, governance, risk and compliance management tools, and disaster recovery and business continuity planning.

An approach that a utility might consider to effectively increase cyber security is to add network security improvements as a part of the expansion and upgrades to capital projects. If the utility has a current vulnerability assessment that includes network improvement recommendations and the network is well documented, the improvements added can be a step-wise approach to implementing the assessment’s recommendations. Without a vulnerability assessment and network documentation, any security improvements implemented may still improve security, but are less likely to be as effective as they might be. In summary, the general technical controls that are very likely to improve network security include (Panguluri et al. 2011):

• Develop secure network topologies.
• Implement logical network separation.
• Effectively employ DMZs (DMZs are separate small buffer networks between a private internal network and an external network).
• Limit physical access.
• Restrict privileges.

2.7 Research into Distribution System Security

Research into drinking WDS security largely began as a result of the events of September 11, 2001. Prior to September 11, 2001, little research was devoted to the improving the security of water systems. While HSPD-7 established a national policy for federal departments and agencies to identify, prioritize, and protect critical from terrorist attacks; HSPD-9, issued on January 30, 2004, directed EPA to “develop robust, comprehensive, and fully coordinated surveillance and monitoring systems… that provide early detection and awareness of disease, pest, or
poisonous agents.” In 2004 EPA released a research and technical support action plan outlining key research questions along with a list of planned research projects (U.S. EPA 2004).

Since September 2001, research has been focused in several major areas: (1) development of methodologies and tools for assessing the consequences of water contamination events; (2) development of methodologies (algorithms) and tools for the optimal placement of sensors in a distribution system; (3) use of water quality sensors to detect contaminants as the principle components of a contamination event detection system (EDS); and (4) development of methodologies and tools for responding to contamination events, including real-time monitoring and modeling capabilities to provide the necessary foundation for implementing effective response actions. In this section, we briefly examine what has been done in each of these research areas and identify some questions that still need to be answered.

2.7.1 Methodologies and Tools to Assess the Consequence of Contamination Events

Since the early 1990s, various researchers (Clark and Deininger 2000, 2001; Grayman et al. 2004; Hickman 1999) have contemplated the use of distribution system models to better understand contaminant transport in a drinking WDS and the resulting public health exposures and consequences. Nilsson et al. (2005) simulated a deliberate biochemical assault on a municipal drinking WDS to demonstrate an effective method to characterize potential consumer exposure to contaminants and evaluate system vulnerabilities. Linking a novel stochastic water-use simulator (PRPsym, a model for simulating stochastic water demands) with EPANET (Rossman 2000), Nilsson et al. (2005) generated empirical frequency distributions of mass dose loadings at select nodes in a typical WDS. Khanal et al. (2006) extended the work of Nilsson et al. (2005) by examining the sensitivity of network response to the variability in the location, timing, duration, and intensity of a contamination event.

PipelineNet is an EPANET-based software tool to investigate propagation of contamination in a distribution system and the resulting public health consequences (Bahadur et al. 2003). PipelineNet was developed by Science Applications International Corporation (SAIC) through funding from EPA to help protect the Winter Olympics in Salt Lake City, Utah, in 2002 from a possible intentional contamination event. PipelineNet was the first modeling and simulation software tool specifically designed to analyze the consequences from intentional contamination events. In 2004, Uber et al. (2004) used a “systems analysis” approach to assess the consequences from an intentional contamination event. Here “systems analysis” is characterized by an ensemble of contamination events, theoretically representing any service connection. Uber et al. (2004) developed an extension to EPANET that allowed the sequential simulation of contamination scenarios using...
a script approach. The script approach allowed the user to specify a mass injection rate, start and stop time for the contamination event, and the model node name where the injection would take place. The script approach also allowed the sequential running of EPANET simulations. The tool was used to simulate and model contaminant transport in three real, distribution system models (Uber et al. 2004). Using the consequence results from an ensemble of contamination events, a statistical analysis was performed to rank the possible contamination injection locations in the distribution system model based on their ability to cause the greatest downstream consequences.

The work of Uber et al. (2004) led to the development of the Threat Ensemble Vulnerability Assessment (TEVA) Research Program, which resulted in the development of the TEVA-Sensor Placement Optimization Tool (SPOT) (U.S. EPA 2013; Morley et al. 2007; Murray et al. 2004). Without specific intelligence information, it is difficult to predict how a terrorist group might sabotage a water system. Therefore, TEVA-SPOT provides the user with the capability to analyze a large number of possible threat scenarios to help determine the potential magnitude of possible consequences. TEVA-SPOT allows the user to create a threat ensemble, or a set of contamination scenarios, based on varying, for instance, the type of contaminant, the amount and concentration of the contaminant, and the location of the contaminant injection into the distribution system. System vulnerability can then be assessed based on the entire threat ensemble.

TEVA-SPOT incorporates a limited, probabilistic-based framework for analyzing the consequences of contamination events in drinking WDSs. Drinking water consumers can be exposed to contaminants from ingestion, inhalation of volatilized chemicals or particles, and/or dermal exposure. For consequences, TEVA-SPOT (graphical user interface version) provides the following capabilities:

- Simulate and model an ensemble of contamination events, e.g., all locations (nodes) in the model, in a distributed, computationally efficient manner making use of a computer’s multiple processing cores.
- Estimate consequences based on public health exposures, doses, and health effects (illnesses and fatalities) from ingestion of contaminated tap water. Public health consequences could include injuries, disease, illness, and deaths. TEVA-SPOT provides the probit dose response model with the input parameters of LD50 (median lethal dose) and beta slope factor (Holcomb et al. 1999).
- Estimate infrastructure contamination as the length of pipe contaminated or gallons of water contaminated.
- Define the ensemble of contamination event locations. Prescribed collections consisting of all nodes, nonzero demand nodes, utility facilities (e.g., tanks and pump stations), user-defined list, and a user-defined random selection of nodes based on number or percentage of nodes from either all nodes, nonzero demand nodes or by pipe diameter. TEVA-SPOT also has the capability of defining the list of contaminant release locations to be those upstream of user-defined critical locations (nodes).
Each scenario in the threat ensemble that is simulated (underlying simulation engine is EPANET) can include an assumption of first order contaminant decay of constituents. In 2011, TEVA-SPOT was upgraded to incorporate the capabilities of EPANET-MSX, i.e., fate and transport modeling of multiple dissolved constituents in distribution systems (Shang et al. 2008). This upgrade permits the modeling of reactions at the pipe wall and in the bulk flow given the specification of constituent reaction kinetics and products, thereby resulting in potentially more accurate estimates of human exposure and health risk. Stochastic modeling is limited to the probabilistic modeling of the timing and volume of tap water ingestion (Davis and Janke 2009). Contaminant water concentration results are collected in binary format, which is used in the optimal placement of sensor monitoring stations.

Given the computational difficulty of analyzing the threat ensemble of large or very large WDS models, research continues to investigate ways to minimize the computational burden associated with identifying the extreme high-consequence events. One example is the work of Perelman and Osfeld (2010) who propose an algorithm that would allow the efficient sampling of a subset of possible events in an effort to preferentially identify those of high consequence.

Needed research includes understanding the influence of model detail or skeletonization on estimating consequences. A better understanding is needed as to how operational or seasonal conditions influence the quantification of consequences given a contamination attack. Also, work is needed to better understand and predict how contaminants will interact with pipe walls, biofilms, and disinfectants. How important is the quality of the distribution system model in predicting consequences and the locations of high-consequence events? For example, could infrastructure information, i.e., using GIS information for a particular water system along with other publically available information, be used to create a hydraulic and water quality model that could be analyzed in TEVA-SPOT to “approximately” determine the consequences from an intentional contamination event? Finally, a better understanding and more precise quantification is needed about the influence of post-service connection piping detail for estimating consequences (Grayman et al. (2008), Janke et al. 2009).

### 2.7.2 Methodologies and Tools for Placement of Sensors

The best approach to mitigate possible consequences from water contamination events involve “early” or advance warning systems (Brosnan 1999). An American Society of Civil Engineer’s study in 2004 provided an early, comprehensive discussion of early warning systems design, deployment and operation. This broad-based report discussed the problem of water contamination with respect to (1) rationale for online monitoring and system design basics, (2) identifying detection instruments for potential threat contaminants, (3) selection and placement of instruments, (4) data analysis and use of distribution system models, (5)
communication systems requirements, (6) response to contamination events, (7) interfacing with existing surveillance systems, operations, maintenance, and upgrades, and (8) exercising the system (ASCE 2004). Roberson and Morley (2005) helped to focus the discussion of CWS design and implementation in a practical direction. The report emphasizes that detection of contamination in order to provide treatment and response is most likely the best that can be done considering the “a myriad [of] limitations” facing water systems.

Research on methods to mitigate the impacts of contamination incidents converged, by 2006, on the concept of a CWS. The goal of a CWS is to detect contamination incidents early enough to allow for an effective response that minimizes further public health or economic impacts. Janke et al. (2006) showed that a CWS based on real-time monitors could be more effective at reducing public health impacts than sampling-based strategies and that response time was critical to reducing impacts. A CWS is defined as a proactive approach that uses advanced monitoring technologies and enhanced surveillance activities to collect, integrate, analyze, and communicate information to provide a timely warning of potential contamination incidents.

Many different approaches to contamination monitoring have been suggested, including using water quality sensors, composite or grab sampling, and placement of sensors. Since most monitoring programs will be budget constrained, cost is a critical factor in the design, deployment, and operation of a CWS. Since 2003, researchers have published numerous papers on sensor placement in drinking WDSs seeking to maximize the benefit of monitoring while minimizing the cost. The Battle of the Water Sensor Networks study compared 15 different approaches to the problem of sensor placement to support a CWS (Ostfeld et al. 2008). CWS design is typically focused just on the problem of optimizing sensor monitoring station placement within the distribution system. For a good synopsis of the research related to the problem of sensor placement optimization, we refer the reader to Hart and Murray (2010), which includes a thorough review of over ninety papers related to sensor placement for CWS design. In the following paragraphs, key points from Hart and Murray (2010) are provided.

Hart and Murray (2010) outline that sensor placement strategies can be broadly characterized by the technical approach and the type of computational approach used. Hart and Murray (2010) describe the following categories to reflect the important differences in various proposed sensor placement strategies:

- **Expert Opinion**: These methods rely on the experience and knowledge of experts. As Hart and Murray (2010) indicate, “expert opinion strategies are guided solely by human judgment.” Hart and Murray (2010) provide the following references for expert opinion-based approaches: Berry et al. (2005a, b) and Trachtman (2006). These papers consider sensor placements developed by experts with significant knowledge of WDSs. The experts described in these papers did not use a distribution system model to carefully analyze network dynamics. Instead, the experts used their experience to identify locations whose water quality is representative of water throughout the network. Therefore, an
The advantage of expert opinion-based approaches is that they do not necessarily require a distribution system model.

- Ranking Methods: Another approach is to incorporate user-defined information to rank potential sensor locations (Bahadur et al. 2003; Ghimire and Barkdoll 2006). In this approach, Hart and Murray (2010) indicate that a user provides “preference values for the properties of a ‘desirable’ sensor location, such as proximity to critical facilities.” These user-defined “preferences” can then be used to rank the desirability of particular locations for the placement of monitors. Further, Hart and Murray (2010) suggest that spatial information can then be integrated to ensure good coverage of the network. Generally, ranking-based approaches use a distribution system model.

- Optimization: Sensor placement can be performed with optimization methods that computationally search for a sensor layout that minimizes some objective, such as “contamination risks.” Hart and Murray (2010) describe this group of methods as those that use “a computational model to estimate the performance of a sensor configuration.” They provide the example, “a model might compute the expected impact of an ensemble of contamination incidents, given sensors placed at strategic locations.” Optimization methods typically rely on the use of a detailed distribution system model.

Hart and Murray (2010) identify seven steps common to most of the optimization-based sensor placement strategies: (1) defining the objective or “contamination risk” to minimize consequences (e.g., public health consequences), (2) describing the characteristics of sensors used in the CWS, (3) selecting the performance objective(s), (4) determining the optimization objective, (5) formulating the optimization model, (6) applying an appropriate optimization strategy, and (7) implementing the design. Published sensor placement research studies approach each step with varying degrees of complexity and with different optimization and simulation strategies. Hart and Murray (2010) divide the 90 papers they examined into nine groups according to how the authors addressed each step. In particular, Hart and Murray (2010) use five categories based on (a) use or nonuse of contaminant transport simulations to compute risk, (b) use of sensor failure model, (c) consideration of multiple design objectives during optimization, (d) type of optimization objective, and (e) whether data uncertainties were modeled. Unfortunately, many smaller water utilities do not possess a sufficiently detailed or accurate distribution system model that would support using an optimization-based approach for sensor placement.

EPA’s TEVA-SPOT software is the only open-source program the authors are aware of that assesses the consequences of contamination events and then uses the quantitative consequence results to optimally place sensors in the design of a CWS. TEVA-SPOT is available in two software applications: the command line, toolkit version, and the graphical user interface version. The command line, toolkit version is meant for academic researchers and software developers (U.S. EPA 2013). The graphical user interface version provides an easy-to-use interface and functionality to make use of a computer’s multicore processing capabilities for
analyzing large WDS models (U.S. EPA 2013). The TEVA-SPOT software applications were developed by the EPA’s Threat Ensemble Vulnerability Assessment (TEVA) Research Program composed of researchers from EPA, University of Cincinnati, Argonne National Laboratory, and Sandia National Laboratories.

Utilities can consider a number of possible goals for an online sensor system such as minimizing public exposure to contaminants, the spatial extent of (pipe) contamination, detection time, or costs. Some objectives may conflict with others, making it difficult to identify a single best sensor network design. Quantifying a sensor placement’s performance with respect to these goals allows some comparison of competing placements. TEVA-SPOT can optimize with respect to a primary objective, and also consider one or more secondary objectives. TEVA-SPOT provides a regret analysis operation mode to allow the user to analyze multiple sensor placement designs with respect to a range of threats. The regret analysis mode allows the user to determine how well a sensor network design performs when confronted with a threat or objective that is different from that used in its design (Davis et al. 2013). There are many practical constraints and costs faced by water utilities that cannot be easily modeled (Murray et al. 2008, 2009). Designing a CWS is not a matter of performing a simple optimization analysis (Murray et al. 2008, 2009). Instead, the design process is better described by a multiobjective problem that requires informed decision making, using optimization tools to identify possible sensor network designs that work well under different assumptions and for different objectives (Murray et al. 2008, 2009; U.S. EPA 2009). Ultimately, water utilities must weigh the costs and benefits of different designs and understand the significant public health and cost tradeoffs (Murray et al. 2008, 2009; U.S. EPA 2009).

The use of TEVA-SPOT for CWS design is composed of a “modeling process” and a “decision-making process” that employs optimization (Murray et al. 2008; U.S. EPA 2009). The TEVA-SPOT modeling process includes creating or utilizing an EPANET-based network model for hydraulic and water quality analysis, describing sensor characteristics, defining the contamination threats, selecting performance measures, estimating range of utility response times following the detection of a contamination incident, and identifying a set of potential sensor locations (Murray et al. 2008; U.S. EPA 2009). The TEVA-SPOT decision-making process involves applying an optimization method and evaluating sensor placements (Murray et al. 2008; U.S. EPA 2009). The overall process is refined by using TEVA-SPOT to perform regret analyses, analyzing tradeoffs, and comparing preferred designs to account for modeling and data uncertainties (Murray et al. 2008; U.S. EPA 2009; Davis et al. 2013).

Most of the research literature focuses on new or improved sensor placement optimization methods. Little research has been devoted to real utility applications. Some examples of real utility applications include the work by Skadsen et al. (2008) and Davis et al. (2013). Davis et al. (2013) analyze the robustness of sensor placement designs to changed conditions in 11 real and diverse water systems. Their work shows how more robust designs can be achieved by using a high
toxicity contaminant, a mass injection rate as high as reasonably feasible, and a design objective that seeks to minimize average consequences (Davis et al. 2013).

### 2.7.3 Water Quality Sensors and Contamination Event Detection

The use of water quality sensors to detect contamination was conceived as a means to provide broad contaminant coverage in the design of early warning contamination systems. It was recognized early that it was not technically feasible to design an early warning contamination system capable of accurately detecting the plethora of contaminants that could be used to contaminate a drinking water supply/distribution system and to cause public health consequences. Additionally, it was recognized that any technology identified for contamination detection would likely need to be deployed at many locations given the large spatial extent of WDSs. Therefore, any suitable technology would need to be economical for large-scale deployment within a distribution system. As a result, many researchers have focused their efforts on identifying online sensor technologies that could be used to detect anomalous changes in the baseline water quality. Once an anomaly is detected and the water utility operator is alerted, further actions (e.g., grab sampling and analysis) could be undertaken by system personnel to identify and quantify the contaminant whenever possible. Additional discussion of these issues can be found in U.S. EPA (2005).

Research associated with using water quality sensors in contamination event detection systems has been focused in two areas: (1) water quality sensor testing in the laboratory or in laboratory-based distribution system simulators (DSS) to determine water quality sensor response to specific contaminants and (2) statistical algorithm development to decipher anomalous water quality sensor response due to contamination as compared to normal operations. EPA funded the development of the open-source event detection system (EDS), called CANARY, through Sandia National Laboratories. CANARY is available for download at: (https://software.sandia.gov/trac/canary) (U.S. EPA). Hach Corporation developed the Guardian Blue early warning system to detect, alert, and classify a wide variety of threat contaminants in drinking WDSs (Kroll 2006).

Two principal groups have been involved with water quality sensor testing. EPA researchers at the EPA’s Test and Evaluation Center in Cincinnati, Ohio and researchers in the sensor industry such as the Hach Corporation in Loveland, Colorado (Kroll 2006). In 2005, EPA published a state of the technology review outlining the technologies and techniques for monitoring and evaluating drinking water quality in the context of early warning systems (U.S. EPA 2005).

Hall et al. (2007) and Hall and Szabo (2010) conducted an in-depth evaluation of how changes in water quality parameters associated with real-time sensors can be used to potentially indicate the presence of contamination. The sensors
investigated were off-the-shelf commercial products designed to monitor standard drinking water parameters such as pH, free chlorine, ORP, dissolved oxygen, specific conductance, turbidity, TOC, chloride, ammonia, and nitrate. Sensors were mounted within a re-circulating pipe loop and challenged with contaminants including secondary effluent from a wastewater treatment plant, potassium ferri-cyanide, a malathion insecticidal formulation, a glyphosate herbicidal formulation, nicotine, arsenic trioxide, aldicarb, and *Escherichia coli* K-12 strain with growth media (Hall et al. 2007 and Hall and Szabo 2010). Overall, the sensors that responded to the most contaminants were free chlorine, TOC, ORP, specific conductance, and chloride. It is important to recognize that the characteristics of the re-circulating, pipe loop distribution system used in the investigation likely significantly influenced the results.

Actual distribution system waters are observed to have much greater variability in their water quality parameters than what could easily be tested in a simple pipe loop configuration. However, Hall et al. (2007) and Hall and Szabo (2010) point out that no single water quality sensor responded to all of the contaminants used in the study, yet some sensors responded to a greater number of contaminants than did others. Hall and Szabo (2010) describes water quality sensor test results from a single pass pipe in addition to a recirculating loop. Hall and Szabo (2010) indicate that detecting contamination in a single pass pipe is more challenging. When used in contamination event detection, it is not only the absolute magnitude of the change that is important, but also the magnitude relative to the size and fluctuations in the baseline along with the slope of the change (i.e., to determine whether the changes occur over several hours or several minutes). Thus, the quantitative evaluation makes use of signal-to-noise principles, which is difficult to generalize and is location-specific. The sensors that responded to a larger number of contaminants were specific conductivity, TOC, free chlorine, chloride, and ORP. The chlorine sensors appeared to respond to all the contaminants studied. However, it is important to recognize that some potential contaminants do not react significantly with chlorine. Hall et al. (2007) and Hall and Szabo (2010) indicate that TOC responded to all the organic (carbon-containing) compounds. The TOC monitor, however, has a much higher capital cost when compared with other sensors (Hall et al. 2007, Hall and Szabo 2010). The calibration requirements for the sensors in these systems range from weekly to monthly (Hall et al. 2007, Hall and Szabo 2010). Hall and Szabo (2010) estimate that a multiparameter monitoring station could have reagent and maintenance costs of several hundred dollars per month.

Contamination event detection in a drinking WDS is a case of examining a set of noisy signals in order to detect events having a low probability of occurrence and yet only appear as very subtle deviations from typical background signals. In these situations, the required sensitivity of the monitoring algorithm and overlap in the background and event signal signatures will lead to false alarms in the event detection (Rizak and Hrudey 2006). Testing of EDS methods has focused on baseline water quality monitoring to distinguish between valid alerts (alerts resulting from unusual water quality in the distribution system) and invalid alerts (alerts that are unrelated to unusual water quality) and simulated testing. Simulated
testing involves using modeling and simulation to create a contamination event within a SCADA derived background water quality dataset and then determine if the EDS can detect the event.

As a part of the WSi Pilot Program, water quality sensors have been deployed and evaluated at several of the pilot cities as a component of a CWS. Some operational experience has been gained to date from these deployments related to water quality sensor performance and operation as part of an online CWS (Allgeier et al. 2008). Allgeier et al. (2008) reviewed the first year of operation for the Cincinnati Pilot’s online water quality CWS. For the Cincinnati Pilot, the CANARY EDS was used to determine whether a given water quality sensor response represented a changed water quality condition and, if so, provide a corresponding alert. Setting an alert threshold sufficiently high will likely not only eliminate the majority of false alarms but also increase the risk of not detecting a contamination event. Allgeier et al. (2008) report that, on average, 3.7 alarms are generated per day across the network of 17 monitoring stations (15 are in the distribution system and 2 are located at the treatment plants). They note that the most common causes of alarms during the baseline operations period consist of “operational changes which resulted in changing water quality and separately, unrelated to operations, sensor errors or malfunctions” (Allgeier et al. 2008). The authors question whether the numbers of false alarms are too high in order for the monitoring system to be sustainable (Allgeier et al. 2008). Later, in 2011, the authors report in more detail on the results of the Cincinnati Pilot’s performance using CANARY (Allgeier et al. 2011). In this study, the authors report that 92 % of the alerts were invalid, with 8 % considered valid. Allgeier et al. indicate that valid alerts consisted of (1) unusual plant conditions, (2) process change at the treatment plant, (3) maintenance or repair activities in the distribution system, (4) main breaks, or (5) verified water quality anomaly with unknown cause (Allgeier et al. 2011).

In the 2011 study, Allgeier et al. (2011) also use modeling and simulation based testing to examine the performance of CANARY. Using the Cincinnati Pilot field data as the basis for a modeling study, 1,588 simulated events are added to the water quality signals from the 15 monitoring stations within the distribution system, and run through the CANARY software (Allgeier et al. 2011). The simulated events represented water quality responses to 17 contaminants. Simulated events were created using laboratory data and EPANET-based hydraulic model simulations. Their “total scenario” detection rate, known as “true positives”, for the simulated events was 40 %, leaving their false negative rate reported to be 60 % (Allgeier et al. 2011). They note that while only 40 % of the simulated contamination incidents were detected, those scenarios not detected typically represented low consequences (Allgeier et al. 2011).

Most of the research data sets used in the development and testing of EDSs have been relatively stable and do not exhibit significant water quality changes associated with changes in network operations. In cases where the water quality is strongly influenced by changes in utility operations, new approaches are likely needed to recognize the impact of these changes water quality and integrate operational data streams into the online event detection system approach. Potential
opportunities to improve event detection in the highly variable water quality conditions of actual systems could include methods to recognize the “recurring patterns in multivariate data streams that are associated with operational changes” (Vugrin et al. 2009) and “direct integration of informative combinations of operational signals to temporarily decrease event detection sensitivity during periods of operational change” (Hart et al. 2010).

To date, EDS analyses have been focused on event detection at each monitoring station independently of observations occurring at other monitoring stations within the distribution network. As utilities continue to add monitoring stations within distribution networks, the concept of “distributed detection,” where information from multiple monitoring stations is combined in real time to provide an integrated detection capability, will likely become possible. Koch and McKenna (2011) propose an approach for combining data from multiple locations to reduce false background alarms. Recent development and testing of an approach to distributed detection has shown that integration of EDS results across a network can significantly reduce false positive detections and help to provide better estimates of a contaminant source location (Koch and McKenna 2011). However, determining a contaminant source location after release is an inherently difficult problem and is discussed in the following paragraphs.

Water quality sensors have been demonstrated to be effective in identifying a change in water quality conditions. Although it is not necessarily a contamination event, the change provides the impetus for additional investigation or perhaps target sampling. What is still needed is ability to connect sensors in a distributed network and integrate the information obtained with a real-time understanding of system hydraulics and water quality to leverage sensor detection information from multiple sites. Leveraging water quality sensor networks for operational and management benefits, i.e., those beyond security, are needed in order to better justify the high capital cost of sensor deployment and operations and maintenance (O&M) for maintenance. Evaluating such connected and distributed networks of water quality sensors for their ability to detect a wide range of contaminant types and their limits of detection is needed. It is probably fair to say, what has been done thus far has largely been illustrative, i.e., more rigorous deployment and testing is needed.

2.7.4 Responding to Contamination Events

Transport of contamination in a drinking WDS to unsuspecting customers can be quick, generally as fast as a few hours, depending on the system. The resulting public health and economic consequences as discussed can be significant. The response time of a water utility and its community to a water contamination event are dependent on the capability of their CWS to identify the contamination event quickly and then implement the necessary procedures to minimize public health consequences and the spread of contamination. As discussed in the previous
section, considerable uncertainties and needed research underlie the performance needed of a CWS to detect a contamination event in sufficient time for the utility and community to properly respond. Even with a rapid notification of the contamination event, an accurate and timely understanding of contaminant transport is needed to properly execute response actions that are specific to the contamination event and that effectively aid in reducing public health and economic consequences. For instance, it is easy to recognize that commensurate with effective and timely contamination event notification is the need for the near immediate identification of the source location of the contamination. With an accurate and timely identification of the contamination source location, response tools could, for instance, dictate which valves should be immediately closed to contain the contamination, or which fire hydrants should be opened to flush quickly and efficiently rid the system of contamination. The underlying critical component needed to support these needs, i.e., accurate and timely CWS-based detection, contamination source identification, and real-time response, is a continuous, real-time understanding of system operations or a real-time model.

Research related to the development of methodologies and tools for responding to contamination events have largely been focused in four broad areas. First, methods to identify the contamination event and initiate response actions quickly. The problem is being able to distinguish a contamination event from normal operations. Second, research to design monitoring networks and methods to identify the location of the source of the contamination. Third, research to develop algorithmic methods and tools to allow the optimal implementation of containment (e.g., valve closure) and recovery actions (e.g., fire hydrant flushing) to reduce public health consequences and the extent of contamination. Fourth, research to link an infrastructure model with SCADA data to provide a continuous, real-time understanding, i.e., model, of system operations.

The effectiveness of any response strategy depends largely on the length of time needed to deploy the necessary actions to stop public health consequences. Response delay time can be defined as the time period from the first uncertain detection to the cessation of any additional public health consequences. Numerous researchers have examined the influence of response time on the magnitude of public health consequences (Janke et al. 2006; Skadsen et al. 2008; Murray et al. 2008) and showed that the effectiveness of a CWS to reduce public health exposures can decrease by 50% or more when response delay increases from 12 to 48 h. Murray et al. (2008) show that the performance of a CWS can decrease substantially (as much as 70%) when the response delay time is increased from 6 to 24 h. It is hard to imagine how response could be initiated in sufficient time without a continuous, real-time understanding of system flows and chemical (water quality) transport.

Bristow and Brumbelow (2006) examine the “temporal and procedural space” between the detection of anomalous water quality event to the response decision(s) which result in the cessation of individuals ingesting contaminated tap water. This includes the “process by which decision-makers realize and affirm contamination and activate the initial phases of an emergency response plan.” Bristow and
Brumbelow (2006) show that the cumulative time required to detect the contamination event, perform emergency response, and address the “compliance process” can take a considerable amount of time, generally on the order of days (Bristow and Brumbelow 2006). They also show that the “first three phases of the response process—transmission of water quality parameters, verification of water contamination, and drafting of warning messages—are the most significant sources of delay” (Bristow and Brumbelow 2006).

Many important aspects of a utility’s response during contamination events could be derived from a system’s water quality monitoring. In a WDS contamination scenario, water quality monitoring results would provide crucial information such as confirmation of a contamination event, the nature of the event, and the extent of contamination, all of which are critical when rapidly planning and executing a mitigating response. Water quality monitoring data could also be used to determine the source of the contamination attack, which is also known as a contamination source inversion problem. Inverse problems are computationally difficult to solve by their nature. Their solution can be computationally demanding, making them difficult to solve in a reasonable amount of time. Observational data needed for their solution is generally in short supply making it difficult to uniquely identify sources of contamination in the network. If the data is of poor quality and the solution procedure is sensitive to error and noise it may be impossible to solve the problem altogether.

Inverse problems are difficult to solve for several reasons including rank deficiency and ill-posedness. “Ill-posedness” means there is no unique solution or stability of solutions. Rank deficiency refers to data that is insufficient to meet the information necessary for the mathematical model to generate a unique or usable solution. Solution uniqueness and stability problems can result in a computational tractability problem, which means the problem cannot be solved in a reasonable amount of time. Some of these issues are a function of monitoring design which dictates the amount and quality of information available to formulate and solve the problem. Model and measurement errors can be an important factor contributing to identification uncertainties. Generally, source inversion problems are under-determined, i.e., not solvable, because the data is too limited and there are more unknown variables than data or observations. This leads to an inverse problem description where there are an infinite number of solutions and inherent nonuniqueness.

Work on source inversion started after research on monitoring system design was well under way. This early work resulted in the development of novel solution procedures not regularly applied to inverse problems. Preis and Ostfeld (2006) developed model tree linear programming method for solution of the source inversion problem. Guan et al. (2006) developed a solution for the source identification problem using a predictor corrector algorithm.

Solutions techniques that use simulation models that advance forward through time represent a conventional approach for solving inverse problems. Laird et al. (2005), however, formulated the source inversion problem by developing an origin tracking algorithm that facilitated the embedding of ordinary differential equations
ODEs) describing water quality transport as constraints directly within a quadratic programming (QP) problem. The approach was highly efficient and scalable; however, the solutions identified were frequently not unique. Employing a somewhat more conventional approach DiCristo and Leopardi (2008) developed a two step procedure. First, a transport pathway analysis is performed that identifies a feasible subset of potential contamination source nodes. Then using the reduced set of feasible sources a more compact discrete linear inverse problem was solved.

Solution nonuniqueness describes a condition when there are many solutions to an inverse problem that are indistinguishable from one another. This makes the problem difficult to solve because the true solution can not be identified. Solution nonuniqueness occurs when the potential sources in a network outnumber the data observations available for their identification. Laird et al. (2006) extended their previous work to address solution nonuniqueness. They develop a two phase solution approach where the QP is solved then the solution subspace identified is searched using mixed integer QP for distinct injections giving rise to the solution of the original NLP. Extending Laird’s work, Wong et al. (2010) and Mann et al. (2012) formulated the source inversion problem considering discrete (positive/negative) grab samples. The problem was solved as a mixed integer linear program (MILP) problem. The procedure developed is adaptive; in that, it can accommodate additional sampling cycles to improve the accuracy of the identification. An origin tracking algorithm is utilized in the formulation of the MILP to effectively reduce problem size.

Solving inverse problems using simulation models running in reverse time is typically not possible because the numerical solutions become unstable. Numerical results become unstable when errors and noise become amplified within the solution algorithm. Generally, conventional numerical solution techniques do not work in reverse time. One of the interesting features of WDSs is the ability to develop stable techniques for solution in reverse time. Starting from the point of observation a contaminant can be transported back in time flowing past potential source locations along the way. DeSanctis et al. (2009) uses a particle back tracking algorithm and binary sensor data to identify potential sources along contaminant transport pathways assuming known network hydraulics. Neupauer et al. (2009) developed a backwards particle tracking method in a probabilistic framework. The algorithm developed treats observation nodes as instantaneous sources of probability which are transported backwards in time to obtain probability density functions (PDFs) of possible prior times when a particle was at an up gradient node. Back tracking time PDFs are conditioned with sensor data to determine likely source node locations and contaminant release times. The example assumes steady state hydraulics, but the method described is flexible and can be expanded to support dynamic hydraulics as well as other sources of uncertainty. Tao et al. (2012) developed a probabilistic treatment of DeSanctis backtracking based solution procedure using consumer complaints in place of binary sensor observations.

Formulating inversion problems using a probabilistic framework is another approach for addressing nonuniqueness by assigning each potential contaminant
source a likelihood of being the true source. Propato et al. (2010) formulated the source inversion problem using a linear description of the input output dynamics of a WDS. The problem is then solved using minimum relative entropy, an entropic-based Bayesian inversion technique. (Liu et al. 2011a) used logistical regression to formulate the source inversion problem. The method required a large number of source realizations to be simulated offline to estimate likelihood model coefficients. The method is flexible as measurement errors and uncertainty can be incorporated into the coefficient calculations. The solutions, however, were better suited to enumerating the set of nonunique source locations than for identifying the true source location.

The global search characteristics of evolutionary algorithms are well suited to solution of nonunique source identification problems. Evolutionary algorithms are coupled with forward simulation models for objective and constraint evaluation. A major shortcoming of this approach, however, is computational tractability. Hundreds of thousands, if not millions, of forward model evaluations may be required to solve a typical inverse problem. Preis and Ostfeld (2007) formulated the source characterization problem as a least squares minimization problem solved using a standard genetic algorithm (GA). A sensitivity analysis was performed to characterize the robustness and accuracy of the proposed solution procedure. The authors noted the substantial computational cost of the procedure. Building on their previous work, Preis and Ostfeld (2008) described a technique for storing water quality transport simulation results in an offline matrix structure to speed up objective function evaluation. The flexibility of their solution approach allowed them to explore the affect of imperfect sensors on solution performance and response time.

Some researchers exploring evolutionary algorithms resorted to distributed computing approaches to improve computational tractability. Zechman and Ranjithan (2009) solved the source identification problem using a hybrid procedure that combined evolutionary strategies with gene encoding techniques found in genetic programming. A binary tree data structure is used to encode variable length contaminant mass loading schedules. Mutation operators modify contaminant release characteristics such as location, start time, release schedule, and schedule duration over the course of the search. The evolutionary strategy, a type of evolutionary algorithm, and encoding chosen allow the solution procedure to flexibly adapt to the uncertainties associated with the source characterization problem. Kumar et al. (2012) formulated the source inversion problem using low resolution sensor data and solved it using an evolutionary algorithm that simultaneously searches objective space for solutions that best explain observed data and decision space to characterize solution nonuniqueness.

A common assumption of early work on the source inversion problem was that of known hydraulics. This is a significant and limiting assumption reflecting the best understanding of the problem available at the time. That assumption can be relaxed somewhat by describing the uncertainties associated with the hydraulic state of the system. Vankayala et al. (2009) used Gaussian and auto regressive models to describe demand uncertainties. The source identification problem is
formulated using an approach to minimize the maximum prediction error objective and then solve the resulting problem with stochastic search procedures. A stochastic demand GA, a different type of evolutionary algorithm, was used to solve the problem for each stochastic demand realization. Many realizations are simulated to build up a statistically valid characterization of the results. This approach can be contrasted with a Noisy GA, which uses a different demand realization for each generation of the GA search and computes fitness of an individual as an average over the set of realizations simulated. Both techniques performed well, but the noisy GA identified the contaminant source with a higher probability. Wang and Harrison (2013) formulated the source characterization with stochastic demands as a Bayesian probabilistic inverse problem. A unique Marko chain Monte Carlo (MCMC) algorithm was developed to address the discrete nature of the PDF associated with transport processes in the WDS.

Rather than assume that system hydraulics or a statistical description of them is available, they can become another inversion problem where system demands are estimated given pressure, flow, and boundary measurements. Preis and Ostfeld (2011) formulated a coupled inverse problem that seeks to simultaneously characterize hydraulic regime and contaminant releases given limited and low resolution data. They extended their previous work by considering hydraulic uncertainty and low resolution sensor data. The approach they described uses a Monte Carlo technique to characterize nodal demands to generate a hydraulics regime that best reflects limited hydraulic observations. The formulation considers a fixed set of observations gathered over an arbitrary length of time.

Operational source inversion requires a solution in real time. (Liu et al. 2010b) formulated the source inversion problem using streaming data from a fixed set of sensors located in the WDS. The adaptive dynamic optimization procedure they developed considers time varying streams of sensed data. Multiple populations are used to simultaneously search objective space as observation information is updated over time and search decision space for maximally different explanations of the observations. Liu et al. (2012) extended their hybrid search algorithm using logistical regression as a pre-screening step to reduce the search space by eliminating unlikely sources from the problem. A local search technique (pattern move) was also incorporated as a selection operator into the evolutionary strategy-based dynamic optimization procedure to improve the algorithms convergence characteristics.

Haxton (formerly Baranowski) (Baranowski et al. 2008) performed a case study analysis at Ann Arbor to identify and evaluate potential response actions following a contamination event. Working closely with the water utility representatives, the authors identified “practical bounds” to determine feasible response strategies and evaluated them using modeling and simulation. A hydraulic response tool was used to identify valve closure locations and hydrant flushing locations and rates to best minimize the extent of pipe contamination. The case study assumed the source or location of the contamination event was known. Valve closure consisted of isolating the tank directly downstream of the contamination event. While optimal hydrant flushing somewhat reduced the extent of pipe contamination, isolation of
the tank proved to be most effective at reducing the spread of contamination (Baranowski et al. 2008). The analysis relied on the identification of the contamination source location. Without the identification of the contamination source location, it would not have been possible to isolate the tank.

Haxton et al. (2012) use an updated modeling and simulation approach to again identify and examine effective hydrant flushing locations but now to minimize public health impacts in addition to the extent of pipe contamination used in the earlier case study at Ann Arbor. Using a comparatively simple distribution system model, Haxton et al. (2012) compare algorithm-based optimized response actions against enumeration-based response actions in the development of a suite of WS tools. Together the studies point to the difficulties (computationally difficult for small models possibly insurmountable for large models) and problems (may spread rather than reduce contamination) with an a priori selection of the “best” hydrant flushing and valve closure locations based modeling and simulation studies (Haxton et al. 2012).

Effectively monitoring for, detecting, and responding to contamination events, unintentional or intentional, will require an integration of infrastructure modeling, data, and information on system operations. The fusion of operational (SCADA) data with infrastructure-aware predictive models is not new to the water community. WDS models are being used increasingly in the planning and decision-making process for drinking water utilities in the USA. These models have and are being used for predicting water quality, sensor location and for assessing the impacts of disaster. In addition, many medium to large unities in the USA recognize the need to incorporate SCADA data systems into infrastructure model and use them both more effectively in their day-to-day operations (Janke et al. 2011). However, institutional constraints, e.g., lack of resources, organization structure, and historical (outdated) operational procedures, hamper the adoption of real-time modeling capabilities at many water utilities in the USA. Typically utility operations are organizationally separated from engineering and modeling activities (Janke et al. 2011). Operations personnel often do not believe in model predictions and generally operate the WDS in a procedural manner without regard to optimization. Enormous quantities of SCADA data are continuously collected at many water utilities but never actually used. WDSs are generally operated without the employment of real-time analytical (e.g., hydraulic or water quality) data to optimally manage distribution system operations, i.e., to reduce energy costs, to manage disinfectant residual, or to identify pipe leaks and water losses. Engineering and modeling staff has a difficult time convincing operations staff to believe in and use their predictive models when they themselves are often not convinced. Convincing either side to explore distribution system optimization will require the fusion of SCADA data with up-to-date infrastructure models.

The need for real-time modeling and operational control is not new. Commercial companies purporting to offer real-time modeling capabilities have been around since early 2000s. Generally, commercial real-time modeling applications follow one of two approaches: (1) “software as a service” provider or (2) off-the-shelf real-time modeling application, which is typically an infrastructure and GIS
centered software tool based off the particular water utilities existing application. Generally, the “software-to-service” providers do not offer a ready, off-the-shelf application for water utilities to install to incorporate real-time modeling into their decision making and management activities. The commercial off-the-shelf real-time modeling applications by design offer such tools, but, generally, the products are new and untested. There are few documented real-time modeling case studies in the literature and fewer still that have definitively substantiated the benefits and value of real-time modeling.

Hatchett et al. (2011) discuss integration of data with a network hydraulic model. Specifically, data available from interconnected and open information architectures, such as from a SCADA system, are fused within a real-time hydraulic modeling framework. The authors describe efforts at field-testing such a system with a partnering water utility. It is based on a “Real-Time Extension” to EPANET (so-named EPANET-RTX). The software libraries seek to connect a model’s controls, demands, and boundary conditions to real-time SCADA data, and provide a visual output of the model’s predictions along with statistical accuracy metrics. In addition to being able to analyze error statistics and data time series, the hydraulic and water quality model is adjustable to the hydraulic model’s parameters dynamically and for exporting historical scenarios (as EPANET input files) for offline analysis.

Hatchett et al. (2011) describe the steps taken to field-validate critical model details and implement real-time simulation. The research seeks to document the utility’s experience and provides recommendations for future development and deployment of the software tools (Janke et al. 2011). The authors believe that the development of the EPANET-RTX platform and pilot-scale installation is a first step in the path to creating an extensible and open-source framework for real-time hydraulic and water quality modeling (Hatchett et al. 2011; Janke et al. 2011). Clearly, many technical issues remain which provide the impetus for further research. Some of the major technical issues include: (1) demand estimation for reliable forecasting (2) data assimilation (e.g., SCADA data cleanup and filtering and modeling data processing), and (3) information technology communication and security (i.e., hardware, software, and network connectivity issues and concerns). Advances in infrastructure hydraulic monitoring technologies (e.g., flow monitoring) and automated meter reading should provide assistance in addressing these issues.

2.8 Summary and Conclusions

A reliable source of clean, potable water is fundamental to a community’s health and viability. Water is the most essential commodity, one that is used every day, by every person in the USA and around the world. Protecting water supply and infrastructure is central to maintaining the water commodity for a community and its survival. Most water supply systems in the USA consist of a water source(s),
treatment facility, and distribution system. The distribution system infrastructure is typically the biggest asset and liability of a water utility. WDS infrastructure is necessarily complex in part because of the required redundancy needed to ensure clean and reliable tap water for every customer every day. WDSs are also complex because of the manner in which the infrastructure have been built, i.e., in parallel with cities and communities growing and expanding to meet the needs of the people they support. Water supply infrastructure in the USA is one of the oldest infrastructures. With this complex and aging infrastructure are numerous potential threats and risks.

Water systems are vulnerable to unintentional and intentional threats. Unintentional threats can occur from natural causes (e.g., droughts, floods, and earthquakes), accidents, or equipment failures, e.g., pipe breaks. Accidents or equipment failures can lead to utility disruptions and customer loss of service or even result in water contamination causing public health exposures, illness, disease, or even death. Cases of accidental contamination in water systems are numerous with illnesses sometimes reaching the many thousands and deaths numbering in double figures.

Intentional threats can include physical acts of sabotage, cyber attack of information or SCADA systems, or contamination. Water systems are vulnerable to such intentional threats due to their physical size, number of physical attributes (e.g., reservoirs, tanks, and pump stations), and sheer number of open access points for sabotage or contamination entry. Here the authors examined numerous published papers, reports, and studies indicating that post treatment storage facilities and the distribution system represent the most vulnerable components of a water system.

Haimes and Horowitz’s (2004) definition of intentional threat is an “adversarial intent to cause harm or damage” and as modified by Willis et al. (2005) to include “intent” and “capability” of the perpetrators. Internal and external threats are discussed, with the observation that the “trusted insider” threat may represent the greatest concern because he or she may not only have the intent but also the knowledge and capability. A synopsis of research studies over the past 10–15 years is reviewed to discuss and describe intentional contamination threats in terms of approach, type of contaminant, and magnitude of possible consequences. The authors also describe possible countermeasures (i.e., physical, CWS, and cyber) which could be implemented by water utilities and communities to help protect and respond to physical and contamination threats.

Due to the magnitude of public health and economic consequences which could result from a contamination event, the consideration of online CWSs has become the focus of the water community. EPA began the WS Initiative pilot utility program to field test a five component conceptual model for a CWS at five large water utilities in the U.S. customer complaint surveillance, public health surveillance, and enhanced security monitoring are important components of the proposed CWS architecture. In terms of the earliest detection and concomitant response, the online contamination monitoring component promises the best opportunity to minimize the consequences of intentional contamination. However,
while many utilities implement some form of monitoring and surveillance activities few operate in a manner to meet the primary objective of a CWS – timely detection of the contamination incident. The reasons for this are many, e.g., technical difficulties, immature technologies, lack of resources, and institutional constraints. Effective online contamination monitoring (i.e., to ensure timely detection of contamination) must be integrated with routine monitoring and routine monitoring must be integrated with operations.

The authors review the state of research related to (1) development of methodologies and tools for assessing the consequences of water contamination events; (2) development of methodologies and tools for the optimal placement of sensors in a distribution system; (3) use of water quality sensors to detect contamination and function as part of an event detection system (EDS); and (4) development of methodologies and tools for responding to contamination events. Effectively monitoring for detecting and responding to contamination events, unintentional or intentional, will require an integration of real-time analytical (SCADA) data with infrastructure-aware predictive models.

Water systems, especially the distribution system, are vulnerable to unintentional and intentional threats. Water contamination threats likely represent the greatest threat to the water utilities and communities they serve, due to the possible significant public health, including loss of life, and economic consequences which could occur. Online contamination monitoring that is integrated with real-time operational control is likely the only approach which can promise early detection and potentially effective response. Effective response is, however, dependent on the timely identification of the contamination source location.

Acknowledgments The authors gratefully acknowledge the efforts and contributions of the peer reviewers and technical editor Marti Sinclair [contract GS35F4594G, TO1533] who helped to significantly improve the material presented here. The views expressed here are those of the authors and do not necessarily reflect the views or policies of EPA.

References


American Society of Civil Engineers (ASCE) (2004) Interim voluntary guidelines for designing an online contaminant monitoring system. American Society of Civil Engineers, Reston

Burrows WD, Renner SE (1999) Biological warfare agents as threats to potable water. Environ Health Perspect 107(12):975–984


Davis MJ, Janke R, Magnuson M (2013) A framework for estimating the adverse health effects of contamination events in water distribution systems and its application. Accepted Risk Analysis

Davis MJ, Janke R, Phillips C (2013a) Robustness of designs for drinking-water contamination warning systems under uncertain conditions. In preparation


Protection Agency uses operations research to reduce contamination risks in drinking water.
Interfaces 39(1):57–68


Securing Water and Wastewater Systems
Global Experiences
Clark, R.M.; Hakim, S. (Eds.)
2014, VIII, 398 p. 114 illus., 93 illus. in color., Hardcover
ISBN: 978-3-319-01091-5