Reliability Engineering and System Safety 179 (2018) 37–51

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Allocating countermeasures to defend water distribution systems against terrorist attack

Jacob Monroe, Elizabeth Ramsey, Emily Berglund*

Department of Civil, Construction, and Environmental Engineering, North Carolina State University, Raleigh, NC 27695, USA

ARTICLE INFO

Keywords:
Water supply security
Countermeasures
Contamination event
Police officers
Security equipment
Physical infrastructure network

ABSTRACT

Water distribution networks are critical infrastructure systems that are vulnerable to terrorist attack. Water utility management has the goal of protecting public health by allocating countermeasures, including security equipment and personnel, as a first line of defense. A malevolent actor may select an attack location, however, using a set of unknown priorities that include performance and susceptibility criteria. This research develops a multi-agent framework to simulate the attack and defense of a distribution system to analyze security resource allocation strategies for protecting against chemical contamination events. A single period attacker-defender game is simulated, in which an attacker seeks to contaminate a system node with high attack utility, and a group of defenders seeks to minimize the public health impact from intentional attack. Terrorist agent decisions are simulated using a multi-attribute utility function, and multiple cases are constructed to simulate alternative rankings of criteria. The water utility manager agent assigns security personnel and deterrent security equipment to nodes using one of three security resource allocation strategies. The agent-based modeling framework is applied to simulate attack and defense for a virtual municipality, D-town. Strategies are evaluated based on the number of consumers exposed to a critical dose when a contaminant is released.

1. Introduction

Water distribution systems convey potable water to a population of residential, commercial, and industrial users in urban areas [17]. A distribution system is a network of interconnected pipes, valves, pumps, tanks, and reservoirs, and can span an extensive geographic area to serve multiple municipalities. These characteristics increase the vulnerability of water networks, along with other critical supply networks such as electric power grids and industrial supply chains, to terrorist attacks. Malevolent sabotage may achieve damage to infrastructure components or injection of chemical contaminants or microorganisms, which result in adverse public health, economic, and social consequences [9,20,28]. An act of water terrorism is a probable threat, and history provides an account of many successful and unsuccessful attacks on water resource supply systems [13,15,18,21–23,28]. Reports from United States law enforcement and intelligence agencies provide evidence that water supply systems have been studied by extremist organizations for the purpose of contaminating water resources and crippling water distribution system infrastructure. For example, documents confiscated following the 2002 arrest of a Lebanese national in Seattle indicated that Al-Qaida members sought specific information on supervisory control and data acquisition (SCADA) systems in order to plan new attacks on American dams and water resource supply systems [15]. Newly emerging terrorist groups have posted international bulletins calling for an increase in lone wolf attacks by their followers in the west, including the disruption of physical infrastructure systems and municipal water supplies [3,46].

The bulk of research on water distribution system threat management has focused on developing secondary lines of defense, which include early warning systems, methods for identifying the source of a contaminant, and response actions [18]. These studies developed approaches for reducing the exposure of a population to chemical and biological contaminants that are released in the distribution system. Few studies have explored options and best management practices for implementing the first line of defense - a set of countermeasures to discourage, limit, or deny physical access to vulnerable points and reduce the occurrence of deliberate sabotage [18,43]. Managers can allocate countermeasures by selecting nodes in the network to place security personnel and security equipment.

The development of game theory and risk analysis have been used to identify effective risk management recommendations for allocating security resources in protecting infrastructure networks [10]. For example, Talarico et al. [40] simulate a dynamic game in which a defender

* Corresponding author.
E-mail addresses: jgmonroe@ncsu.edu (J. Monroe), evramsey@ncsu.edu (E. Ramsey), emily_berglund@ncsu.edu (E. Berglund).

https://doi.org/10.1016/j.ress.2018.02.014
Available online 12 February 2018
0951-8320/

allocates security resources and an attacker chooses a target to attack in a multi-modal chemical transportation network. Here, we develop a simulation approach to evaluate strategies for allocating countermeasures in a water distribution system. An agent-based modeling approach simulates the dynamics between attack and defense and takes a comprehensive approach to assessing the effects of choices made by attackers and defenders. Both the attacker agent and the defender agent use hydraulic information about a water distribution network to select locations. The attacker agent uses multi-attribute utility theory to prioritize objectives and select a node. The consequences of an attack are simulated using a hydraulic simulation that is coupled to an agent-based model of consumers to realistically simulate the number of exposures. This framework provides a new approach to simulate attack-defense dynamics and the effects of the presence of security personnel, flow directions within the water distribution network, and water use habits of a population of consumers on the performance of defensive strategies. The purpose of the framework is to provide insight and assessment about the protection that police coverage and security equipment allocation strategies can provide for a water distribution system that is susceptible to a malevolent chemical attack. Because the framework uses hydraulic simulation, engineering tools that are available to utilities, and multi-attribute utility functions to represent terrorist goals, it can be applied for a realistic utility to guide management decisions. Previous research (e.g., [24,29,39]) did not include realistic simulation to allow application for decision-making.

The framework is applied for a virtual municipality, D-Town, to demonstrate its use for evaluating management strategies. Strategies for placing security equipment are developed based on critical nodes and pressure zone management. In addition, a random roving strategy and a planned roving strategy are tested for simulating police officers. An attacker is simulated using a multi-attribute utility approach to select nodes for attack based on the performance and susceptibility of nodes. The attacker and defender agents are simulated to capture the real-time dynamics between an attacker and the presence of security personnel.

2. Countermeasures for water distribution systems

2.1. Hardening nodes

In allocating countermeasures, a small set of nodes should be selected among hundreds or thousands to be hardened through security equipment. Typically, utilities place security equipment at visual and accessible nodes, such as tanks and reservoirs [2]. Critical nodes in the distribution system can be identified based on the consequences of injection, which can be calculated as the number of constituents who consume a toxic dose after the injection of a harmful contaminant at a node. Hydraulic simulation can be used to model the propagation of a chemical contaminant through a distribution system and assess which nodes generate high consequences. The Threat Ensemble Vulnerability Assessment and Sensor Placement Optimization Tool (TEVA-SPOT) [30] computes impacts of contamination incidents, based on probabilistic consequence assessments and hydraulic simulation using EPANET (Rossman 2000). TEVA-SPOT was developed to design contamination warning systems and has been used in a range of water distribution system threat management applications, including evaluating utility response times, optimizing sensor network designs, and quantifying potential public health consequences over a range of possible scenarios [30,31]. TEVA-SPOT provides the capability to rank nodes in a network based on the potential number of consumer exposures for a set of contamination event, using contaminant and dose-response information. Node rankings can be used to place security equipment to harden critical nodes.

Another approach to identify critical nodes is through the use of information about pressures zones in a water distribution network. Water distribution systems are commonly sub-organized into pressure zones, which are individual service regions within a distribution system that have one or more supply sources (reservoirs, storage tanks, and pumping stations) to provide a constant hydraulic gradient throughout the zone. Managing a network through the design of pressure zones simplifies the maintenance of acceptable pressure differentials, reduces leaks, lowers pumping costs, and avoids over-pressurizing the network [12,25,36]. During a contamination event, pressure zones may be closed to isolate portions of the network and contain and subsequently flush a harmful chemical species. This may be used as an approach to avoid shutting down the entire system [33]. Pressure zones can create multiple hydraulic sub-systems, which can vary considerably in terms of consumer demand, number of connected nodes, average nodal attack utility, and potential for economic loss and social disruption following a contamination event.

The design and modification of pressure zones can be influenced by political boundaries, as each of these sub-sections can be located within or across different communities and townships. Some city water service boundaries extend well beyond the core city area into suburban locations, neighboring municipalities, and even unincorporated regions of land [8]. Within different pressure zones, there may be differences in the attitudes among community stakeholders, public officials, and water utility managers about the threat of a terrorist attack on the distribution network. Diverse management and social aspects can create difficulties in implementing a system-wide security allocation approach, especially considering a multifaceted utility financial support system and jurisdictional restrictions on the boundaries of multiple city law enforcement agencies. Water service utility systems that cover only a single city may also be subject to opposition from internal community leaders and law enforcement managers, who are influenced by inadequate funding and a difference in security objectives. Consequentially, security resource allocation systems can be based on pressure zone boundaries to simplify management. Additionally, for systems in which the majority of highly ranked nodes are located in one pressure zone, it may be advantageous to diversify the location of countermeasures across pressure zones, instead of placing all security measures in one pressure zone with high consequence potential. Highly ranked nodes within each pressure zone can be selected for placing security equipment.

2.2. Police roving

Water distribution systems may also be defended by police roving systems. The routine patrol officer assignment problem is different from other emergency service assignments because there are multiple systems to defend, including transportation and school systems, in addition to water infrastructure [1,41]. Research studies developed optimization approaches [1,6,19], agent-based modeling frameworks [14,16], and game theoretic approaches [41] to allocate police officers for traffic law enforcement. These modeling studies represent police officer patrol movement as a stochastic process, which accounts for the random nature of daily domestic and traffic violations. Patrol units are also instructed to move randomly so that adversaries cannot learn routes and plan accordingly. A simulation approach provided by game-theoretic concepts for police allocation uses a weighted randomization strategy. In this approach critical targets are assigned high weights so that they are visited more frequently than less critical targets [41]. While it is not the current practice to assign law enforcement officers to guard nodes of a water distribution network, this research assesses how effective this type of strategy could be in protecting public health.

2.3. Assessing countermeasures through simulation frameworks

Skolicki et al. [39] developed an evolutionary computation-based approach to evolve decisions of attackers and defenders in selecting nodes for attack and defense. Defenders and attackers select hydrants to guard and as locations for injecting contaminant, respectively, and actors learn improved strategies over many iterations of an evolutionary algorithm. Michaud and Apostoloakis [29] use multi-attribute utility theory to develop an approach to rank water distribution system components that

should be protected, based on vulnerability to malevolent threats. They do not use hydraulic simulation to assess the potential public health implications of protective strategies. Kroshl et al. [24] emphasize that good defensive strategies must consider the behavior of the adversary, even though that information may be incomplete or imperfect, and they develop an agent-based model to simulate attackers and defenders for a spatially distributed physical network.

The simulation framework developed here improves on previously conducted research to include modeling and information that would realistically be available to improve the decision-making strategies of both attackers and defenders. For example, the multi-attribute utility approach that was used to evaluate vulnerability of nodes [4,29] neglects information that attackers may use to update decisions based on observations of security equipment. This information is included in the attacker decision-making approach as formulated here. In addition, the approach developed here allows attackers to use hydraulic simulation and insider information about the flow directions and affected populations to select nodes. Previous research modeled utility managers as using a learning process to respond to attacks (as simulated by Skolicki et al. [39] and Kroshl et al. [24]). The framework that is developed here assumes that utility managers would use engineering judgment and hydraulic tools that are available to identify susceptible nodes, rather than learn response strategies over numerous failures.

3. Methods: agent-based modeling framework

An ABM framework is developed to simulate the dynamics of attack and defense of a water distribution system. ABM is a simulation approach that simulates the actions and interactions of multiple agents within a closed environment (Holland 1975; Miller and Page 2007). Agents select behaviors using a set of mathematical or logical rules in response to the actions of other agents and environmental conditions. Agents may be reactive and respond using predetermined rules. Alternatively, an agent may be active and select behaviors to maximize objectives, satisfy goals, or improve an individual fitness value. Collectively, a population of agents forms a complex system and generates unexpected emergent phenomena, as a result of interactions among agents.

A set of studies developed an ABM approach to simulate public health consequences of water contamination events. A hydraulic model was coupled with an ABM to simulate the number of consumers exposed to a contaminant in a water quality failure event [38,48]. Further studies assessed the risk associated with alternative bacterial contamination events [34], and Shafiee [37] simulated the number of consumers protected by mitigation strategies, including broadcasts through the news media, dissemination of warnings via siren vehicles, and hydrant flushing. Previously conducted research explored response strategies that would be implemented in response to mitigate an event in progress; the research presented here explores the defense of a network *in anticipation of an event* by hardening water network nodes through security measures. A terrorist and a utility manager are represented as agents, and the interactions of attack and defense strategies are simulated in a dynamic game. In addition, water consumers are simulated as agents to assess the public health impacts of a chemical attack (Fig. 1).

The attacker, defender, and police officer agents interact to affect the placement and success of a chemical attack. Defender agents place security equipment at specific nodes, which deter attackers from selecting those nodes for attack. Attacker and police officers interact directly: if a police officer is located at a node when the attacker places a contaminant, there is a 50% probability that the attack will be thwarted by the police officer. Consumer agents do not interact with the other human agents, but only with the water distribution system. Consumer agents ingest treated or contaminated water from the water distribution system and become ill. The details of all the agent interactions and behaviors are provided as follows.

3.1. Defender agent

A defender agent selects node hardening strategies and defense strategies. The defender agent represents a person with decision-making power, such as a city manager or a utility manager. Hardening strategies place security equipment, including cameras, lights, and empty police cars at nodes of the water distribution network. Defensive strategies are the strategies that are used by police officer agents to visit nodes. Nodes are simulated as access points that can be seen by the public. Within the water distribution model that is included in this framework, nodes represent an aggregated number of connections, including multiple houses (such as a neighborhood), manholes, and hydrants. Nodes represent a number of components that are accessible in public places and can be attacked, for example, by inducing backflow at hydrants, accessing valves, or accessing pipes through manholes.

3.1.1. Critical node ranking (TEVA-SPOT)

Nodes are ranked based on the effectiveness of that node, or the consequence of an attack that is initiated at that node. Nodes that are more likely to affect a higher number of people are prioritized for protection. (Nodes are equally prioritized for attack, as shown in the Section 3.3). The Threat Ensemble Vulnerability Assessment and Sensor Placement Optimization Tool (TEVA-SPOT) [5,42] is used to identify critical nodes. TEVA-SPOT simulates an attack at each node in the distribution system and simulates consequences as a measure that is used to rank nodes. Because the agent uses the rank of nodes to make decisions about selecting nodes to defend, it is the relative number, rather than the exact number of exposures that is critical for prioritizing nodes. The number of critical nodes is determined as a percentage of total nodes in the network, and the highest ranking nodes are identified as critical nodes.

3.1.2. Defense strategies

3.1.2.1. Random defense strategy. The random defense strategy assigns police officer agents to randomly rove all nodes within the distribution system for defensive cover. This strategy does not prioritize water infrastructure protection above other law enforcement priorities.

3.1.2.2. Critical node defense strategy. A defense strategy is developed to assign security personnel to visit critical nodes in the distribution system, based on the rank of nodes as assigned through the use of TEVA-SPOT. Police officer agents visit critical nodes randomly.

3.1.2.3. Pressure zone defense strategy. A pressure zone defense strategy allocates defense personnel at critical nodes within pressure zones. Here, an equal number of nodes is assigned as critical nodes within each pressure zone using the top ranking nodes within a pressure zone. Police officer agents are assigned to rove among critical nodes within each pressure zone.

3.1.3. Node hardening strategies

3.1.3.1. Conventional strategy. Conventional strategies place security equipment at a minimum number of nodes. Security lights are placed at schools, reservoirs, and storage tanks. Security cameras are placed at reservoirs and at pump stations near reservoirs.

3.1.3.2. Critical node hardening strategy. The critical node hardening strategy builds on the conventional strategy and allocates additional security equipment to critical nodes in the distribution system. Security lights, cameras, and empty police cars are placed at the highest ranking nodes in the distribution system.

3.1.3.3. Pressure zone hardening strategy. The pressure zone hardening strategy also builds on the conventional strategy. Additional security equipment, including security lights, cameras, and empty police cars, are allocated to critical nodes within each pressure zone. Here, an equal number of nodes is assigned as critical nodes within each pressure zone using the top ranking nodes within a pressure zone.

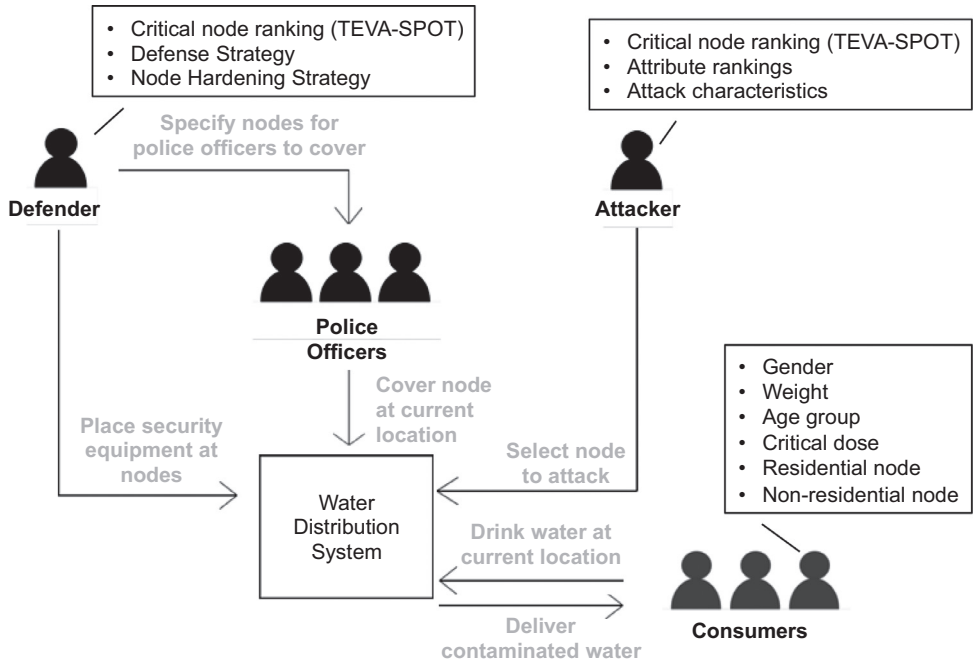

Fig. 1. ABM framework simulates an attacker versus defender game to simulate public health consequences as consumer exposure during a chemical contamination event. Agent attributes are shown in boxes.

3.2. Police officer agent

A police officer agent is assigned a roving zone based on the defensive strategy chosen by the defender agent. The current location of the police officer agent is chosen at random at the beginning of each time step from the group of nodes that are within the roving zone. If a police officer agent shares the same current location as the attacker agent during a time-step in the simulation, then there is a 50% probability that the attacker agent is not successful in carrying out an attack.

3.3. Attacker agent

The attacker agent represents a terrorist equipped with a fixed quantity of conservative contaminant. The attacker selects a node from a list of attackable nodes to inject the contaminant using one of the decision models described as follows. All junctions, tanks, and reservoirs are considered attackable nodes; pumps and valves are not, as they are assumed to be inaccessible to attacker agents.

The terrorist attacker agent uses a multi-attribute utility function to select a node [32]:

$$U_j = \sum_{i=1}^{n} w_i * S_i \forall j \quad (1)$$

where U_j is the aggregate attack utility of node j, w_i is the relative attribute utility weight of attribute i, and s_i is the attribute criterion score for attribute i. Patterson and Apostolakis [32] defined susceptibility based only on accessibility of infrastructure components and identified a number of performance attributes as part of a multi-attribute utility model that was developed to screen a set of potential attack locations and determine vulnerable infrastructure. Susceptibility attributes here include perceived police traffic, empty police car presence, visible security camera presence, physical view of the attack site, and security light presence. Performance attributes include perceived number of exposed consumers, perceived social disruption to society, and perceived economic disruption to society.

Scores (s_i in Eq. (1)) are assigned to attributes, shown in Table 1. The attacker agent assesses the presence of security cameras and security lights as placed by the manager agent to assess “Security Camera” and “Security Light” . The attacker agent assesses the location of the node with respect to other nodes to assign scores for “Social Disruption to Society” and “Economic Disruption to Society”, and landcover and land use types are used to assess “Physical View of Site” and “Perceived Police Traffic” . Finally, the attacker agent uses the outputs from TEVA-SPOT, the critical node ranking tool, to assign a score for “Perceived Consumer Exposure” . Similar to the defender agent (Section 3.1.1), the attacker agent uses the list of nodes that are ranked based on simulated consequences. The nodes are divided equally based on their ranks into three categories of “high”, “medium”, and “low” to determine scores, as shown in Table 1.”

Relative weights (w_i) are assigned using the Rank Sum approach (29,32,35), in which the weights are the individual ranks normalized by dividing the sum of the ranks (e.g., Table 2). The formula for calculating relative weights using a Rank Sum approach is shown by Eq. (2):

$$w_i = \frac{2(n+1-i)}{n(n+1)} \quad (2)$$

where w_i is the relative weight of attribute i and n is the total number of attributes in the decision model [35]. The terrorist attacker agent calculates a utility value across a set of nodes and selects among nodes with high utility values. In the following scenarios, the terrorist attacker agent selects among the top 5% of nodes using a uniform distribution.

3.4. Consumer agents

Consumers are simulated as agents that act using a set of behavioral rules to represent (1) mobility within the network and (2) ingestion of water. In the framework here, consumer agents are not adaptive and do not update their water use behaviors once they become exposed to the contaminant. These mechanisms can be included in future research that extends the current framework. The behaviors for consumer agents that are described as follows are based on the detailed descriptions provided by Shafiee and Zechman [38].

Table 1
Attribute scores used in attacker multi-attribute utility decision model.

Attribute	Potential scores
Perceived Police Traffic	None (1.0); Low (0.67); Medium (0.33); High (0.0)
Perceived Consumer Exposure	High (1.0); Medium (0.5); Low (0.0)
Security Camera	Not present (1.0); Present (0.0)
Security Light	Not present (1.0); Present (0.0)
Physical View of Site	Completely blocked (1.0); Partially blocked (0.5); Completely open (0.0)
Social Disruption to Society	Within 4 Nodes of School or Commercial Node (1.0); Within 4 Nodes of Residential Node (0.5); Other (0.0)
Economic Disruption to Society	Within 4 Nodes of Commercial Node (1.0); Within 4 Nodes of Industrial Node (0.5); Other (0.0)

Table 2
Relative weights for ranked attributes used in multi-attribute utility decision model for the attacker agent.

Rank	Relative weights
1	0.2222
2	0.1944
3	0.1667
4	0.1389
5	0.1111
6	0.0833
7	0.0556
8	0.0278

3.4.1. Mobility

During a contamination event, consumers may continue to visit residential, industrial, and commercial locations. Consumer agents are simulated as traveling between residential and non-residential nodes, so that the total number of consumer agents at a node at each time step exerts a volume of demand that matches the total demand that is specified at that node in the hydraulic simulation input data. Each consumer agent is assigned as employed or unemployed. A mobility algorithm uses a randomized process is used to assign parameters for employed consumer agents to simulate their travel: a residential node, non-residential node, time of day that specifies when the consumer agent leaves the residential node, and length of time that the consumer agent spends at a non-residential node. These values are assigned so that the total number of agents at each node at each time step matches the overall water demand that is exerted at that node, as specified in the hydraulic input data. Unemployed consumer agents are simulated at residential nodes and they do not move around during the simulation. As consumer agents travel among nodes, they may cross the boundary of the contaminant plume.

3.4.2. Ingestion and exposure

Each consumer agent is initialized with a distinct pattern for consuming and using water, based on gender and age group. Data are used from a study that reports statistics for age, gender, and weight, for the US population, as grouped into 11 discrete age groups [45]. A probabilistic approach uses an exponential distribution to assign random water volumes to consumer agents based on the mean value for each age group [45]. Eq. (3), which is the inverse form of an exponential distribution function, is used to assign a daily consumption volume to each consumer agent.

$$v = v_m \ln(1-r) \tag{3}$$

where v is the volume of water, v_m is the mean volume associated with each age group, and r is a randomly generated value between zero and one.

A consumer agent is assigned five times during a day when it consumes tap water. A probabilistic approach developed by Davis and Janke [11] specifies probability density functions for the times at which a consumer takes three daily meals, depending on the timing of previous meals. Minor meals are taken at the mid-point between major meals to simulate five daily ingestions.

As consumer agents ingest contaminated water, the mass of contaminant in an agent's body accumulates. Once a consumer agent has ingested a critical dose, he is considered exposed. The critical dose varies for different contaminants.

3.5. Water distribution model

Flows in a pipe network are simulated using EPANET (Rossman 2000), which calculates hydraulics, including flow volumes and velocities in pipes, and water quality values at nodes (pipe junctions) as a chemical contaminant propagates through the network. EPANET is embedded in the simulation framework and tightly coupled with the agent-based models. Simulation output reports pressures at nodes, height of water in storage tanks, and chemical contaminant concentrations at nodes and at pipes in discrete time steps.

4. Illustrative application: D-town

4.1. Attributes for hydraulic simulation

D-Town is a virtual municipality that was developed with a realistic water distribution system for the purpose of conducting water utility management and security research (Fig. 2) [26]. The water distribution system is modeled with 399 junctions, seven storage tanks, 443 pipes, 11 pumps, five valves, and a single reservoir. As part of this analysis, land use classifications were added to the representation of D-Town, and of its 348 populated nodes, 233 are residential, 67 are commercial, and 48 are industrial. To accurately represent demand patterns for different land use types, demand patterns for residential, commercial, and industrial nodes were applied at these respective nodes, as developed by Brumbelow et al. [7]. Changes to demand patterns increase the population density at some nodes, and to accommodate increased flow, changes were made to the infrastructure in D-Town, compared to the original input file developed by Marchi et al. [26]. A pump was added at the reservoir, increasing the volumes of the water tanks to maintain pressure, and the main pipes connecting the reservoir to tanks T1 and T4 were enlarged to provide adequate flow. A system-wide demand multiplier of 0.6 is applied to reflect winter water use where flow rates are at their lowest. Low demands lead to high concentrations of the contaminant, which can lead to early exposure of the population.

The total number of attackable nodes is 407, and the network has been designed with five pressure zones (Fig. 2a). Junctions with exerted demands are labeled as residences, schools, commercial establishments, or industrial facilities. Commercial establishments include churches, public buildings, and local businesses. Three demand patterns are specified to represent residential, commercial, and industrial

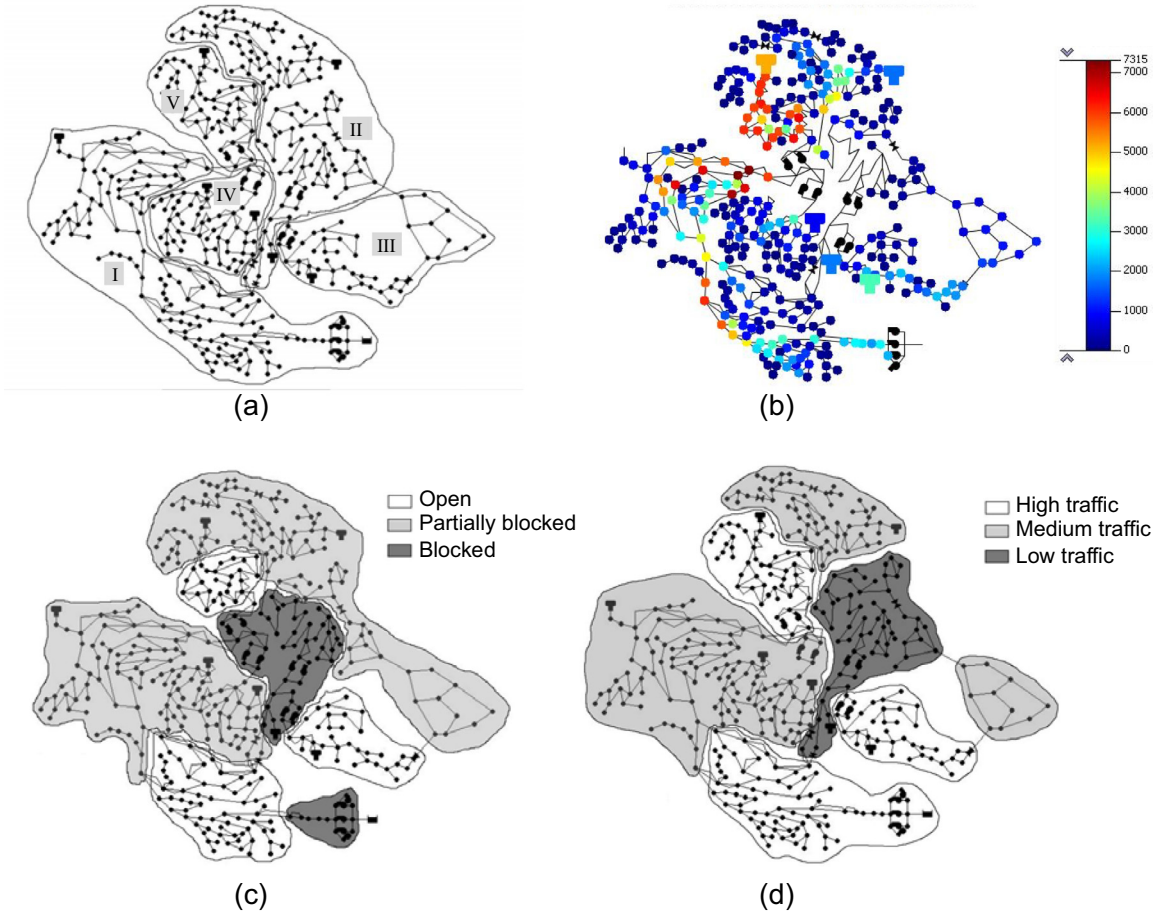

Fig. 2. Maps of D-Town node characteristics. (a) Five hydraulic pressure zones; (b) Number of exposures due to a contaminant event initiated at a node (output of TEVA-SPOT); (c) View of a node; (d) Police traffic.

demands. Schools are characterized as commercial water demands. Industrial demands are constant throughout a 24-hour day, to represent three 8-hour shifts. The demands at other nodes represent a diurnal pattern that increases through the day and decreases to nearly zero at night.

4.2. Application of TEVA-SPOT

TEVA-SPOT was executed to rank nodes based on the consequences of attack, and output from TEVA-SPOT analysis is used by both the attacker and defender agents. TEVA-SPOT is run before the agent-based modeling framework is executed, and output of TEVA-SPOT is used as input information for the attacker agent and the defender agent. TEVA-SPOT simulates number of exposures in a consequence assessment, and the results from this assessment are used as a proxy for expected consumer exposure by both the attacker agent and the defender agents in their decision framework. Therefore, while EPANET is directly coupled with the agent-based models, TEVA-SPOT is not.

The settings for using TEVA-SPOT are described as follows. The underlying assumptions for TEVA-SPOT do not take into account the mobility of consumers in the city or the stochasticity in the volume of water consumed and the timing of ingesting water for individual consumers. TEVA-SPOT estimates population based on demand patterns alone and simulates that the population of D-Town is 60,225 persons with a per capita usage of 100 gallons per day. A cumulative arsenic mass of 2.5 kg was simulated as injected for one hour, from 6AM to 7AM (416,667.67 mg/minute). In total, 357 injection sites were simulated, including all non-terminal nodes and facility nodes. The health impact analysis was conducted using the dose calculation method, which simulates the ingestion of tap water. The timing of ingestion is calculated using a demand-based algorithm. The mean volume that is consumed by each individual is 1.41 liters/person/day. The average body mass is 71.8 kg, and the critical dose is 0.05 mg/kg.

TEVA-SPOT is simulated for the 357 nodes, and requires approximately 2.5 min to run on a 64-bit operating system with an Intel Core i7-3770 CPU at 3.40 GHz and a 16 GB RAM. A map of event consequences is shown in Fig. 2b. The figure shows the level of consequences, and because the number of exposures is used to rank nodes, this figure also represents the rank of nodes. The 50 nodes that are not included in the analysis using TEVA-SPOT because they are terminal nodes are appended to the end of the list of ranked nodes in alphabetic order. Additional TEVA-SPOT results representing the consequences and rank of nodes are provided in Appendix A.

4.3. Attributes for consumer agents

The population in D-Town is 79,379 residents, and 75% of the population is employed, corresponding to data about the U.S. population [44]. Agents are initialized to represent each consumer, and consumer agents are assigned mobility parameters to exert demands at each node and time step, as specified in the hydraulic model input data. To calculate exposure to arsenic, a consumer agent is flagged as “exposed” when it accumulates 0.05 mg/kg of its body weight of arsenic [47]. This represents a symptomatic response, such as a lowest observed effect level (LOEL). Values for consumer agent attributes are provided in Table 3.

Table 3
Summary of parameter settings for ABM framework application to D-Town. * indicates settings that are varied and tested in results.

Agent	Parameter	Setting
Attacker Agent	Top percentage of ranked nodes with uniform probability of attack	5%
	Rank order of objectives*	Exposure (1), Police Traffic (2), Empty Car (3), Security Camera (4), Social Disturbance (5), Economic Disturbance (6), Physical View (7), Security Light (8)
	Attack characteristics	25 kg of arsenic injected over 1 h at 1:00AM
Defender Agent	Node hardening strategy*	Conventional, Critical Node, or Pressure Zone
	Number of critical nodes for defense strategy	40
	Defense strategy*	Random, Critical Node, or Pressure Zone
	Percentage of police officer agents to protect water infrastructure*	50%
Police Officer Agent	Police officer agents on duty	57
	Probability that police officer agent will deter an attack when attacker is met	50%
Consumer Agent	Number of consumer agents	79,379
	Percentage of population employed	75%
	Number of age groups	11
	Age range for each age group (yrs.)	{≤0.5, 0.5–0.9, 1–3, 4–6, 7–10, 11–14, 15–19, 20–24, 25–54, 55–64,≥65}
	Percentage of population, female by age group (%)	{0.8, 0.7, 4.9, 4.6, 6, 6, 7.4, 7.3, 44.6, 7.6, 10.1}
	Percentage of population, male by age group (%)	{0.7, 0.7, 4.3, 4.5, 5.3, 5.9, 6.6, 7.1, 42.6, 8.6, 13.7}
	Average weight, female by age group (kg)	{6, 9, 14, 20, 31, 50, 61, 64, 69, 71, 67}
	Average weight, male by age group (kg)	{6, 9, 14, 21, 32, 52, 73, 80, 85, 84, 80}
	Average volume of ingested water, female by age group (mL/day)	{301, 394, 316, 394, 430, 525, 653, 911, 1023, 1117, 1108}
	Average volume of ingested water, male by age group (mL/day)	{291, 325, 306, 419, 474, 665, 861, 1039, 1182, 1172, 1153}
	Mode time for ingestion of tap water for 5 events. Probability distributions are generated by probabilistic approach	{8am, 10am, 12pm, 3pm, 6pm}
	Residential & Non-residential nodes	Generated by mobility algorithm
	Mode of working start time	8AM
	Average working duration (hrs.)	8
	Critical dose	0.05 mg/kg of arsenic

4.4. Attributes for attacker utility function

Areas within the municipality are classified based on land use, land cover, pressure zone, police coverage, and contamination performance (Fig. 2c and d). Land use types include high-density residential, low-density residential, high-density commercial, low-density commercial, and coniferous forest. Land cover types represent the physical view of the area and include open view, partially blocked view, and completely blocked view. The zones created in the perceived police traffic map are given labels including low police traffic, medium police traffic, and high police traffic. The coniferous forest land cover corresponds to a completely blocked view and low police traffic; residential land cover corresponds to partially blocked view and medium police traffic; commercial land cover corresponds to completely open view and high police traffic. A few nodes in the commercial zone were assigned partially open view land cover, due to their proximity to residential nodes. The reservoir was assigned as open view land cover. It is expected that appropriate data about land use, land cover, and police traffic would be available to apply this framework for a real municipality. Values for attributes of the attacker agent are provided in Table 3.

4.5. Attributes for defender agent decisions

Based on the total population in a small township, the police force is initialized with 171 police officers [27]. There are 57 police officers on duty during each 8-hour work shift. For the critical node and pressure zone defense strategies, 50 additional security lights, 20 additional security cameras, and 15 empty police cars are placed at highest ranking nodes in the network. This security equipment is placed in addition to conventional placement of equipment at schools, reservoirs, storage tanks, and pump stations (Fig. 3a). In addition, some police officers are dedicated to rove 40 critical nodes (10% of the network) under the critical and pressure zone strategies (Fig. 3b and c). Settings for the ABM are specified in Table 3.

4.6. Modeling scenarios

The ABM framework is applied to simulate a terrorist attacker agent that attempts to initiate a contamination event in D-Town at 1:00AM. For this event, the attacker is simulated as injecting 25 kg of arsenic over a one-hour duration. The short event represents an incident in which a large load of contaminant is injected in the system at once. The terrorist attacker agent uses a multi-attribute utility rule to select a node to attack. The defender agent places security equipment before the attack using conventional, critical node, or pressure zone node hardening strategies. The defender agent also selects the random, critical node, or pressure zone police roving strategies (Fig. 3b). If a police officer is at the node that the attacker selects, then there is a 50% probability that the attack is not successful. If an attack on a node is unsuccessful, then the number of exposed consumers is counted as zero for that simulation. If an attack on a node in the distribution system is successful, then the ABM-EPANET framework is simulated for 48 hours using 1-hr time steps to determine the number of exposed consumers.

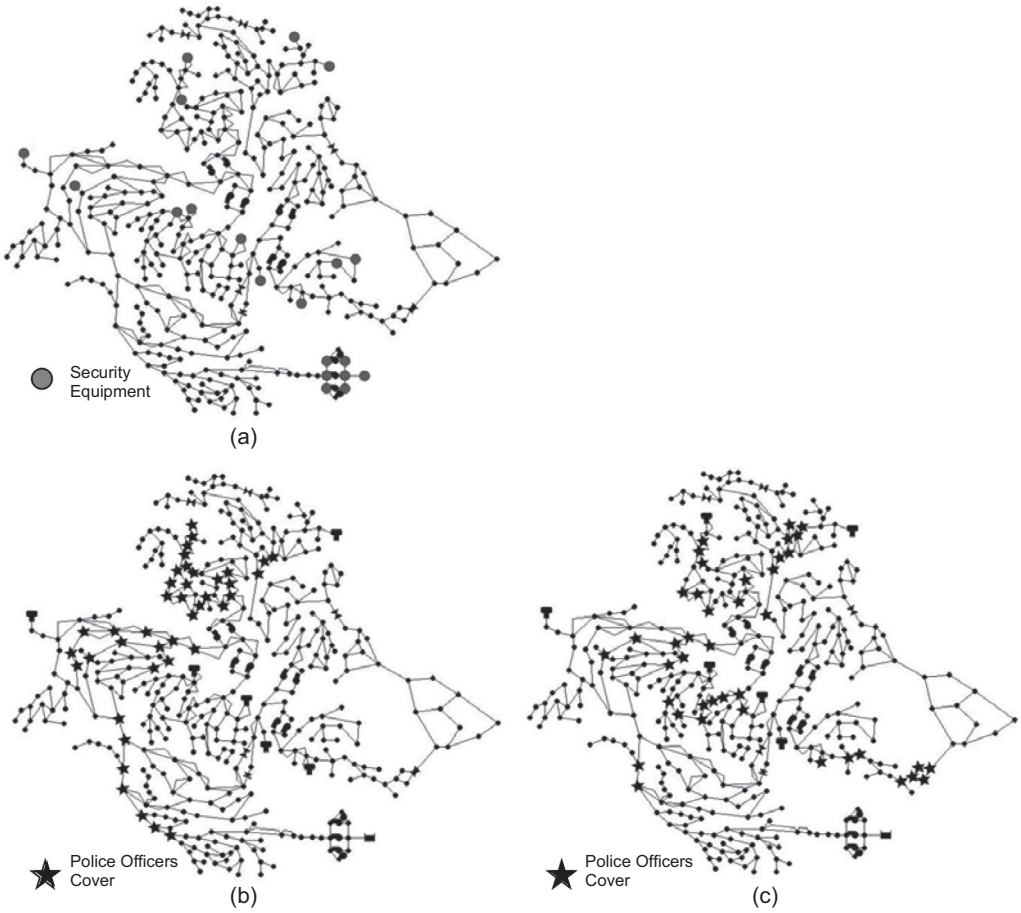

Fig. 3. (a) Security equipment coverage map for the conventional strategy. (b) Police officer coverage map of critical nodes for the critical node strategy. (c) Police officer coverage map of critical nodes for the pressure zone strategy.

Table 4
Multi-attribute utility rankings and relative weights for five different cases for attacker agent decision-making (Weights for each rank are provided in Table 2).

Attribute	Rank Case 1	Rank Case 2	Rank Case 3	Rank Case 4	Rank Case 5
Exposure	1	2	2	3	1
Police Traffic	2	1	3	1	4
Empty Car	3	3	1	2	5
Security Camera	4	4	4	4	6
Social Disturbance	5	5	5	5	2
Economic Disturbance	6	6	6	6	3
Physical View	7	7	7	7	7
Security Light	8	8	8	8	8

Five cases are tested, which vary the ranking of attributes by the terrorist attacker agent (Table 4). The five cases were constructed to represent alternative priorities of an attacker agent. Because the specific goals and priorities of a terrorist are typically unknown, and data about this are imperfect and incomplete, several cases are simulated to represent a range of priorities. Case 1 prioritizes exposing as many consumers as possible to a contaminant followed by reduction of risk of capture; Case 5 prioritizes exposing high number of consumers and disrupting social and economic activities. The performance of the conventional/random, critical node, and pressure zone defense strategies are evaluated across the five cases to identify robust strategies that defend well against unknown ranking of goals by terrorists. Each combination of rank case and defender strategy is evaluated for a large number of random simulations. Randomness affects the police roving strategies and the decision of the attacker in each simulation.

5. Results

5.1. Performance of defense strategies for contamination events

The three management strategies are tested for the different attacker agent cases, based on the multi-attribute utility decision-making model. The attack is simulated for 1000 random trials for each combination of management strategy (three types) and attacker case (five types). A total of 15,000 simulations are carried out. Successful attacks are simulations in which the attacker agent selects a node to attack and carries out the

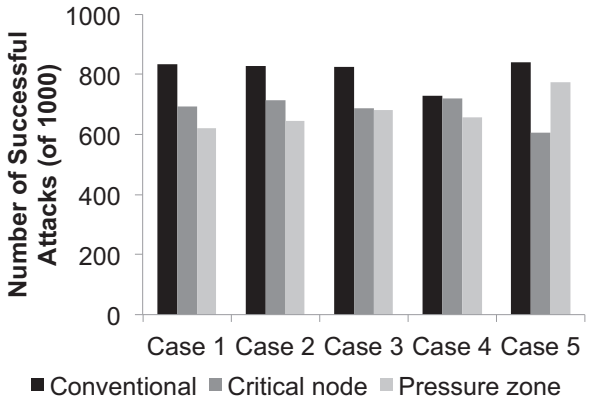

Fig. 4. Number of successful attacks out of 1000 simulations.

attack, based on the presence of a police officer at that node. For successful attacks, the ABM simulates the exposure of the population over a 48-hour time period. The model simulates that consumer agents travel among nodes within the city, ingest water, accumulate arsenic, and become exposed. A successful attack may generate zero or more exposures. Output from the ABM reports the number of consumers that are exposed at each time step, or hour, and the final number of exposed consumers at the last time step of the simulation is used to report the exposure associated with successful attacks. A large number of random simulations is required to adequately represent the behavior of the sociotechnical system. Though there are 407 nodes that the attacker agent can select, there is stochasticity in the presence of police officers at a selected node, a probability (50%) of success if there is a police officer at that node, and stochasticity in consumer behaviors. These properties affect the final number of exposed consumers. For each combination of management strategy and attacker case, the ABM output for 1000 random simulations is aggregated and reported as (1) the number of successful attacks out of 1000 and (2) the cumulative probability distribution of number of exposed consumers for 1000 simulations. For one successful attack, the ABM requires approximately 60 seconds to execute.

The critical node and the pressure zone strategies result in fewer successful attacks, compared to the conventional strategy, for all cases (Fig. 4). For Case 4, the conventional strategy performs better than it does for other cases. This is because the attacker prioritizes avoiding nodes with police traffic and empty police cars. As a result, the agent attempts more attacks in pressure zone 2 and fewer in pressure zone 5, compared with other Cases 1, 3, 4, and 5, and has more success in that pressure zone.

For Case 5, the critical node strategy performs better than the pressure zone strategy by a larger margin than other cases. For this case, the attacker prioritizes nodes that have high consequences and are located near economic and social activities. The critical node strategy allocates more security equipment to nodes with high exposure, compared to the pressure zone strategy. These nodes are located near economic and social activities, such as industrial nodes, commercial nodes, and schools, which are visited by high numbers of consumers throughout a 24-hour period. The critical node strategy protects these nodes with a high priority, and this defense strategy is effective against an attacker who has also prioritized these nodes. The pressure zone strategy allocates security equipment throughout the network, rather than focusing on high-impact nodes.

The success of defender strategies is also evaluated on the consequences of attacks. The number of exposed consumers in a successful attack ranges from less than 20 to more than 8,800. These numbers are similar to the consequences predicted by TEVA-SPOT (shown in Fig. 2b and in the Appendix), although there are differences in both the mass of the contaminant injected (2.5 kg for TEVA-SPOT simulations, and 25 kg for ABM-EPANET) and the time of day of the attack (6AM for TEVA-SPOT simulations, and 1AM for ABM-EPANET). Although the ABM-EPANET was simulated using a higher contaminant mass, it was initiated earlier in the morning, compared to events that were simulated using TEVA-SPOT. Events that are initiated early in the morning, as simulated by the ABM-EPANET framework, do not result in high exposures because few agents are drink water at that time.

Exposed consumers are those that are flagged as exposed when they ingest a critical amount of contaminant, here 0.05 mg/kg of their body weight of arsenic. To compare the number of exposed consumers, or number of sicknesses, for the three defender strategies, the cumulative probability distribution is displayed (Fig. 5). For all attacker cases, the critical node and pressure zone strategy perform better than the conventional strategy. The pressure zone and critical node strategies place more security equipment than the conventional strategy, and it is expected that they should result in fewer exposures. The critical node strategy performs results in fewer exposures than the pressure zone strategy.

Table 5
Equipment allocation for levels of coverage. Each coverage strategy places security equipment in addition to the conventional strategy. Base case corresponds to the original allocation for critical node and pressure zone strategies (results show in Section 5.1).

Strategy	Number of security lights	Number of security cameras	Number of empty cars
Base Case	50	20	15
5% Increase	70	28	21
10% Increase	91	36	27
15% Increase	111	44	33

5.2. Tradeoffs between investment in security equipment and exposure

The ABM framework is applied to explore gains in public health protection, measured as exposure to a contaminant, for varying levels of security. Here, four strategies are simulated and assessed for increasing levels of security coverage, expressed as the percentage of nodes in the network that are covered (Table 5). These strategies are simulated for critical node and pressure zone defense strategies and for three cases of the attacker agent's utility. Each scenario is simulated for 500 random realizations. Analysis of results demonstrated that stochasticity is captured by 500 realizations, and the reduction in realizations was made to reduce computational complexity.

Increasing levels of coverage results in an improvement in public health protection for the critical node and pressure zone strategies (Figs. 6 and 7, respectively). For the critical node strategy, the improvement in public health is more definitive. This is because security equipment is placed at nodes resulting in high exposure, and the attacker selects from nodes with less impact. For Case 5, the attacker does not prioritize the presence of security equipment as a top concern; for this case, there is still a decrease in the number of exposed consumers, though the results for the 5% improvement do not show a clear gain in performance. The pressure zone strategy results in lower gains in protecting public health through the addition of new security equipment. Again, because nodes are selected for coverage based on not only exposure, but also pressure zones, some significant nodes are not protected, and the attacker continues to successfully select and attack those nodes. These results emerge due to the complex relationship between placing security equipment and the real-time decision-making of the attacker. The presence of security equipment averts an attack at one node, but may cause an attacker to seek an alternative node that has relatively high consequences and is located in an area of low police traffic. Consider

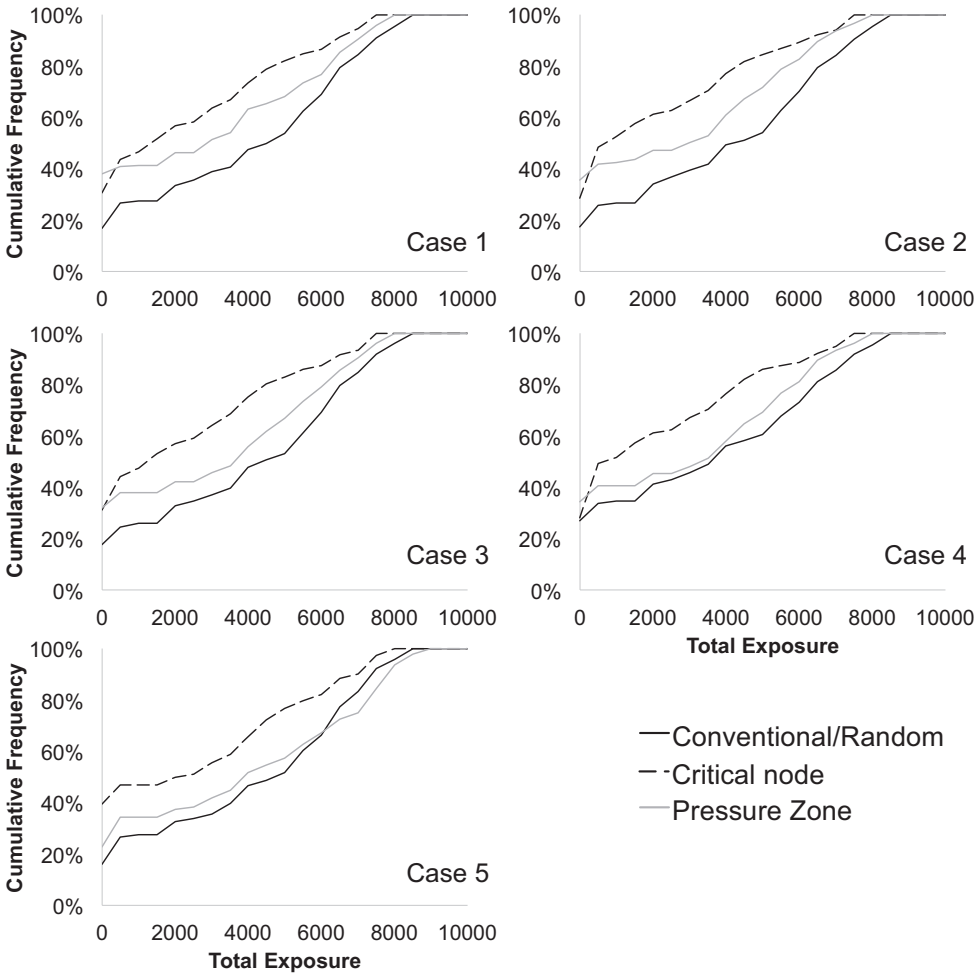

Fig. 5. Performance of each defense strategy for 1000 simulations. Exposure refers to the number of exposed consumers. Attacker is simulated for five multi-attribute utility cases, listed in Table 4.

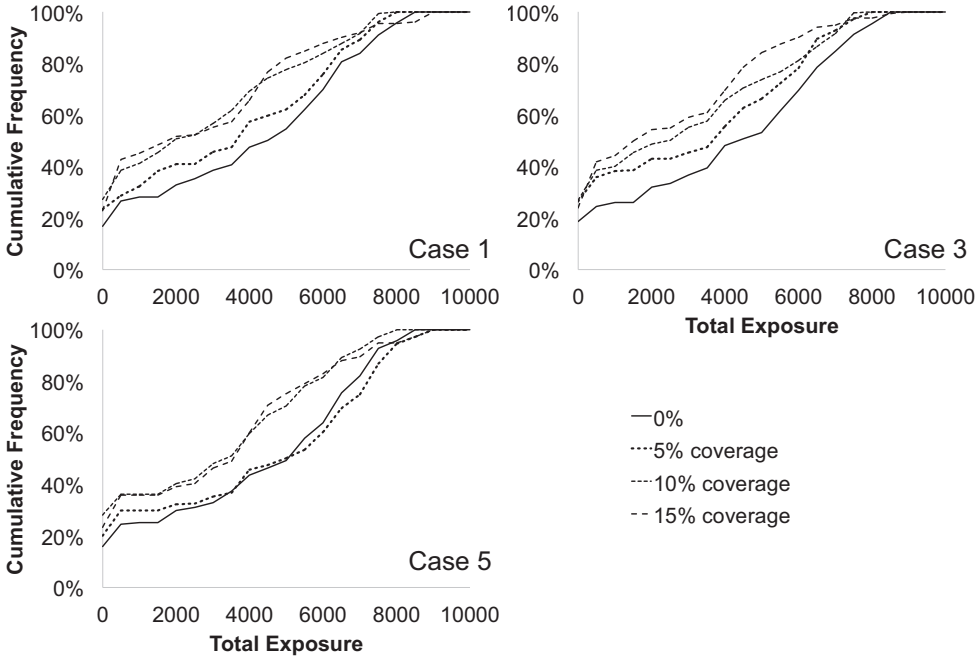

Fig. 6. Performance of critical node strategy for varying levels of security equipment for attacker Cases 1, 3, and 5. Exposure refers to the number of exposed consumers. 0% increase in coverage corresponds to the base case critical node strategy for placing security equipment.

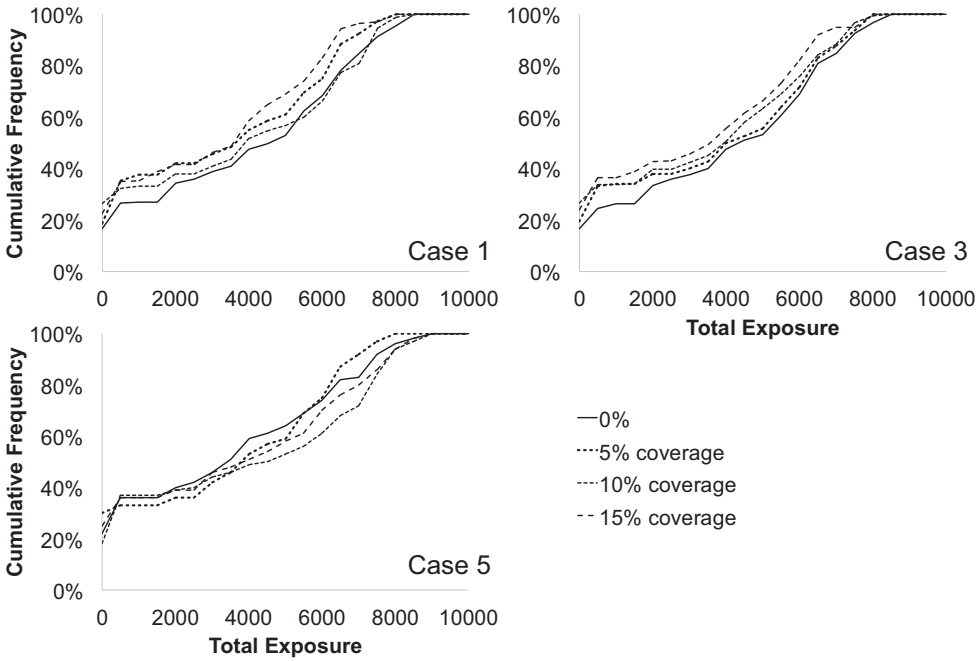

Fig. 7. Performance of pressure zone strategy for varying levels of security equipment for attacker Cases 1, 3, and 5. Exposure refers to the number of exposed consumers. 0% increase in coverage corresponds to the base case pressure zone strategy for placing security equipment. Results shown for 500 simulations.

the case of minimal security equipment, in which some nodes generate very high exposure values that are not ranked highly for attack because of characteristics such as police traffic and surrounding view. When security equipment is increased, nodes that were previously ranked highly become less attractive, and therefore nodes those nodes with high exposure may become more attractive to the attacker.

The placement of security equipment also affects the number of exposures based on the distribution of attacks among pressure zones. Consider the number of successful attacks in pressure zones (Fig. 8). For the critical node strategy, the addition of new equipment is placed primarily in pressure zone 5, and as a result, successful attacks in pressure zone 5 decrease with increasing equipment. However, more successful attacks occur in the other pressure zones as the attacker turns his attention elsewhere (Fig. 8a). For the pressure zone strategy, successful attacks in pressure zone 1, 2, and 5 decrease marginally with additional equipment, because the additional equipment is placed uniformly across all the pressure zones. These results demonstrate that the relationship between the placement of security equipment and police roving strategies is important in averting the number of successful attacks, and future research should explore the development of optimal police roving strategies based on the level of security equipment.

5.3. Exploring police allocation strategies

The strategies explored above assume that 50% of the police force (28 of 57 officers in each shift) is directed to cover nodes based on infrastructure protection. Because a police force has many objectives, in addition to thwarting attacks on infrastructure, the number of police officers dedicated to significant nodes may be considerably higher or lower than 50%. Here, we evaluate the critical node strategy for varying levels of police allocation, ranging from 19 to 81%, while using the conventional approach for placing security equipment and the critical node approach for placing security equipment (Fig. 9a and c). This results in six additional scenarios. Case 1 is used in these simulations alone to simplify discussion. For these simulations, the critical node approach

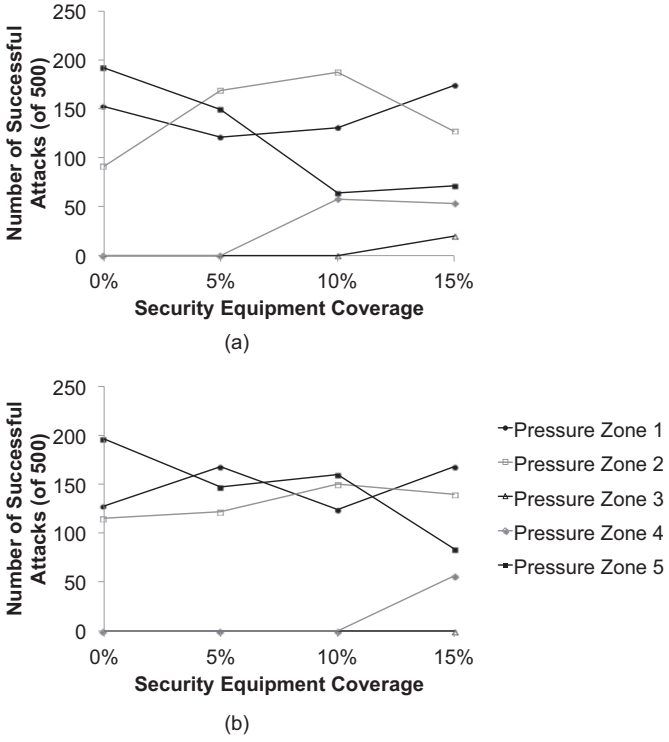

Fig. 8. Number of successful attacks in each pressure zone for varying levels of security equipment coverage for (a) critical node strategy and (b) pressure zone strategy. Results shown for Case 1.

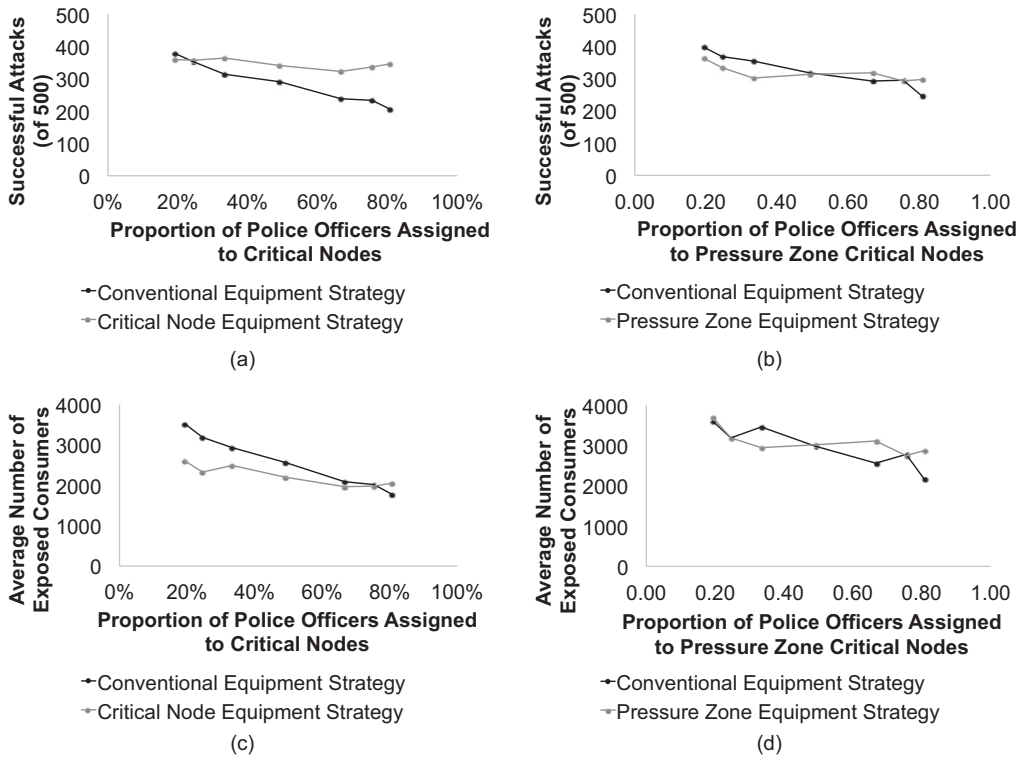

Fig. 9. Number of successful attacks for varying levels of police coverage for (a) critical node personnel strategy and (c) pressure zone personnel strategy. Average number of exposed consumers for (b) critical node personnel strategy and (d) pressure zone personnel strategy. Results shown for 500 simulations.

places 50 additional security lights, 20 additional security cameras, and 15 empty police cars. Each scenario is simulated for 500 random realizations.

As shown in Fig. 9a, the number of successful attacks actually increases for the critical node strategy, when the number of officers increases and the critical node strategy is used to place security equipment. However, the complete picture is shown in Fig. 9c, that these successful attacks result in a lower number of exposed consumers. Similarly, the pressure zone strategy is assessed for varying levels of police allocation, with the conventional and pressure zone approaches for placing equipment (Fig. 9b and d). For both the conventional strategy and the pressure zone strategy for placing equipment, the increase in officers dedicated to targeted nodes decreases both the number of successful attacks and the exposed consumers. For both the pressure zone and critical node strategies, in general, the addition of equipment beyond the conventional approach does not improve the protection against attacks (that is, the critical node equipment and pressure zone equipment strategies do not perform better than the conventional equipment strategy in Fig. 9a and b).

An important management question should be answered before selecting the strategy for placing equipment and security personnel. Decision-makers should determine if they are more interested in fewer successful attacks or fewer exposed consumers. Because terrorists may have goals for causing widespread fear, rather than maximizing the number of deaths, alternative strategies may be preferred. Ultimately, the goals of a terrorist remain unknown, and a strategy that is robust across multi-attribute utility function cases may be preferred for implementation.

6. Conclusions

This research develops an agent-based modeling framework to simulate attacker and defender decisions, and their consequences, in the case of potable water contamination. Decision-making strategies for a water utility are simulated based on *a priori* analysis of the hydraulics in a water distribution system. Many water utilities conduct hydraulic analysis to assess vulnerabilities in their infrastructure systems, and this research uses readily available tools that a utility may use, including a hydraulic simulation model (EPANET), pressure zone management, and a toolbox for consequence assessment to reduce the number of exposed consumers in a contamination event (TEVA-SPOT). The water utility selects locations for countermeasures, including security equipment and personnel, based on the output of these models. A terrorist is simulated as an attacker who selects one node from many attackable nodes to place a contaminant. The decision-making strategy of the terrorist is simulated using multi-attribute utility theory. Because there is a wide range of uncertainty concerning attacker decisions, five cases are simulated to rank priorities in alternative orders.

The ABM-EPANET framework includes a number of parameters and assumptions. In this research, we test the significance of a number of settings, including: (1) the type of defense and node hardening strategies (random/conventional, critical node, and pressure zone), (2) the rank order of the attacker priorities, (3) the percentage of police officers dedicated to protecting water infrastructure, and (4) the percentage of nodes that are covered by security equipment. For most cases, the critical node defense strategy outperforms the pressure zone strategy, by allocating security to nodes with high consequences, rather than spreading resources out in the network to cover pressure zones. However, the case, or rank order for the attacker agent, affects the results. Specifically, Case 4 ranks the lack of security equipment highly, and Case 5 ranks disturbance highly, instead of the number of exposures. Because defender agents determine strategies based on reducing exposures, the performance of defense for Cases 4 and 5 are generally reduced, compared to the performance for Cases 1, 2, and 3. Varying levels of security coverage represents increasing costs for protecting public health.

An increase in security equipment decreases the number of exposures, as an attacker may seek out alternative nodes in areas of lower police traffic. An increase in police officers allocated to critical nodes can result in an increased number of successful attacks and in lower average exposures. It is critical to refine public health protection goals in selecting a defense strategy. Unintended results of increased coverage may direct attacks at previously unattractive nodes that may be more (or less) susceptible, such as hospitals, schools, or low-income housing areas. Though results may be counter-intuitive, increasing security may also result in more successful attacks, though, on average, attacks have lower consequences. These outcomes may be unacceptable in a public forum.

In the framework developed here, the defender and attacker agents use a critical node ranking tool, TEVA-SPOT, that varies in its predictions from the simulation model, the ABM-EPANET framework, to evaluate the consequences of events. The TEVA-SPOT tool was used here in an approach similar to that taken by a utility manager. A utility manager may not know the timing or injected mass of an anticipated contamination event, and she or he may have to select values based on engineering judgment. Here, the timing and mass of the events simulated using TEVA-SPOT and the ABM-EPANET framework varied, though the type of contaminant (arsenic) and the duration of the event match, and simulated results were within the same magnitude of exposures. It is expected that the accuracy with which the utility manager selects settings for TEVA-SPOT impact the outcomes of the event, but would not dramatically change the ranking of nodes, which is what drives the management strategies. It is impractical to assume that a utility manager could accurately predict these outcomes or that every combination of event characteristics could reasonably be tested. If the same settings were used for both TEVA-SPOT and the ABM-EPANET simulation, the number of predicted consequences would vary, based on the underlying assumptions of each model. The ABM-EPANET framework includes behaviors of each individual, including mobility and randomness in ingestion timing and volume, which are neglected in the TEVA-SPOT simulation. TEVA-SPOT is a tool that is readily available to utilities, as it can be freely downloaded, while the ABM-EPANET framework is an alternative approach that has not been used by practitioners. The ABM-EPANET framework captures behaviors of individuals that can better predict the variations in the outcomes of a contamination event.

In the research presented here, consumers are encoded with behaviors to specify that they drink contaminated water and become exposed. In related research, consumers are simulated with adaptive behaviors, and stop using water once they become sick or learn about contaminated water from peers or utility managers [38]. These adaptive behaviors can be included in the framework presented here to explore interactions among consumers, water utility managers, and perpetrators.

Acknowledgments

This material is based upon work supported in part with funding from the Laboratory for Analytic Sciences (LAS). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the LAS and/or any agency or entity of the United States Government. Thanks to our research team, Hayden Strickling, Michael Knepper, and M. Ehsan Shafiee for assisting in model and case study development.

Appendix A. TEVA-SPOT results

TEVA-SPOT was used to rank nodes for priority for both the defender and attacker agents. Results of the analysis generate the number of consequences per node (Fig. A1) and the rank of each node (Fig. A2) for prioritizing nodes for attack and defense.

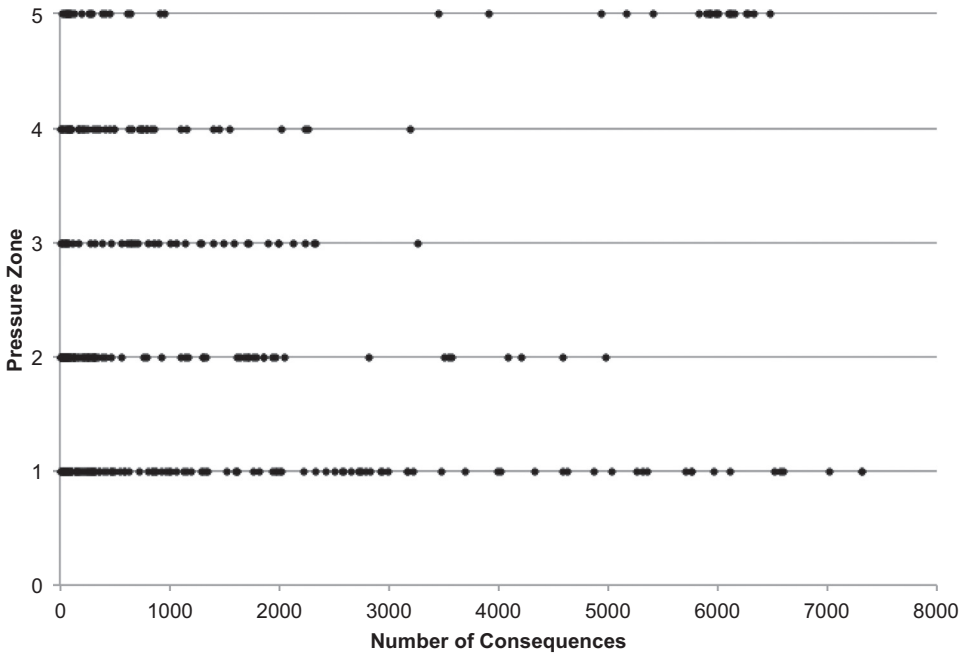

Fig. A1. Results of TEVA-SPOT analysis, showing number of consequences for each node, based on location within pressure zone.

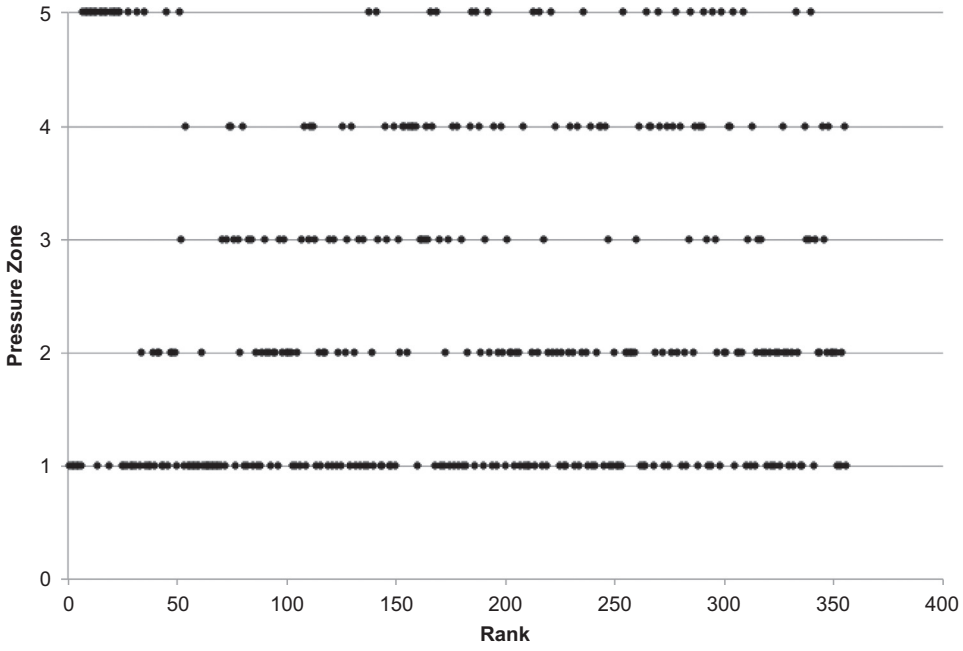

Fig. A2. Results of TEVA-SPOT analysis, showing rank of each node, based on location within pressure zone.

References

[1] Adler N, et al. Location-allocation models for traffic police patrol vehicles on an interurban network. Ann Oper Res 2013:1–23 Print.
[2] American Water Works Association. Physical security technologies for water and wastewater utilities. AWWA Research Foundation; 2008. Print.
[3] Aljazeera Kosovo cuts water supplies after ISIL 'Poison' plot. Aljazeera 2015 12 July 2015. Web. Accessed 28 Sept. 2015.
[4] Apostolakis GE, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Anal 2005;25(2):361–76.
[5] Berry J, Boman E, Riesen LA, Hart W, Phillips C, Watson J-P. User's manual TEVA-SPOT TOOLKIT 2.5.2, EPA 600/R-08/041B. Cincinnati, OH: Office of Research and Development, U.S. Environmental Protection Agency; 2012.
[6] Bliss T, Guria J, Jones W. A road safety resource allocation model. Transport Rev. 1999;19(4):291–303 Print.
[7] Brumbelow K, Torres J, Guikema S, Bristow E. Virtual cities for water distribution and infrastructure system research. World environmental and water resources congress, Florida: Tampa; 2007. May 15–19.
[8] Cesario L. Modeling, analysis, and design of water distribution systems. Amer Water Works Assn; 1995.
[9] Chalecki EL. A new vigilance: identifying and reducing the risks of environmental terrorism. Global Environ. Polit. 2002;2(1):46–64.
[10] Cox LA. Game theory and risk analysis. Risk Anal 2009;29(8):1062–8.
[11] Davis M, Janke R. Development of a probabilistic timing model for the ingestion of tap water. J Water Resour Plann Manage 2009;135(5):397–405.
[12] Ferrari G, Savic D, Becciu G. Graph-theoretic approach and sound engineering principles for design of district metered areas. J Water Resour Plann Manage 2014;140(12):13 04014036.
[13] Foran JA, Brosnan TM. Early warning systems for hazardous biological agents in potable water. Environ Health Perspect 2000;108(10):993–6.
[14] Furtado V, Vasconcelos E. A multiagent simulator for teaching police allocation. AI Mag 2006;27(3):63–74 Print.
[15] Gleick P. Water and terrorism. Water Policy 2006;8:489 Print.
[16] Guedes R, Furtado V, Pequeno T. Multiagent models for police resource allocation and dispatch. In: IEEE joint intelligence and security informatics conference; 2014. p. 288–91. Print.
[17] Hamada M. Water supply system: planning aspects. Critical urban infrastructure handbook, 11, Boca Raton: CRC; 2014. Print.
[18] Janke R, Tryby M, Clark R. Protecting water supply critical infrastructure: an overview. In: Clark R, Hakim S, editors. Securing water and wastewater systems: global experiences. Protecting Critical Infrastructure, 2; 2014. p. 29–85.
[19] Kar K, Datta TK. Development of a safety resource-allocation model in Michigan. Transp. Res. Rec. 1865 2004:64 Print.
[20] Khan AS, Swerdlow DL, Juranek DD. Precautions against biological and chemical terrorism directed at food and water supplies. Public Health Rep 2001;116(1):3–14.
[21] Kerigan-Kyro C. NATO and critical infrastructure resilience - planning for the unknown. In: Edwards M, editor. Critical infrastructure protection, 116. NATO Science for Peace and Security Series E-Human and Societal Dynamics; 2014. p. 1–12.
[22] Kornfeld IE. Terror in the water: threats to drinking water and infrastructure. Widener Law Symp J 2002;9:439–84.
[23] Kroll D. Securing our water Supply: protecting a vulnerable resource. Tulsa, OK: PennWell Corporation; 2006.
[24] Kroshl W, Sarkani S, Mazzuchi T. Efficient allocation of resources for defense of spatially distributed networks using agent-based simulation. Risk Anal 2015;35(9):1690–705.
[25] MacDonald G, Yates C. DMA design and implementation, an American context. In: Proc. IWA Specialised Conf. Leakage. Halifax, NS: IWA Publishing; 2005.
[26] Marchi A, Salomons E, Ostfeld A, Kapelan Z, Simpson A, Zecchin A, Maier H, Wu Z, Elsayed S, Song Y, Walski T, Stokes C, Wu W, Dandy G, Alvisi S, Creaco E, Franchini M, Saldarriaga J, Páez D, Hernández D, Bohórquez J, Bent R, Coffrin C, Judi D, McPherson T, van Hentenryck P, Matos J, Monteiro A, Matias N, Yoo D, Lee H, Kim J, Iglesias-Rey P, Martínez-Solano F, Mora-Meliá D, Ribelles-Aguilar J, Guidolin M, Fu G, Reed P, Wang Q, Liu H, McClymont K, Johns M, Keedwell E, Kandiah V, Jasper M, Drake K, Shafiee E, Barandouzi M, Berglund A, Brill D, Mahinthakumar G, Ranjithan R, Zechman E, Morley M, Tricarico C, de Marinis G, Tolson B, Khedr A, Asadzadeh M. Battle of the water networks II. J. Water Resour. Plann. Manage. 2014;10:04014009 1061/(ASCE)WR.1943-5452.0000378.
[27] McCabe J. An analysis of police department staffing: how many officers do you really need? An ICMA Center for Public Safety Management White Paper; 2012.
[28] Meinhardt PL. Water and bioterrorism: Preparing for the potential threat to US water supplies and public health. Annu Rev Public Health 2005;26:213–37.
[29] Michaud D, Apostolakis G. Methodology for ranking the elements of water-supply networks. J Water Resour Plann Manage 2006;12(4):230–42.
[30] Murray R, et al. Sensor network design of contamination warning systems: a decision framework. Am Water Works Assoc. 2008;100(11):97–109 2008.
[31] Murray R, et al. US environmental protection agency uses operations research to reduce contamination risks in drinking water. Res Manage Sci 2009;39(1):57–68 2009Print.
[32] Patterson S, Apostolakis G. Identification of critical locations across multiple infrastructures for terrorist actions. Reliab Eng Syst Saf 2007;92(2007):1183–203 Print.
[33] Preis A, Ostfeld A. Multiobjective contaminant response modeling for water distribution systems security. J Hydroinf 2008;10(4):267–74 2008Print.
[34] Rasekh A, Shafiee ME, Zechman EM, Brumbelow K. Sociotechnical risk assessment for water distribution system contamination threats. J Hydroinf 2013;16(3):531–49.
[35] Roberts R, Goodwin P. Weight approximations in multi-attribute decision models. J Multi Criteria Decis Anal 2003;11:291–303 Print.
[36] Roger D. Reducing leakage in Jakarta, Indonesia. In: Proc. IWA specialised conf. leakage, Halifax, NS. IWA Publishing; 2005.
[37] Shafiee ME. Modeling sociotechnical water distribution system contamination events to evaluate and identify mitigation strategies. Raleigh, NC: North Carolina State University; 2014.
[38] Shafiee ME, Zechman E. An agent-based modeling framework for sociotechnical simulation of water distribution contamination events. J Hydroinf 2013;15(3):865–7 2013Print.
[39] Skolicki Z, Arciszewski T, Houck M, De Jong K. Co-evolution of terrorist and security for water distribution systems. Adv Eng Softw 2008;39:801–11.
[40] Talarico L, Reniers G, Sorensen K, Springael J. MISTRAL: a game-theoretical model to allocate security measures in a multi-modal chemical transportation network. Reliab Eng Syst Saf 2015;138:105–14.

[41] Tambe M. Introduction and overview of security games. Security and game theory : algorithms, deployed systems, lessons learned. Cambridge University Press; 2012. 2. Print.
[42] TEVA-SPOT Toolkit A sensor placement optimization tool for water security. TEVA-SPOT Toolkit 2017. Sandia National Laboratories, 01 Jan. 2010. Web. 8 Apr.https://software.sandia.gov/trac/spot>.
[43] Tularam G, Properjohn M. An investigation into modern water distribution network security: risk and implications. Secur. J. 2011;24(4):283–301.
[44] U.S. Department of Labor (USDOL). Economic news release. Bureau of Labor Statistics, Accessed December 3, 2015 http://www.bls.gov/news.release/empsit.t01.htm.
[45] US Environmental Protection Agency (USEPA). Estimated per capita water ingestion in the United States. US environmental protection agency -822–00-008. DC: Office of Water, Washington; 2000.
[46] Winter J. Law enforcement bulletin warned of ISIS Urging Jihad attacks on US soil. Fox News 2014 18 Sept.Web. 11 Aug. 2015.
[47] White J. Hazards of short-term exposure to arsenic contaminated soil. Office of Environmental Health Assessment Services; 1999. Post Office Box 47846.
[48] Zechman E. Agent-based modeling to simulate contamination events and evaluate threat management strategies in water distribution systems. Risk Anal 2011;31(5):758–72 2011.