water

MDPI

*Article*

# Reliability of a Contamination-Detection Sensor Network in Water Distribution Systems during a Cyber-Physical Attack

**Gopinathan R. Abhijith, Elad Salomons and Avi Ostfeld ***

Faculty of Civil and Environmental Engineering, Technion, Haifa 32000, Israel
* Correspondence: ostfeld@technion.ac.il

**Abstract:** The vastness of water distribution systems (WDS) makes them vulnerable to exposure to different types of accidental/intentional contamination. Although most such contamination events that occurred in the recent past were accidental, criminal intent was involved in a few. Considering the accessibility of WDS and the potentially harmful outcomes of drinking-water contamination, online water-quality monitoring sensors are typically positioned in selected locations throughout WDS as a preventive strategy. These sensors, once positioned, communicate over a cyber-infrastructure layer and are liable to cyber-physical attacks—the sensor and/or its communication system becoming compromised or the sensor network becoming malfunctioned such that part of its components is deactivated. However, the sensor network placement state-of-the-art has thus far overlooked these cyber-physical attack scenarios. The current study attempts to overcome this limitation in the state-of-the-art by developing and demonstrating a methodology for evaluating the impact of a cyber-physical attack on a sensor network, compromising its functionality partially. Our proof-of-concept, using a simple network and a straightforward cyber-physical attack scenario, has revealed the vast potential of examining the performance of sensor networks under accidental/intentional malfunctioning and providing valuable information for decision makers in water utilities and regulators.

**Keywords:** water quality; sensor placement; water distribution systems; cyber-physical attacks



**Citation:** Abhijith, G.R.; Salomons, E.; Ostfeld, A. Reliability of a Contamination-Detection Sensor Network in Water Distribution Systems during a Cyber-Physical Attack. *Water* **2022**, *14*, 3669. https://doi.org/10.3390/w14223669

Academic Editor: Andreas N. Angelakis

Received: 20 October 2022
Accepted: 11 November 2022
Published: 14 November 2022



## 1. Introduction

Water distribution systems (WDS) are spatially extensive; hence, they are vulnerable to 'accidents'. At large, accidents causing problems with the physical integrity of WDS can cause substantial economic loss and environmental damage, but their direct threat to human health is limited. On the contrary, accidents involving a contaminant intrusion in WDS cause drinking-water quality deterioration and could induce acute or chronic health risks to the water consumers.

For any contaminant not prevailing within the distribution pipe environment [1] to reach consumer taps, intrusion(s) (accidental or intentional) should happen, either at the treatment plants or within the distribution network domain (reservoirs, tanks, pipes). Although backflow preventers impede contaminant entry into the pipes from the outside, they are not prevalent at every pipe joint, and if they exist, they might not always be functioning. Presumably, due to the integrity flaws in WDS and/or its components malfunctioning in contamination prevention [2], several accidental and intentional contaminant intrusion events in WDS have been reported in the past [3,4].

An Online Contaminant Monitoring System (OCMS) employing water quality (WQ) sensors is generally admitted [5] as the primary tool to minimize contaminant intrusion impacts. An OCMS is designed to detect unexpected events of drinking-water contamination and furnish knowledge on the contamination event-location of contamination with the WDS domain and intrusion characteristics (contaminant type, intrusion time and duration, concentration, and mass intrusion rate). In fact, designing an OCMS is one of the most explored problems in WDS security enhancement through modeling [6–10].

Due to cost constraints, WQ sensors cannot be placed at every node of a WDS; hence, the available resources must be optimally deployed. This motivated the development of countless methodologies to allocate a limited number of sensors within a distribution network optimally. The pioneering work in this direction is attributed to Lee et al. [11]. These researchers solved the WQ sensor placement problem using mixed-integer linear programming and assuming steady-state hydraulic conditions within the network. The maximum demand coverage was selected as their objective function. Afterward, Harmant et al. [12] improved the WQ sensor placement methodology by including water quality and considering unsteady hydraulic conditions. With the evolution of heuristic optimization, Al-Zahrani and Moeid [13] employed genetic algorithms to solve the same problem formulation. Following the work of Lee et al. [11], Kessler et al. [14] added an all-shortest path algorithm to the coverage problem and constructed a pollution matrix. The pollution matrix comprised data on the nodes contaminated by multiple possible contamination events. These researchers defined the contaminated node as a node in which the contaminant concentration is above a predefined threshold value. Later on, Ostfeld and Salomons [9] expanded this study and introduced a randomized pollution matrix which holds binary information about a set of randomly generated multiple contaminant intrusion locations and times. This was applied to determine whether a system node is contaminated during a specific random contaminant intrusion event. Although numerous studies were reported on further altering, expanding, and improving the methodologies above-mentioned and applying them to several probable contamination scenarios in different WDS [7,8,15–18], the benchmark in this field of study is the battle of the water sensor networks (BWSN) conference held in Cincinnati in the year 2006 [19]. The BWSN conference compared fifteen approaches to optimal WQ sensor placement in WDS, and these approaches primarily evaluated four objectives: (1) the time of detection; (2) the affected population prior to detection; (3) consumption of contaminated water prior to detection; and (4) likelihood of detection.

The extensive research efforts in WQ sensor network placement modeling have resulted in the development of several tools. TEVA-SPOT, developed by the U. S. Environmental Protection Agency, Sandia National Laboratories, Argonne National Laboratory, and the University of Cincinnati [20], is a widely applied tool for developing an OCMS. After implementing an OCMS in a WDS, communication occurs via a Supervisory Control and Data Acquisition (SCADA) system.

Nevertheless, as WDS is vulnerable to accidents, the OCMS and the associated SCADA system are susceptible to malfunctioning by natural causes or cyber-physical attacks. The malfunctioning could result in (1) OCMS giving erroneous predictions, (2) OCMS being entirely non-functional and giving no predictions, and (3) OCMS being partially functional. Although the above three likely scenarios resulting in full or partial deactivation of OCMS components are critical in governing its reliability, surprisingly, the WQ sensor network placement studies evaluating these scenarios have not yet been reported. In this direction, the current study attempts to close this gap in the state-of-the-art by developing a methodology for assessing the consequence of an OCMS and/or the associated SCADA system becoming only partly operational due to a cyber-physical attack. The study's findings would advance the state-of-the-art to enhance the procedure of placing an OCMS in WDS and assist the decision makers in water utilities and regulators to identify the critical sensors in an OCMS that necessitates increased security under possible cyber-physical attacks.

## 2. Materials and Methods

### 2.1. Methodology

The detailed methodology adopted in this study is schematically represented in Figure 1. The first step involves utilizing TEVA-SPOT to design an OCMS and develop the impact curve (i.e., the relation between the number of sensors deployed vs. the mean impact of possible contamination). The designing of an OCMS involves deciding on the optimal locations of placing a predefined number of WQ sensors ($\eta_{total}$) within a distribution

network to minimize contaminant intrusion impacts. In this regard, the objective function was selected as the mean volume of consumption of contaminated water before detection (Equation (1)).

$$V_c = \sum_{m=1}^{M} \sum_{j=1}^{J} \sum_{t=1}^{T_c} \hat{d}_{c,jt} \times \Delta t \quad (1)$$

where: $V_c$ = volume of contaminated water consumed before detection ($m^3$); $m$ = contaminant intrusion scenario index; $M$ = set of contaminant intrusion scenarios; $j$ = node index; $J$ = set of demand nodes; $t$ = time index; $T_c$ = set of time steps for which node $j$ receives contaminated water; $\hat{d}_{c,jt}$ = actual quantity of contaminated water supplied to node $j$ at time $t$ ($m^3/s$); and $\Delta t$ = time-step width (s).

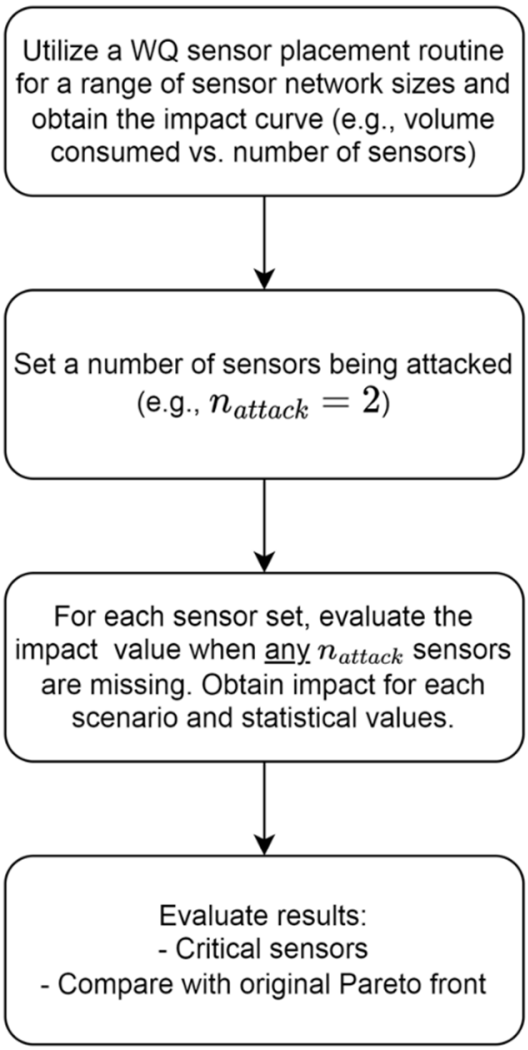


**Figure 1.** Schematic of the proposed methodology.

Once the OCMS was designed, the impact curve signifying the relationship between the mean volume of contaminated water consumed by the water consumers before detection of contaminant intrusion and the number of WQ sensors was generated. On generating the impact curves, it was assumed that there is no time delay in the WQ sensors for detecting contamination and that the WDS's operator response to contaminant-intrusion detection is instantaneous. In other words, the WQ sensors are activated instantly with contamination detection, and contaminant spread is controlled simultaneously by remedial measures such as the actuation of flushing units or by public notification to stop consuming water.

The second step of the methodology involves simulating cyber-physical attack scenarios and analyzing the designed OCMS performance under possible malfunctioning of its

components. As already mentioned, we are limiting to the case that the OCMS is partly functional after the attack, i.e., only those WQ sensors that have been attacked are entirely not giving out any signals (WQ predictions), and the remaining ones are fully operational. Though we could have accounted for the case in which the WQ sensors that were attacked are 'operational' but give out erroneous signals, we decided not to consider this because this might require advancing the methodology to distinguish between erroneous and proper signals. However, it could be noted that the proposed methodology is fully applicable even under such a case once the WQ sensor(s) giving out erroneous signals are pinpointed. Under a cyber-physical attack, only $\eta_{total} - \eta_{attack}$ WQ sensors would be functional within the OCMS.

The third step comprises assessing the impact value (mean volume of contaminated water consumed by the water consumers before detection of contaminant intrusion) when a predefined number ($\eta_{attack}$) of WQ sensors within the OCMS are under cyber-physical attack. This step involves determining all the possible combinations of functional WQ sensors. As the only information known is the $\eta_{attack}$ value and further whereabouts (locations) of the WQ sensors that could be non-operational are unknown, the number of possible sets of operational sensors is determined as ${}_{\eta_{total}} - {}^{\eta_{total}}_{\eta_{attack}} P$. For example, for $\eta_{total}$ and $\eta_{attack}$ values six and two, respectively, 360 possible combinations of operational WQ sensors would evolve, and all of them are individually considered to calculate the impact values.

The fourth and final step includes interpreting the results to demarcate the critical sensors and assess the overall reliability of an OCMS during a cyber-physical attack. For every $\eta_{total}$ value, ${}_{\eta_{total}} - {}^{\eta_{total}}_{\eta_{attack}} P$ impact values would be generated. From the generated sets of impact values, six values (minimum, 25th percentile, median, 75th percentile, maximum, and mean) are specifically picked to evaluate the effects of the cyber-physical attack on the reliability of contamination detection by the designed OCMS. The maximum impact value corresponds to the case when the in-effect OCMS with only the $\eta_{total} - \eta_{attack}$ number of WQ sensors under operation is not adequate to timely detect the contaminant intrusion incident. Therefore, those WQ sensors that may fall within the set of WQ sensors of length $\eta_{attack}$, subjected to cyber-physical attack, that gives out the maximum impact value could be deemed as the most critical WQ sensors within the OCMS.

### *2.2. Test Problem*

The test problem studied is the C-Town WDS (Figure 2), one of the benchmark networks employed in WDS engineering. This network, consisting of 429 pipes and 388 demand nodes, is based on a real-world, medium-sized network [21]. The WDS consists of five pressure zones, each controlled by one or two water tanks. In total, the network has seven tanks (T1 to T7), whose water level controls the operations of one valve. The network has 11 pumps, and they are spread across five pumping stations (S1 to S5). The pumping station S1 draws water from the only source and delivers it to Tank T1 and several demand nodes. The remaining four pumping stations pump the water from the lower elevation zone to four higher elevation zones, each controlled by water tanks.

In this study, we varied $\eta_{total}$ between 1 and 11 sensors and assumed that the number of sensors subjected to cyber-physical ($\eta_{attack}$) was two. We also analyzed an additional scenario with three WQ sensors under cyber-physical attack ($\eta_{attack}$ = 3) for the OCMS designed with $\eta_{total}$ = 6 to perceive the effects of $\eta_{attack}$ on the reliability of an OCMS under partial operational conditions. The cyber-physical attack scenario is not evaluated for the OCMS design with $\eta_{total}$ = 1, 2, and 3. Furthermore, for designed OCMS with $\eta_{total}$ > 8, the number of possible combinations to evaluate under a cyber-physical attack becomes very high (>181,440 combinations). Only 50,000 combinations were randomly selected to handle the computational complexity under such cases.

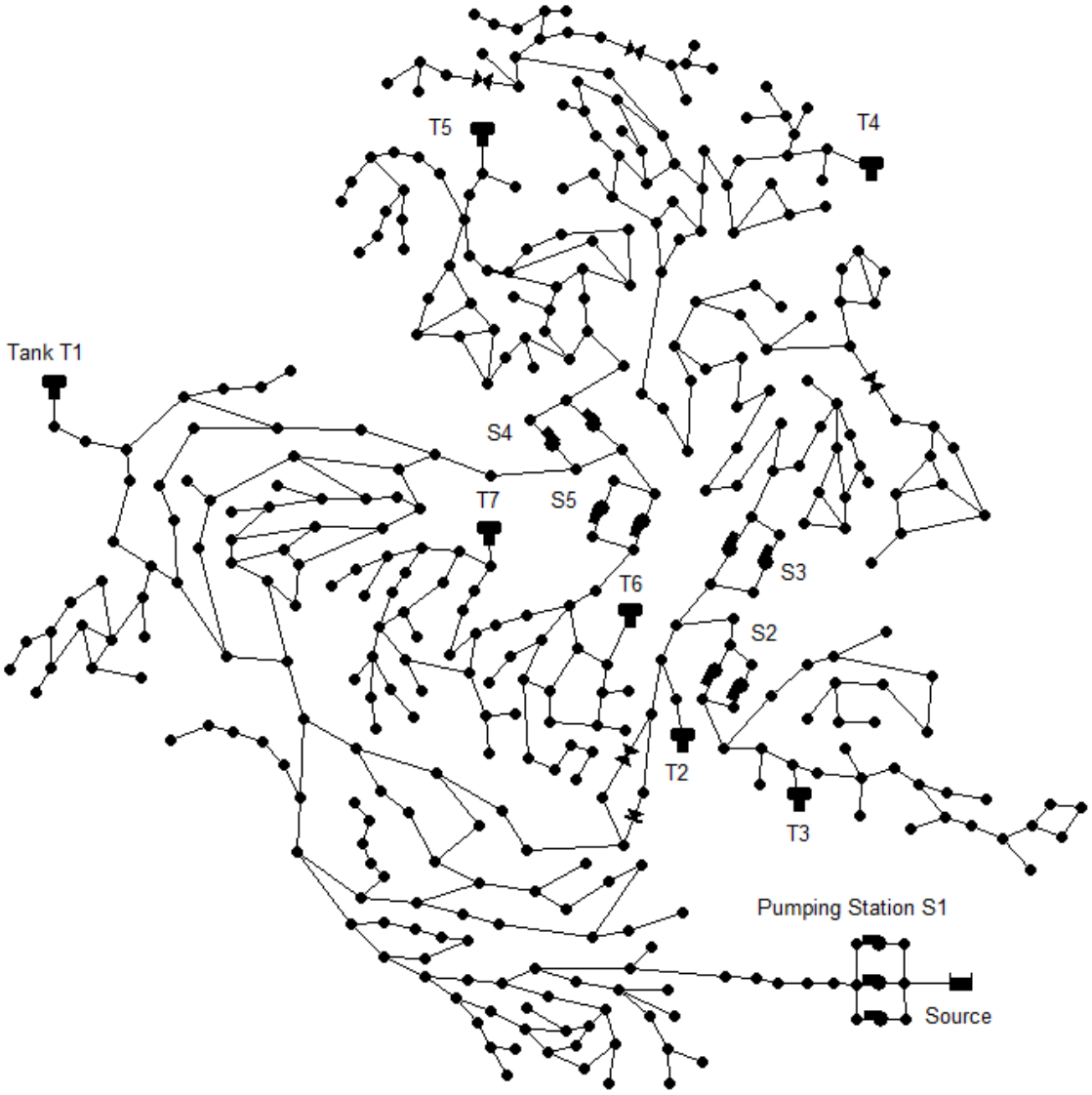


**Figure 2.** Test problem considered (the C-Town network). S1–S5 denotes the five pumping stations, and T1–T7 denotes the seven tanks.

## 3. Results and Discussion

### *3.1. Design of OCMS*

The TEVA-SPOT was applied to decide the optimal locations of placing the WQ sensors within the considered distribution network for minimizing the volume of contaminated water consumed during a contaminant intrusion event (Equation (1)). Diverse OCMS designs corresponding to $\eta_{total}$ = 1, 3, . . . , 11 were evolved by operating a total of 2328 contaminant intrusion scenarios for each $\eta_{total}$, i.e., six different contaminant intrusion scenarios corresponding to the time of intrusion for 388 demand nodes of the Test problem. Increasing the value of $\eta_{total}$ from 1 to 11 enabled us to explore the effects of the successive increase in the WQ sensors' number on minimizing the contaminant intrusion impacts. The spatial distribution of the WQ sensors for the case with $\eta_{total}$ = 5 and 6 is illustrated in Figure 3.

As can be seen from Figure 3, some similarities are apparent between the two designs. The locations corresponding to nodes J109, J239, J352, and J67 emerged as the optimal locations for WQ sensor placement in both the OCMS designs corresponding to $\eta_{total}$ = 5 and 6. However, instead of node J492, J131 and J385 came out as the optimal locations for WQ

sensor placement when the $\eta_{total}$ value was increased from five to six. Altogether, the OCMS designs obtained revealed its high sensitivity to the $\eta_{total}$ value.

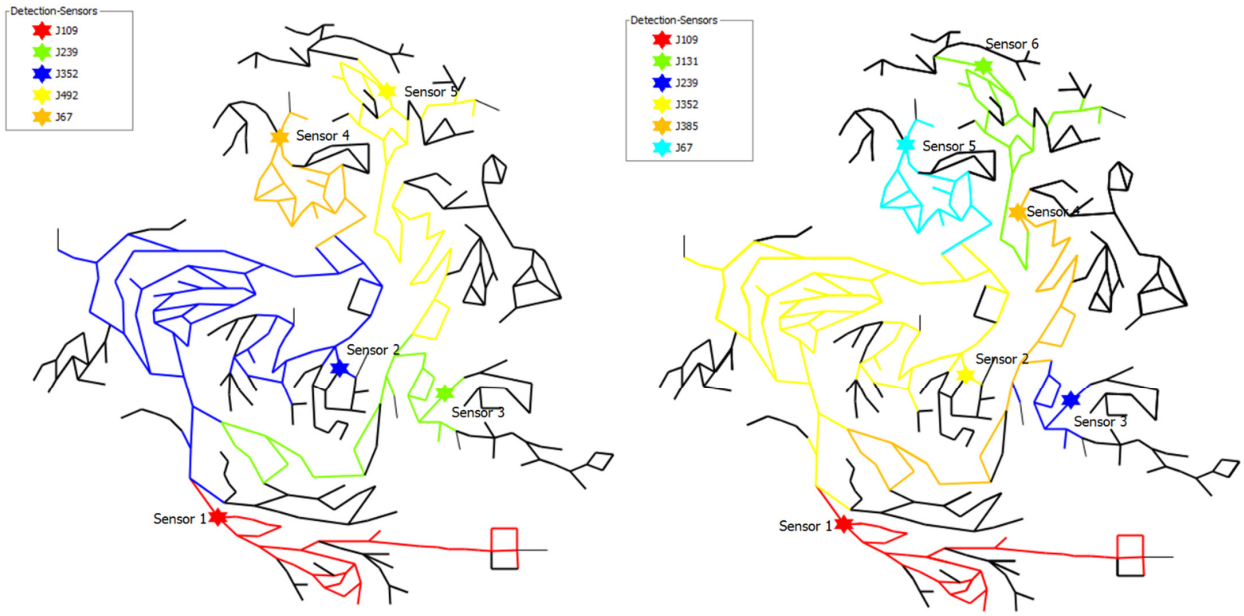


**Figure 3.** OCMS designs generated with TEVA-SPOT for $\eta_{total}$ = 5 (**left**) and 6 (**right**).

### *3.2. Determination of Impact Values*

The variations of the impact values determined for different OCMS designs (corresponding to $\eta_{total}$ = 2, 3, . . . , 11) versus the number of WQ sensors (Figure 4 and Table 1) exposed the significant impact of the $\eta_{total}$ value on any OCMS performance. In the absence of an OCMS within the distribution network, the mean impact value during contamination intrusion was estimated as 10,138 $m^3$ (Table 1). Introducing an OCMS with only one WQ sensor was found capable of reducing the above value to 2161 $m^3$, i.e., by ~79%. Introducing an additional WQ sensor further reduced the impact value by 95%. Simultaneously, the stage-wise reduction (between adding one WQ sensor and adding two WQ sensors within the distribution network) in the impact value decreased from 95 to 76%.

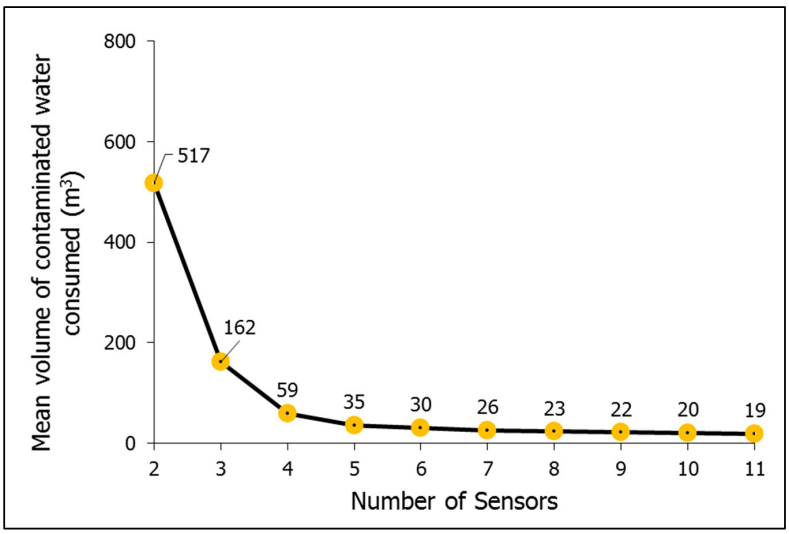


**Figure 4.** Mean volume of contaminated water consumed before detection during a contaminant intrusion event versus number of sensors under a normal scenario ($\eta_{attack}$ = 0).

**Table 1.** Impact values obtained with and without cyber-physical attack of WQ sensors.

| Number of Sensors ($\eta_{total}$) | Normal Scenario ($\eta_{attack}$ = 0) | Cyber-Physical Attack Scenario ($\eta_{attack}$ = 2) | |
|---|---|---|---|
| | Mean Impact Value ($m^3$) | Mean Impact Value ($m^3$) | Median Impact Value ($m^3$) |
| 0 | 10,138 | - | - |
| 1 | 2161 | - | - |
| 2 | 517 | - | - |
| 3 | 162 | - | - |
| 4 | 59 | 1282 | 1033 |
| 5 | 35 | 911 | 590 |
| 6 | 30 | 525 | 464 |
| 7 | 26 | 338 | 370 |
| 8 | 23 | 225 | 154 |
| 9 | 22 | 197 | 127 |
| 10 | 20 | 166 | 119 |
| 11 | 19 | 136 | 37 |

Intriguingly, the subsequent introduction of WQ sensors (increase in the $\eta_{total}$ values) failed to engender comparable effects corresponding to adding only two WQ sensors within the network. As seen in Figure 4, even though the overall reduction in the impact value improved from 95 to 98% by increasing the $\eta_{total}$ value from 2 to 3, the stage-wise reduction dropped to 69%. Likewise, a steady drop in the stage-wise reduction in the impact values was evident with the subsequent increase in the $\eta_{total}$ values. Beyond $\eta_{total}$ = 5, the variations in the overall reduction in the impact value remained almost unnoticeable. The consequent effects of minimizing the extent of contaminant spread within the C-Town network also became nearly constant (Figure 4). Therefore, for the test problem analyzed, an OCMS design with $\eta_{total}$ = 5 could be considered 'best' to minimize contaminant intrusion impacts. However, as previously mentioned, such a conclusion is classically made only by making a tradeoff between the impact values and the cost of implementing and operating an OCMS. Moreover, this study attempts to explore the implications of factors such as the reliability of an OCMS under cyber-physical attacks towards making these conclusions.

### *3.3. Evaluating the Cyber-Physical Attack Scenarios*

The impact values obtained by considering cyber-physical attack scenarios corresponding to $\eta_{attack}$ = 2 are detailed in Table 1. Figure 5 also schematically illustrates the variations in the impact values corresponding to scenarios under which the designed OCMS with $\eta_{total}$ = 4, 5, 6, 7, and 8 are subjected to cyber-physical attacks, and the number of available WQ sensors within the OCMS is reduced to 2, 3, 4, 5, and 6, respectively.

Intriguingly, after analyzing 12 different combinations of operational WQ sensors, a ~21 times increase in the mean impact value was detected when the OCMS design with $\eta_{total}$ = 4 was subjected to a cyber-physical attack. As seen in Figure 5, the maximum impact value (2706 $m^3$) was almost 111% greater than the mean value. For the OCMS design with $\eta_{total}$ = 5, although the magnitude of the mean impact value obtained under a cyber-physical attack was lower than the case with $\eta_{total}$ = 4, the relative increment in the value (~25 times) was more substantial. Furthermore, the maximum impact value for the OCMS design with $\eta_{total}$ = 5 obtained after analyzing 60 possible combinations of operational WQ sensors was found to be ~188% higher than the mean value. However, similar to the mean impact value, this value (2631 $m^3$) was also lower than that obtained for the OCMS design with $\eta_{total}$ = 4. Nevertheless, the relative decrease in the mean and maximum impact values for the OCMS design with $\eta_{total}$ = 5 from that with $\eta_{total}$ = 4 was estimated as ~29 and ~3%, respectively. Similar outcomes were derived when 360 different possible combinations of cyber-physical attack scenarios were analyzed for the OCMS design with $\eta_{total}$ = 6.

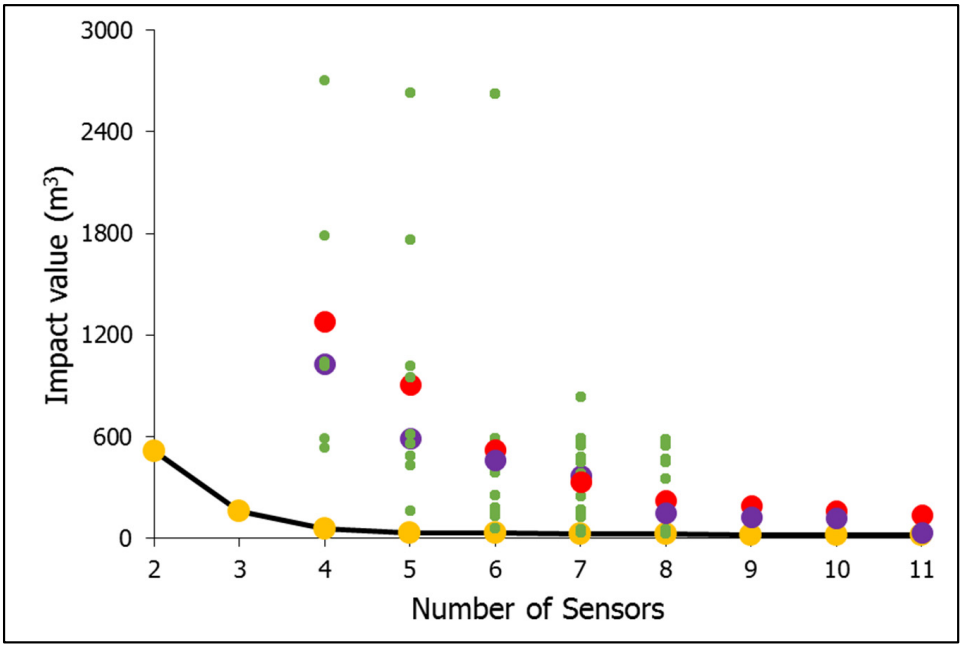


**Figure 5.** Variations in the impact values corresponding to scenarios under which the designed OCMS are subjected to cyber-physical attacks. The green circles indicate the impact values obtained for OCMS with $\eta_{total}$ = 4, 5, 6, 7, and 8. The red and violet circles signify the mean and median impact values, respectively. The black line with yellow circles denotes the mean impact values in the absence of a cyber-physical attack.

Relative to the OCMS with $\eta_{total}$ = 6, the OCMS with $\eta_{total}$ = 7 was observed to be more resilient to the malfunctioning of the WQ sensors. As seen in Table 1 and Figure 5, the mean impact value under the cyber-physical attack scenario was 13 times higher than that under the absence of the same for the OCMS with $\eta_{total}$ = 7. Even though the reduction in the mean impact value is not very noteworthy compared to the case of OCMS with $\eta_{total}$ = 6, the decrease in the maximum value appeared relatively significant. The maximum impact value obtained for the OCMS with $\eta_{total}$ = 6 under a cyber-physical attack was 2624 $m^3$. On the contrary, the same value found for the OCMS with $\eta_{total}$ = 7 (after considering 2520 cyber-physical attack scenarios) was ~68% lower (i.e., 835 $m^3$).

This shows that although not many changes are attributable between the performances of the two OCMS designs with $\eta_{total}$ = 6 and 7 under normal conditions (absence of a cyber-physical attack), significant variations appear when the WQ sensors' malfunction is accounted for under possible cyber-physical attacks. Increasing the WQ sensors' number from 7 to 8 also significantly improved minimizing the contamination spread during a contaminant intrusion concurrently under a cyber-physical attack (Table 1 and Figure 5). Overall, the results stress the importance of considering cyber-physical attacks and potential malfunctioning of the OCMS components in designing and evaluating the OCMS in WDS.

### *3.4. Identifying Critical WQ Sensors in an OCMS*

Each cyber-physical attack scenario analyzed signifies the case of only $\eta_{total} - \eta_{attck}$ WQ sensors out of $\eta_{total}$ within the OCMS being operational. Figure 6 schematically illustrates the variations in the impact values over the 360 cyber-physical attack scenarios (possible combinations of four WQ sensors out of six) considered for the designed OCMS with $\eta_{total}$ = 6. The values were found to vary between 60 and 2624 $m^3$, with 525 $m^3$ and 464 $m^3$ as the mean and median values, respectively.

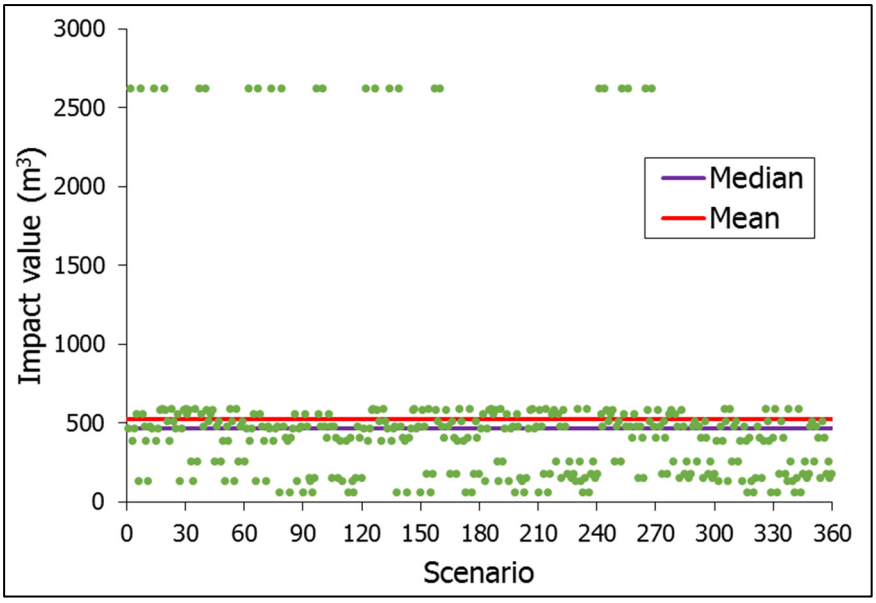


**Figure 6.** Impact values (green circles) corresponding to the scenario under which the designed OCMS with $\eta_{total}$ = 6 is subjected to a cyber-physical attack ($\eta_{attack}$ = 2).

Both the minimum (60 $m^3$) and maximum (2624 $m^3$) impact values were repeated 24 times (out of 360). From a closer look, the WQ sensors at locations J67 and J352 were absent in all $\eta_{total} - \eta_{attck}$ numbers of operational WQ sensor combinations that gave out the maximum value. Similarly, in all 24 combinations where we obtained the minimum value, the WQ sensors at the above two locations were present. This indicated the significance of these two WQ sensors in governing the performance of the designed OCMS. Their presence or absence dictated the celerity with which the OCMS detected a contaminant intrusion scenario within the Test problem with four available WQ sensors. Thus, from the results obtained, J67 and J352 can be demarcated as the critical WQ sensors corresponding to the designed OCMS with $\eta_{total}$ = 6.

However, it may be noted that the critical WQ sensors for other OCMS designs corresponding to different $\eta_{total}$ values could be entirely dissimilar. Hence, making a general conclusion about the critical locations of WQ sensors within the C-Town network would be illogical. Since fully securing the OCMS against any form of cyber-physical attacks is essentially impossible, the above-mentioned straightforward approach could enable water utility managers to recognize the critical locations of the WQ sensors and introduce additional security measures to prevent their malfunctioning and improve the overall reliability of the OCMS system.

### *3.5. Determining the Optimal Number of WQ Sensors in an OCMS*

Figure 7 gives an overall depiction of all the scenarios analyzed—with and without cyber-physical attacks. The results indicate an alarming increase in the spread of contamination during a cyber-physical attack. For example, from analyzing 2328 scenarios for the designed OCMS with four WQ sensors, the maximum volume of contaminated water consumed before detecting a contaminant intrusion within the C-Town network was estimated as 729 $m^3$. However, this value increased ~3.7 times during a cyber-physical attack scenario. Intriguingly, for the designed OCMS with $\eta_{total}$ = 5 and 6, the relative increase in the maximum impact values was much higher (~6.6 and ~8.4 times, respectively). Moreover, the decline in the curves representing the variations in the maximum impact value versus the number of WQ sensors was also found to be entirely different for the cases with and without cyber-physical attacks (Figure 7).

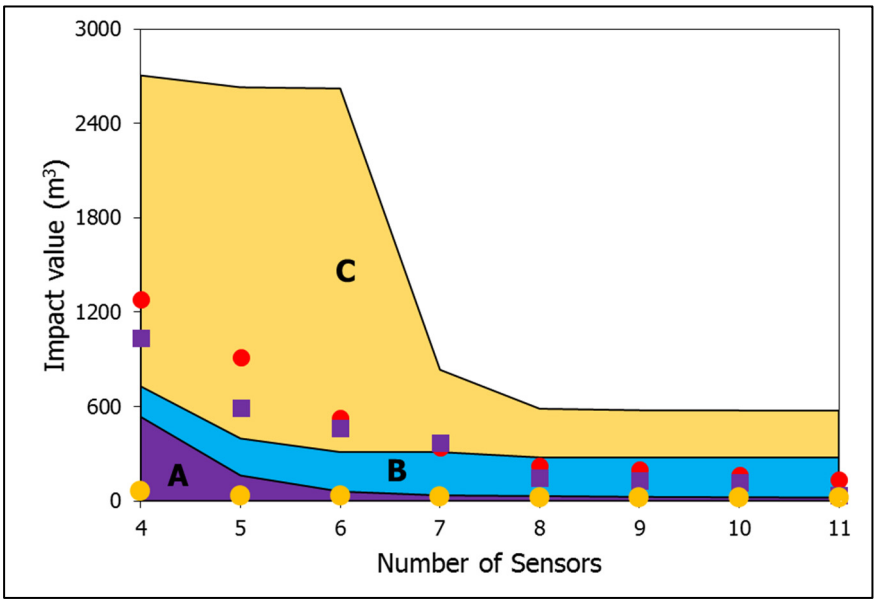


**Figure 7.** Impact values corresponding to normal and cyber-physical attack scenarios for the OCMS with $\eta_{total}$ = 4, 5, . . . , 11. The yellow circles signify the mean impact value under a normal scenario. The red circles and violet squares indicate the mean and median impact values under cyber-attack scenarios, respectively. The violet region (**A**) denotes the area between the minimum impact values corresponding to normal and cyber-physical attack scenarios. The blue region (**B**) signifies the area between the maximum impact values corresponding to normal scenarios and minimum impact values corresponding to cyber-physical attack scenarios. The yellow region (**C**) denotes the area between the maximum impact values corresponding to normal and cyber-physical attack scenarios.

Nevertheless, a peculiar decline in the curves mentioned above was observed when the number of WQ sensors was increased beyond six. The maximum impact value under a cyber-physical attack scenario for an OCMS designed with seven WQ sensors was found to be 338 $m^3$. This value was only ~2.7 times higher than the value obtained under a normal scenario and was much lower than that obtained with $\eta_{total}$ = 6. As expected, the extent of contaminant spread declined with increasing the number of WQ sensors within the distribution network beyond seven. However, beyond the $\eta_{total}$ value 8, increasing the number of WQ sensors failed to induce significant differences in the maximum impact value (Figure 7). Between $\eta_{total}$ = 8 and 9, the relative decline in the maximum impact value under cyber-physical attack scenario was obtained as just 1.6%. Between $\eta_{total}$ = 9 and 10, this figure further dropped to a mere 0.2%. These results signify that even with 10 WQ sensors, the volume of contaminated water that could be consumed before detecting a contaminant intrusion under a cyber-physical attack might be as high as ~576 $m^3$. This number is startling because, in the absence of a cyber-physical attack, the maximum volume of contaminated water that could be consumed before detecting a contaminant intrusion would be only ~397 $m^3$, with just five WQ sensors optimally placed. With eight sensors, this value could even be reduced to 277 $m^3$, i.e., almost half of that obtained under a cyber-physical attack (with eight operating WQ sensors out of ten).

Thus, from a detailed analysis of the results, it can be concluded that under cyber-physical attacks and potential malfunctioning of the WQ sensors, it is virtually impossible to minimize the spread of contamination beyond a certain degree if the OCMS is designed following a conventional approach (overlooking the scenarios of WQ sensors operation being compromised). Altogether, from the results, eight can be interpreted as the number of sensors that need to be placed within the C-Town network to minimize contamination spread. However, this figure cannot be deemed optimal because the OCMS designs corresponding to $\eta_{total}$ > 11 were not analyzed under cyber-physical attacks. Moreover,

the results discussed above only correspond to the scenarios of only two WQ sensors being attacked.

Figure 8 schematically illustrates the variations in the statistical values obtained for the designed OCMS with $\eta_{total}$ = 6 when the $\eta_{attck}$ value was increased from 2 to 3. A substantial increase in the impact values was evident when 120 different scenarios were analyzed with three WQ sensors malfunctioning instead of two (Figure 8). The mean impact value increased from 30 $m^3$ under no cyber-physical attack to 1054 $m^3$ when only three (out of six) were functional under contaminant intrusion events. This was almost twice what we obtained when four (out of six) were operational. In total, these results signify the importance of considering different cyber-physical attack scenarios in analyzing the reliability of the OCMS designed with the traditional approach using the TEVA-SPOT. Moreover, these results imply that the inference on the optimal number of WQ sensors required for an OCMS can be arrived at only by making a cost–benefit tradeoff by interpreting the designs obtained concurrently varying the $\eta_{total}$ and $\eta_{attack}$ values within valid ranges.

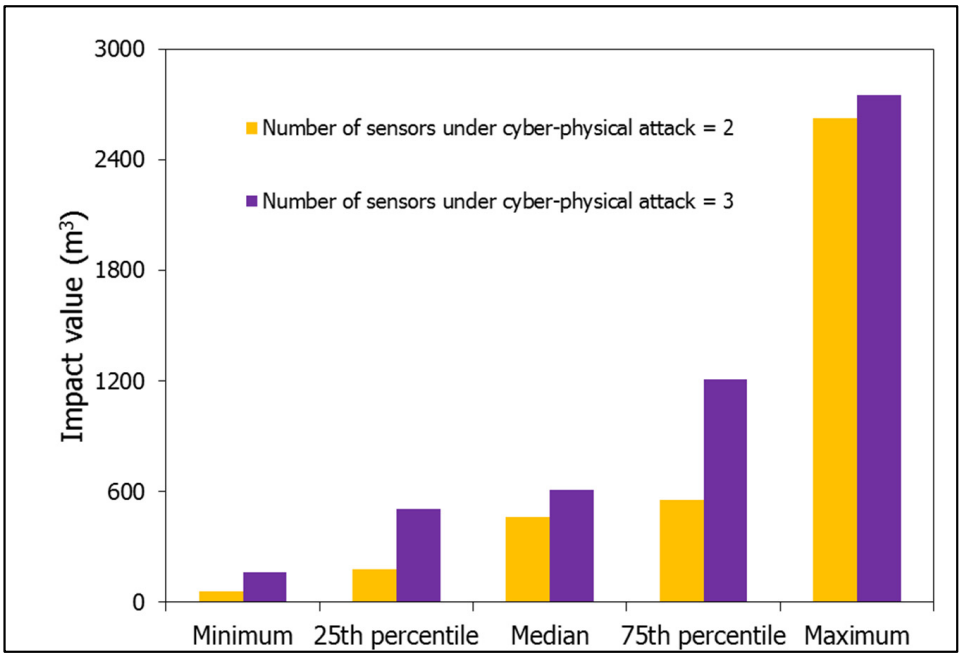


**Figure 8.** Impact values corresponding to the scenario under which two and three WQ sensors of the designed OCMS with $\eta_{total}$ = 6 is malfunctioning.

### *3.6. Defining the Reliability of an OCMS Subjected to Cyber-Physical Attacks*

Carefully looking at the mean and median impact values (Figure 7) provides some interesting insights into the performance of designed OCMS under cyber-physical attack scenarios. As seen in Figure 7, the mean impact values were found to be greater than the corresponding median values for almost all the OCMS designs. Even under normal scenarios, the same trend was observed. For example, for the designed OCMS with $\eta_{total}$ = 1, the mean impact value under a normal scenario was obtained as 2161 $m^3$. However, the corresponding median value was only 35 $m^3$. This shows that the mean impact value estimated from diverse contaminant intrusion scenarios is entirely controlled by the outliers, specifically the maximum impact values. Comparing the other statistical figures (25th percentile = 6 $m^3$ and 75th percentile = 451 $m^3$, respectively) also proves that under the majority of the scenarios, the impact value is much lower than the mean impact value. These results stress the significance of recognizing critical sensor locations within a designed OCMS.

An associated question would be which statistical value among the mean and median of the impact values would be pragmatic to better interpret and analyze the reliability of

a designed OCMS under cyber-physical attacks. We presume that considering only the mean of the impact values obtained under scenarios with and without attack would only give an incomplete picture of the performance of the OCMS. Similarly, only accounting for the median of the impact values might not reflect the worst-case settings with respect to contaminant spread as well. Towards formulating reliability indices, the best approach would be accounting for all of the five statistical values (as shown in Figure 8) along with the mean. However, this could over-complicate the formulation. Moreover, this could constrain its applicability in an optimization model for designing the WQ sensor locations. Therefore, considering all the above aspects, we propose a straightforward reliability index formulation that considers both the mean and median impact values (Equations (2)–(4)) that can be easily incorporated as a constraint or a penalty variable in the objective function.

$$f_{mean} = 1 - \frac{IV_{\eta_{total}-\eta_{attck},\, mean} - IV_{\eta_{total},\, mean}}{IV_{\eta_{total}-\eta_{attck},\, mean}} \tag{2}$$

$$f_{median} = 1 - \frac{IV_{\eta_{total}-\eta_{attck},\, median} - IV_{\eta_{total},\, median}}{IV_{\eta_{total}-\eta_{attck},\, median}} \tag{3}$$

$$f(\eta_{total}, \eta_{attck}) = \frac{1}{2} \times [f_{mean} + f_{median}] \tag{4}$$

where: $f_{mean}$ and $f_{median}$ = reliability index values corresponding to mean and median impact values for an OCMS subjected to cyber-physical attack; $f$ = effective reliability index; $IV_{\eta_{total},mean}$ and $IV_{\eta_{total},median}$ = mean and median impact values obtained under a normal scenario; and $IV_{\eta_{total}-\eta_{attck},\, mean}$ and $IV_{\eta_{total}-\eta_{attck},\, median}$ = mean and median impact values corresponding to a cyber-physical attack scenario.

The $f$ value is a function of $\eta_{total}$ and $\eta_{attack}$ for a specific WDS. Its value equal to 1 signifies that the designed OCMS is fully reliable and performs without any flaw, even under a cyber-physical attack. On the contrary, higher $f$ values indicate that the capability of an OCMS to minimize contaminant intrusion impacts is significantly affected by the malfunctioning of $\eta_{attack}$ number of WQ sensors.

Since the mean impact values are susceptible to outliers, $f_{mean}$ is expected to reflect more on the cases where the critical sensors are malfunctioning. Therefore, we believe that taking the sum of both $f_{mean}$ and $f_{median}$ in Equation (4) is expected to incorporate the overall effects of cyber-physical attacks on WQ sensors in a better way.

## 4. Conclusions

In this study, we have developed and demonstrated a methodology for evaluating the impacts of cyber-physical attacks on a designed OCMS, partially malfunctioning its components and compromising its functionality. Varied OCMS designs corresponding to the number of WQ sensors varying between 1 and 11 were developed by analyzing 2328 contaminant intrusion scenarios for the well-tested C-Town network using TEVA-SPOT, one of the widely applied tools for optimally deciding sensor locations. Minimizing the volume of contaminated water consumed during a contaminant intrusion event was adopted as the objective function.

From a superficial interpretation of the results, an OCMS design with five fully operational WQ sensors arrived as the 'best' to minimize contaminant intrusion impacts. The maximum volume of contaminated water that could be consumed before detecting a contaminant intrusion was determined as 397 $m^3$. Significant variations in the predictions on contaminant spread within the distribution network became apparent when scenarios corresponding to possible cyber-physical attacks and malfunctioning of any two random WQ sensors were accounted for. The obtained results signified that even with ten WQ sensors, the volume of contaminated water that could be consumed before detecting a contaminant intrusion under a cyber-physical attack might be as high as 576 $m^3$. The simulation outcomes also established that under cyber-physical attacks, it is virtually unattainable to

minimize the spread of contamination beyond a certain degree if the OCMS is designed overlooking the scenarios of WQ sensor operation being compromised partially/fully.

A detailed look into the results also highlighted that the presence or absence of specific WQ sensors is vital in dictating the celerity with which the OCMS could detect a contaminant intrusion scenario within the C-Town network. A straightforward approach for demarcating these locations within the distribution network was derived and explained. In addition, we have also proposed a simple reliability index formulation that can be incorporated easily into the sensor-placement optimization problem to evolve OCMS designs with enhanced reliability against cyber-physical attacks. Altogether, the findings of the presented study could be deemed beneficial in examining the performance of sensor networks under accidental/intentional malfunctioning, providing valuable information for decision makers in water utilities and regulators, and enhancing the planning and development of WDS operation [22].

**Author Contributions:** Conceptualization, E.S. and A.O.; methodology, E.S. and A.O.; software, E.S.; validation, E.S. and A.O.; formal analysis, E.S.; investigation, E.S. and A.O.; resources, E.S. and A.O.; data curation, E.S., G.R.A. and A.O.; writing—original draft preparation, G.R.A.; writing—review and editing, E.S. and A.O.; visualization, E.S. and G.R.A.; supervision, A.O.; project administration, A.O.; funding acquisition, A.O. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work is (partially) supported by the Trudy Mandel Louis Charitable Trust.

**Data Availability Statement:** Data available on request.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. El-Chakhtoura, J.; Saikaly, P.E.; Van Loosdrecht, M.C.M.; Vrouwenvelder, J.S. Impact of Distribution and Network Flushing on the Drinking Water Microbiome. *Front. Microbiol.* **2018**, *9*, 2205. [CrossRef] [PubMed]
2. Lindley, T.R.; Buchberger, S.G. Assessing Intrusion Susceptibility in Distribution Systems. *J. Am. Water Work. Assoc.* **2002**, *94*, 66–79. [CrossRef]
3. Liang, J.L.; Dziuban, E.J.; Craun, G.F.; Hill, V.; Moore, M.R.; Gelting, R.J.; Calderon, R.L.; Beach, M.J.; Roy, S.L. Surveillance for Waterborne Disease and Outbreaks Associated with Drinking Water and Water Not Intended for Drinking—United States, 2003–2004. *MMWR Surveill Summ.* **2006**, *55*, 31–65. [PubMed]
4. Yokoyama, K. Our Recent Experiences with Sarin Poisoning Cases in Japan and Pesticide Users with References to Some Selected Chemicals. *Neurotoxicology* **2007**, *28*, 364–373. [CrossRef] [PubMed]
5. American Society of Civil Engineers (ASCE). *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*; American Society of Civil Engineers: Reston, VA, USA, 2004.
6. Ostfeld, A.; Kessler, A.; Goldberg, I. A Contaminant Detection System for Early Warning in Water Distribution Networks. *Eng. Optim.* **2004**, *36*, 525–538. [CrossRef]
7. Preis, A.; Whittle, A.; Ostfeld, A. Multi-Objective Optimization for Conjunctive Placement of Hydraulic and Water Quality Sensors in Water Distribution Systems. *Water Sci. Technol. Water Supply* **2011**, *11*, 166–171. [CrossRef]
8. Nikolopoulos, D.; Ostfeld, A.; Salomons, E.; Makropoulos, C. Resilience Assessment of Water Quality Sensor Designs under Cyber-Physical Attacks. *Water* **2021**, *13*, 647. [CrossRef]
9. Ostfeld, A.; Salomons, E. Optimal Layout of Early Warning Detection Stations for Water Distribution Systems Security. *J. Water Resour. Plan. Manag.* **2004**, *130*, 377–385. [CrossRef]
10. Zhao, Y.; Schwartz, R.; Salomons, E.; Ostfeld, A.; Poor, H.V. New Formulation and Optimization Methods for Water Sensor Placement. *Environ. Model. Softw.* **2016**, *76*, 128–136. [CrossRef]
11. Lee, B.H.; Deininger, R.A.; Clark, R.M. Locating Monitoring Stations in Water Distribution Systems. *J. Am. Water Work. Assoc.* **1991**, *83*, 60–66. [CrossRef]
12. Harmant, P.; Nace, A.; Kiene, L.; Fotoohi, F. Optimal Supervision of Drinking Water Distribution Network. In Proceedings of the 29th Annual Water Resources Planning and Management Conference, Tempe, AR, USA, 6–9 June 1999; ASCE: Tempe, AR, USA, 1999; pp. 1–11.
13. Al-Zahrani, M.A.; Moied, K. Locating Optimum Water Quality Monitoring Stations in Water Distribution System. In *World Water and Environmental Resources Congress 2001*; ASCE: Orlando, FL, USA, 2004; Volume 111, pp. 1–9.
14. Kessler, A.; Ostfeld, A.; Sinai, G. Detecting Accidental Contaminations in Municipal Water Networks. *J. Water Resour. Plan. Manag.* **1998**, *124*, 192–198. [CrossRef]

15. Ostfeld, A.; Uber, J.G.; Salomons, E.; Berry, J.W.; Hart, W.E.; Phillips, C.A.; Watson, J.-P.; Dorini, G.; Jonkergouw, P.; Kapelan, Z.; et al. The Battle of the Water Sensor Networks (BWSN): A Design Challenge for Engineers and Algorithms. *J. Water Resour. Plan. Manag.* **2008**, *134*, 556–568. [CrossRef]
16. Gong, W.; Suresh, M.A.; Smith, L.; Ostfeld, A.; Stoleru, R.; Rasekh, A.; Banks, M.K. Mobile Sensor Networks for Optimal Leak and Backflow Detection and Localization in Municipal Water Networks. *Environ. Model. Softw.* **2016**, *80*, 306–321. [CrossRef]
17. Sankary, N.; Ostfeld, A. Bayesian Localization of Water Distribution System Contamination Intrusion Events Using Inline Mobile Sensor Data. *J. Water Resour. Plan. Manag.* **2019**, *145*, 4019029. [CrossRef]
18. Oliker, N.; Ostfeld, A. Inclusion of Mobile Sensors in Water Distribution System Monitoring Operations. *J. Water Resour. Plan. Manag.* **2016**, *142*, 4015044. [CrossRef]
19. Cao, H.; Hopfgarten, S.; Ostfeld, A.; Salomons, E.; Li, P. Simultaneous Sensor Placement and Pressure Reducing Valve Localization for Pressure Control of Water Distribution Systems. *Water* **2019**, *11*, 1352. [CrossRef]
20. Berry, J.; Boman, E.; Riesen, L.A.; Hart, W.E.; Phillips, C.A.; Watson, J.-P. *User's Manual TEVA-SPOT Toolkit. Version 2.5.2*; United States Environmental Protection Agency: Cincinnati, OH, USA, 2012.
21. Price, E.; Ostfeld, A. Battle of Background Leakage Assessment for Water Networks Using Successive Linear Programing. In Proceedings of the 16th Conference on Water Distribution System Analysis, WDSA 2014, Bari, Italy, 14–17 July 2014; Elsevier: Bari, Italy, 2014; Volume 89, pp. 45–52.
22. Lungariya, P.; Katharotiya, N.; Mehta, D.; Waikhom, S. Analysis of Continuous Water Distribution in Surat City Using EPANET: A Case Study. In Proceedings of the 1st National Conference on Recent Advances in Civil Engineering for Global Sustainability (RACEGS-2016), Surat, India, 29–30 March 2016. [CrossRef]