Computers and Chemical Engineering 87 (2016) 246–256

Contents lists available at ScienceDirect

Computers and Chemical Engineering

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

Sensor network design for contaminant detection and identification in water distribution networks

Venkata Reddy Palleti[a], Shankar Narasimhan[a,*], R. Rengaswamy[a], Ravi Teja[b], S. Murty Bhallamudi[b]

[a] Department of Chemical Engineering, Indian Institute of Technology Madras, Chennai 600036, India
[b] Department of Civil Engineering, Indian Institute of Technology Madras, Chennai 600036, India

ARTICLE INFO

Article history:
Received 6 August 2015
Received in revised form
15 December 2015
Accepted 28 December 2015
Available online 4 February 2016

Keywords:
Water distribution network
Contaminant detection
Observability
Identifiability
Bipartite graph

ABSTRACT

Water distribution networks (WDN) are vulnerable to either intentional or accidental contamination. In order to protect against such intrusions, effective and efficient online monitoring systems are needed. Due to cost and maintenance reasons, it is not possible to locate sensors at each and every potential intrusion point. In this work, we design minimal sensor networks which satisfy the two important properties of observability (ability to detect an intrusion) and identifiability (ability to identify the point of intrusion). Based on the hydraulic analysis of the network, a bipartite graph is constructed between intrusion points and the corresponding nodes that can potentially be affected by the contaminant. The problem of sensor network design is converted to a minimum set cover problem on the bipartite graph, and is solved using a greedy heuristic algorithm. The proposed method is illustrated using a medium scale urban WDN.

1. Introduction

Water distribution networks (WDNs) are a vital part of any city. Water distribution networks consist of a network of pipes, reservoirs, pumps, valves, storage tanks and sumps. Any contamination that enters the WDN can adversely impact a large section of the population. Intrusions to the WDNs can be due to either accidental or intentional contamination. Accidental contamination occurs due to the failure of network elements such as pipes and joints. The most serious threat to the water distribution system is intentional contamination. It can either be physical or chemical attacks. The physical disruption of the network leads to significant economic loss but does not pose any threat to human beings. In contrast to physical attacks, introduction of chemical or biological contaminants into the network poses a direct threat to the human population and may cause widespread disease and death. In order to guard against such intrusions, an effective and efficient monitoring system through online sensors is needed. Due to cost and operational reasons, it is not possible to locate sensors at each and every potential point of intrusion. It is required to optimally choose the sensor locations and minimize the number of sensors used for effective monitoring. Several factors such as the ability to detect and identify the point of intrusion, the expected time required to detect an intrusion, the number of people that may be affected prior to detection and containment of intrusion, etc. have to be considered while designing such sensor networks.

The problem of sensor network design for WDNs has been considered by several researchers in recent times. Lee and Deininger (1992) have addressed the problem of optimal sensor locations in water distribution network for monitoring the quality of the water supplied to customers. The sensor locations are chosen to maximize the demand coverage. The water quality at a demand node is said to be covered (or monitored), if the water quality of a node upstream of the demand node is measured, and a minimum specified fraction of the demand flows through that node. The problem of sensor network design is formulated as an integer program that maximizes the demand coverage. Kumar et al. (1997) applied a greedy heuristic to solve the integer program formulation of Lee and Deininger (1992) to deal with large networks. Kessler et al. (1998) developed a method for locating sensors for a given level of service. The level of service is defined as the maximum volume of contaminated water consumed prior to detection of a contaminant. A matrix of 0-1 coefficients, termed as pollution matrix (PM) was constructed based on the maximum contaminated volume (i.e., the level of service). The sensor network design problem is formulated and solved as a minimum set cover problem.

---

* Corresponding author. Tel.: +91 44 22574165.
E-mail address: naras@iitm.ac.in (S. Narasimhan).

http://dx.doi.org/10.1016/j.compchemeng.2015.12.022

Ostfeld and Salomons (2004) improved the study of Kessler et al. (1998) by considering multiple demand loadings and unsteady water quality propagation conditions. They constructed a randomized pollution matrix (RPM) and used genetic algorithm (GA) for solving the optimization problem. Berry et al. (2005) presented an integer programming formulation for sensor placement which minimizes the expected fraction of the population at risk. Later, Shastri and Diwekar (2006) modified the model proposed by Berry et al. (2005) by incorporating the nodal demand uncertainties in the objective function. Propato (2006) proposed a mixed-integer linear programming (MILP) model to identify optimal sensor locations which can be applied to steady or unsteady state hydraulic conditions. Initially, a 0-1 polynomial programming problem is proposed and then it is transformed to MILP formulation. Furthermore, the formulation can accommodate various design objectives such as time to detection, population exposed, contaminated water consumed, and number of failed detections.

Over the last decade, the focus has gradually moved to multiple objective formulations. Watson et al. (2004) were probably the first to propose a multiple-objective formulation for sensor placement using a mixed-integer linear programming model. They have considered the objectives such as population exposed, time to detection, weighted volume consumed, failed detections and extent of contamination. Ostfeld et al. (2008) described a multi-objective sensor network design competition for water networks called as the Battle of Water Sensor Networks (BWSN), and discussed the solutions provided by fifteen independent research groups who participated in this competition. The following four objectives were considered in the BWSN problem: (1) Expected time of detection. (2) Expected population affected prior to detection. (3) Expected consumption of contaminated water prior to detection. (4) Detection likelihood. Aral et al. (2010) developed a single-objective optimization model that incorporates all the four criteria proposed in BWSN and solved it using a Progressive Genetic Algorithm (PGA) for dealing with large scale WDNs. Various methodologies were developed to reduce the computational complexity in dealing with the large scale complex WDNs for sensor placement (Chang et al., 2012; Klise et al., 2013). Recently, Ohar et al. (2015) studied the optimal placement of water quality sensors in WDNs which exploits the chemical reactions between organophosphate contaminants and free chlorine.

The objectives that have been considered so far in sensor network design for WDNs focus essentially on the effect of the contaminant on the population served. An important objective that is not considered is the ability of the sensor network to identify the source of contamination. If the exact source of intrusion can be identified based on the response of the sensors, it can help water authorities to take corrective action (such as shutting down the appropriate sub-network) in order to prevent or minimize the impact on the population served by the WDN. Furthermore, knowing the source of intrusion can also aid in clean-up operations before resuming water supply. Although, sensor network design for source identification has not been studied, a related problem that has been investigated by various researchers is the source identification problem given the sensor network design (Laird et al., 2005, 2006; Perelman and Ostfeld, 2013). However, these techniques are useful only if the amount of contaminant introduced into the WDN is known.

The present study focuses on sensor network design for monitoring any contamination that may be deliberately introduced into a WDN through vulnerable intrusion points. The sensor network design objectives considered in this study are (i) the ability of the network to detect a contaminant and (ii) the ability to identify the point at which the contaminant has been introduced, because in our opinion these are the most fundamental properties that any sensor network design should satisfy. The solutions are obtained using graph theoretic algorithms, since these can effectively exploit the structural properties of the network, leading to efficient solutions for large scale networks.

2. Sensor network design for contamination detection

2.1. Problem description and assumptions

As described in Section 1, several different criteria have been used to design a sensor network for intrusion detection in WDNs. While all of these are important, the fundamental requirements of any such monitoring system is that it should be capable of detecting an intrusion regardless of where it has occurred, and it should be capable of identifying the point of intrusion. Only if these two properties are met, is it possible to take mitigating action, which raises other pertinent issues such as time available for taking such action and the population size that will be affected before such action is taken, etc. Therefore, in this study, the following basic questions are addressed in the design of sensor network for contaminant detection and identification for a given water distribution network.

1 What is the minimum number of sensors required to detect an intrusion for a given set of potential intrusion locations in a water distribution network? (Observability problem)
2 What is the minimum number of sensors required to detect and identify the source of intrusion for a given set of potential intrusion locations in a water distribution network? (Identifiability or resolution problem)

A trivial solution is to place the sensors at every potential site of intrusion. This would satisfy both the observability and identifiability criteria. However, networks are large in size and have many such potential points of intrusion. Placing a sensor at every such point may not be economically feasible. Hence, the objective of the present study is to develop various algorithms that minimize the number of sensor locations.

Contaminant detection and identification in WDN can be viewed as a fault diagnosis problem. Several different approaches and criteria have been used to design sensor networks in chemical processes (Ali and Narasimhan, 1993; Raghuraj et al., 1999; Bagajewicz, 2000). Among these, the work by Raghuraj et al. (1999) deals with the problem of sensor network design for fault diagnosis with the specific objectives of ensuring observability and identifiability. We propose to adapt this approach to solve the sensor network design problem for contaminant detection problem in WDNs.

Although, accidental contamination can occur at any point in a WDN, deliberate contamination (such as terrorist attacks) will occur only at points in the WDN which are accessible. Typically, the pipes carrying water are buried underground and are not easily accessible. Storage reservoirs, water treatment plants and pumping stations are above ground and are accessible. Furthermore, the piping system is also accessible at points where manual or automatic valves are located. Therefore, in this work we consider reservoirs (main and intermediate), water treatment plants, pumping stations and valve locations as potential points of intrusion. A fire hydrant can also be a potential intrusion point, if a high pressure system (greater than the pressure at the hydrant point) is used to deliberately introduce the contaminant. All such points where a contaminant can be deliberately introduced are termed as vulnerable points and are assumed to be known or specified in this work. A vulnerable point where contaminant is introduced is said to be attacked. Once a vulnerable point is attacked, the contaminant is transported along with the water and may be get further diluted. It is assumed that sufficient quantities of contaminant is introduced at a vulnerable point such that the concentration level of