European Journal of Operational Research 000 (2016) 1–18

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Production, Manufacturing and Logistics

Optimal sensor deployment to increase the security of the maximal breach path in border surveillance

Ezgi Karabulut[a], Necati Aras[b,*], İ. Kuban Altınel[b]

[a] H. Milton Stewart School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA
[b] Department of Industrial Engineering, Boğaziçi University, 34342 İstanbul, Turkey

ARTICLE INFO

Article history:
Received 4 May 2014
Accepted 7 September 2016
Available online xxx

Keywords:
OR in defense
Border surveillance
Wireless sensor networks
Bilevel programming
Maximal breach path

ABSTRACT

Wireless Sensor Networks (WSN) are based on the collaborative effort of a large number of sensors which are low-cost, low-power, multi-functional small electronic devices. They provide a distributed sensing and monitoring environment for the area of interest and hence are used for applications such as environmental monitoring, border surveillance, and target tracking. In this work we study optimal deployment of WSNs for border surveillance using a static Stackelberg game frame and propose a bilevel optimization model for the optimal deployment of a heterogenous WSN so that the security of the area under consideration is increased as much as possible. There are two players in this game: defender and intruder. The defender is the leader and tries to determine the best sensor locations so as to maximize the security measured in terms of coverage intensity at discretized points in the area. The well-informed intruder assuming the role of the follower is capable of destroying some of the sensors so as to identify the maximal breach path, which represents the safest path from his perspective and thus increases the chance of being undetected by the sensors. This new approach results in a mixed-integer linear bilevel programming formulation that is difficult to solve exactly. Therefore, we propose three Tabu search heuristics and realize computational experiments on a large set of test instances in order to assess their performances.

1. Introduction

Sensors are small, low-cost, and low-power multifunctional devices with functional capabilities of sensing, communication and processing. Wireless Sensor Networks (WSNs) provide a distributed environment consisting of a large number of sensors, and have a variety of applications in remote environmental monitoring, border surveillance, and target tracking (Akyildiz, Melodia, & Chowdhury, 2007). Among the different types of optimization problems occurring within the context of WSNs we can mention data routing, sink mobility, and coverage problems. Routing optimization focuses on the determination of the path used by each sensor to send its collected data to a sink using other sensors so as to minimize the transmission energy (Güney, Aras, Altınel, & Ersoy, 2010). In other words, each path consists of a number of sensors that transmit data they collect to a sink using their battery energy. Sink mobility optimization is concerned in finding the best temporal locations of one or more mobile sinks. This helps to increase the lifetime of the WSN since the optimal data paths change depending on the location of the sinks, and sensors with high remaining energy become relay sensors (Keskin, Altınel, Aras, & Ersoy, 2014). Coverage problems deal with finding the best locations of the sensors so as to maximize the largest possible point/area coverage in the field of interest under various restrictions such as limited deployment budget, a fixed number of sensors to be deployed, or a minimum coverage threshold within the field (Altınel, Aras, Güney, & Ersoy, 2008).

The problem considered in this paper belongs to the class of coverage problems in the sense that there is an authority who is in charge of border surveillance to detect the intruders who would like to penetrate through the area. This is achieved by establishing a WSN and carefully determining the sensor locations in the network so as to increase the likelihood of detecting the intruder. The detection is actually achieved by the coverage intensity of the deployed sensors at discretized points within the area. We assume that the intruder can observe the sensor locations and has the capability of destroying some of the sensors depending on his capacity with the aim of pursuing the least secure and observable path in the WSN. This path is called the *minimal exposure path* or *maximal breach path* (MBP). Hence, the objective of the intruder is to infiltrate through the area by minimizing the total coverage at the

[*] Corresponding author. Fax: +90 212 2651800.
E-mail addresses: ezgi.karabulut@gatech.edu (E. Karabulut), arasn@boun.edu.tr (N. Aras), altinel@boun.edu.tr (İ. Kuban Altınel).

http://dx.doi.org/10.1016/j.ejor.2016.09.016

points of the MBP, which represents the most secure path from his standpoint. The system authority, on the other hand, has the opposite objective and aims at making the best decisions of sensor deployment (placement) so that the total coverage intensity at the points of the MBP remains as high as possible after some of the sensors are destroyed by the intruder.

The problem described above can be cast in the form of a Stackelberg game between two players called leader and follower (von Stackelberg, 1934). In our context, the system authority, whom we call the system planner in the sequel, is the leader of the game while the intruder is the follower. Stackelberg games can be formulated as bilevel programming problems, where bilevel programming is defined as "a mathematical program that contains an optimization problem in its constraints" (Bracken & McGill, 1973). Equivalently, it can be said that the leader is the main decision maker who takes into account in his so-called upper level problem (ULP) the optimization problem of the follower referred to as the lower level problem (LLP), which appears as a constraint in the ULP besides other constraints. For each decision set of the leader, there is an optimal reaction (or multiple optimal reactions) of the follower. Hence, by knowing the optimization problem of the follower, the leader incorporates the reaction of the other player into his modeling framework.

We formulate this problem first as a mixed-integer nonlinear bilevel problem, where nonlinearities occur only in the objective functions. The first nonlinearity appears as a product of two binary decision variables and the second one as a product of binary and continuous variables. Although it is possible to remove these nonlinearities and obtain a mixed-integer linear bilevel problem, the fact that LLP still contains binary decision variables makes our problem difficult to solve since efficient exact solution methods for this type of bilevel programming (BP) problems do not exist yet. Therefore, we propose hybrid heuristics combining mathematical programming with Tabu search.

The remainder of this paper is structured as follows. The next section includes a brief introduction to interdiction and surveillance. Section 3 contains the mathematical programming formulations. The proposed solution methods are explained in Section 4. Section 5 presents the experimental setting and computational results. Finally, the concluding remarks are presented in Section 6.

2. Overview of interdiction problems

Critical infrastructure consists of physical assets whose loss causes considerable disruption in operational and functional capabilities of that system. For example, production facilities and distribution centers can be regarded as critical infrastructure in a supply chain network. Similarly, bridges and viaducts on the highways connecting cities are critical infrastructure in a road transportation network. With the increasing number of deliberate attacks, the academic community's interest in the security planning of critical infrastructure has gained momentum. In the developed interdiction models, the vulnerabilities of a network is identified from the viewpoint of the service provider by anticipating the extent of the maximal or worst-case damage to the service provision by an attacker. The problem analyzed in this paper falls mainly into the category of the facility interdiction problems. The service provider or system planner (SP), acting as the leader, makes the decisions about the locations to be deployed by sensors, where the potential locations are a given set of points. In contrast to the objective of the leader, which is to increase the likelihood of detecting the intruder, the follower of the game has the capability of interdicting some of the sensors so as to follow the MBP that has the minimum observability on a network. That is, the sum of the coverage intensities (product of coverage probabilities) at the nodes of this intruder network is the smallest (largest) on the MBP. The existence of the intruder network makes the problem considered in this paper different from other facility interdiction problems, where customers are served directly from the nearest facility with positive remaining capacity. In our case, the intruder moves on a path whose nodes belong to vertices of the intruder network. In the remainder of this section, we mainly review the papers on facility location-interdiction problems that do not involve any decision about the protection of the interdicted components. Furthermore, we also highlight the most relevant papers within the context of WSNs since our paper is basically an application in WSN design.

There exists a handful of papers in the literature on facility interdiction problem where the SP makes the decision about locating facilities with and without protection. The first one of the papers without protection is by O'Hanley and Church (2011), in which the authors consider a maximal coverage type of supply/demand system. The defender decides on the locations of at most p facilities among a set of candidate sites that are exposed to disruptive actions by an intelligent attacker. In another paper without protection, Berman, Drezner, Drezner, and Wesolowsky (2009) examine a defensive p-median maximal covering problem with a single arc interdiction, where the attacker tries to decrease the coverage of customer nodes as much as possible by damaging one of the network links. Among the papers focusing on facility location-interdiction with protection, we can mention the work by Aksen, Aras, and Piyade (2013) which investigates a defender–attacker game in a p-median type problem setting where initial capacity acquisition and post-attack capacity expansion at the facilities are also taken into account to accommodate all customer demands in the event of the worst-case interdiction by the attacker. The same type of game is considered by Aksen and Aras (2012) in a setting of fixed-charge facility location problem, while Keçici, Aras, and Verter (2012) studies a maximal coverage type service network with fixed-charge facilities. Aksen, Akca, and Aras (2014) incorporate partial facility interdiction decisions into a median-type facility interdiction problem with capacitated facilities and outsourcing option. It is important to point out that none of the papers mentioned above include an underlying flow network, namely customers are served directly from one or more undisrupted facilities after the attack.

The following two papers deal with facility interdiction on an underlying flow network. In Berman and Gavious (2007), the State determines K sites of emergency response facilities on a shortest path network whose nodes are a number of cities. The terrorist, who has exact information about the response facility sites chosen by the State, attacks the cities with a certain success probability upon which the State sends its resources over the shortest path from the closest response facility to the attacked city. In a follow-up paper by Berman, Gavious, and Huang (2011), the assumption of the terrorist being perfectly knowledgeable about the response facility sites is relaxed, which leads to a simultaneous move game between the two players for which Nash equilibria can be found numerically.

Within the context of WSN design the most relevant papers to ours focus on the coverage issue in a WSN and try to identify the MBP. The basic structure of a MBP-related coverage problem in WSN is exemplified by Yates, Batta, and Karwan (2011). Meguerdichian, Koushanfar, Potkonjak, and Srivastava (2005) bring a novel perspective to the computation of the MBP and they work in the continuous domain in order to find the MBP in a WSN given the locations of the sensors in contrast to the general approach of discretizing the area. Başdere, Aras, Altınel, and Afşar (2013) develop a BP formulation where the defender wants to determine the best locations of the sensors to maximize the point coverage in the area with the anticipation that an intruder will attack and destroy some of the sensors to reduce the coverage. The main difference of this paper from the present one is that there is no effort

Please cite this article as: E. Karabulut et al., Optimal sensor deployment to increase the security of the maximal breach path in border surveillance, European Journal of Operational Research (2016), http://dx.doi.org/10.1016/j.ejor.2016.09.016