Optimization Problems in Infrastructure Security

Evangelos Kranakis[1]* and Danny Krizanc[2]

[1] School of Computer Science, Carleton University, Ottawa, Ontario, Canada.
[2] Dept. of Math. & Comp. Science, Wesleyan University, Middletown CT, USA.

Abstract. How do we identify and prioritize risks and make smart choices based on fiscal constraints and limited resources? The main goal of *infrastructure security* is to secure, withstand, and rapidly recover from potential threats that may affect critical resources located within a given bounded region. In order to strengthen and maintain secure, functioning, and resilient critical infrastructure, proactive and coordinated efforts are necessary.

Motivated from questions raised by infrastructure security, in this paper we survey several recent optimization problems whose solution has occupied (and continues to occupy) computer science researchers in the last few years. Topics discussed include:

1. Patrolling.
2. Sensor Coverage and Interference.
3. Evacuation.
4. Domain Protection and Blocking.

The central theme in all the problems mentioned above will involve mobility in that the participating agents will be able to move over a specified region with a given speed.

Security in itself is undoubtedly a very broad and complex task which involves all layers of the communication process from physical to network. As such the limited goal of this survey is to outline existing models and ideas and discuss related open problems and future research directions, pertaining to optimization problems in infrastructure security.

Key words and phrases. Blocking, Coverage, Evacuation, Infrastructure Security, Interference, Mobile Robots, Patrolling.

1 Infrastructure Security

Infrastructure security is concerned with securing physical assets so as to withstand, and rapidly recover from potential threats that may affect critical resources located or enclosed within a given bounded region. The apparent diversity of such systems makes potential threats difficult to grasp and the required rigorous security analysis almost impossible to pursue. It turns out that

* Supported in part by NSERC Discovery grant.

diverse infrastructure sectors such as buildings and roads, border systems, economic structures and materials, energy and water supply systems, internet and telecommunication systems, etc, have surprisingly similar structures that are often amenable to a rigorous risk analysis.

It is generally accepted that before 9/11, infrastructure security was only an afterthought since it was considered unthinkable that anyone would intentionally destroy critical infrastructure such as commercial buildings, power plants, water supplies, voice and data communications. Security was usually sacrificed for economic efficiency and the resulting systems were optimized only for profit, efficient operation, and low cost. In subsequent years researchers motivated by a new security reality attempted to develop critical infrastructure protection as a scientific discipline with formal analysis and design principles.

Research developments focused around a supervisory control and data acquisition (or SCADA for short) system which is a type of large scale computer based industrial control system for monitoring and controlling industrial facility based processes which exist in the physical world and as such may include multiple sites, and large distances. SCADA control systems may include various general buildings, transport systems, heating and ventilation systems, as well as energy production and consumption. Original SCADA architectures were rather primitive in design and conception but evolving systems include distributed and networked control augmented with sensor systems based on the internet of things. Typical designs of SCADA are quite complex and include system concepts and details of system components, control system for human computer interaction by supervisory station(s) employing various types of communication methods as part of the network infrastructure.

The most robust and efficient solutions are networked based and combine security threat assessment with risk analysis. By representing critical resources as nodes in a network with links one can identify critical components by various mathematical techniques involving, for example, counting, location, clustering, etc, and thus provide a measure of the complexity of the security task. Further, by making estimates of the cost and probability of an attack one could provide a "security strategy" which would ultimately reduce security risks in an effective way. Thus, researchers were led to vulnerability analysis and risk assessment which are essentially based on network theory. Standard literature on infrastructure security (see, e.g., book references such as [9, 33, 40] and elsewhere in various network security conferences) describe such techniques and show how to apply quantitative vulnerability analysis to a variety of infrastructure sectors in our society so as to be able to decide in the best way possible how to allocate limited resources that will eventually minimize the overall security risk.

The purpose of this survey is not to repeat methods and techniques which are already described adequately in the infrastructure security literature. The focus is rather on describing how combinatorial optimization techniques can be applied to design new and faster algorithms that will improve the computational complexity required to defend infrastructure in some security problems arising in sensor and robotic research. The four specific tasks selected for study

are patrolling, coverage & interference, evacuation, and protection & blocking. Methods proposed have the potential to enhance infrastructure security merely by facilitating the choice of optimal designs. The main characteristic of all the problems discussed is that they rely on mobile agents (robots, sensors) that can move over a given region with specific speeds and in some instances communicate with each other by exchanging messages. For each task we provide a brief literature review, outline its main features as well as solutions and describe some of the models proposed.

2 Patrolling

Patrolling has been defined as the act of surveillance consisting in walking perpetually around an area in order to protect or supervise it. Patrolling occurs in any situation where we are required to monitor a region, such as the perimeter of a building or campus, for activities posing a potential security threat. In the classic surveillance (also known as art gallery) literature, agents are placed at fixed positions to monitor the interior of a polygonal region [37] This contrasts sharply with our more recent studies on patrolling where the agents move around to cover the region. In such a setting patrolmen are assigned to monitor specified subregions by moving perpetually at regular intervals through areas assigned to them (see Figure 1). The patrolmen may be looking for any signs of

Fig. 1. Agents patrol a barrier by moving perpetually at constant speeds. What trajectories should the agents follow so that the time a point on the barrier is left unvisited by a agent is minimized?

specific problems (including, for example, detecting intrusions or security lapses, responding to service calls, resolving disputes and/or making arrests, reporting crimes, and conducting traffic enforcement) which need to be identified. The duration of patrolling may vary in time depending on the nature of the objective but here we are interested in the perpetual movement of the monitoring agents (human or robotic). The accepted measure of the algorithmic efficiency of patrolling is called *idleness* and it is related to the frequency with which the points of the environment are visited [2]. (This criterion was first introduced in [35].)

We are interested in patrolling a domain represented by a geometric graph in a setting where 1) some of the patrolmen may be unreliable (faulty) in that they fail to report their monitoring activities, and/or 2) parts of the domain are not critical and as such do not need to be patrolled. More specifically, we are interested in the following problem:

> *Patrolling.* We are given a team of patrolmen and a domain to be monitored. Assume that some of the patrolmen may be unreliable. We want

to design a strategy constructing perpetual patrolmen trajectories, so that, independently of which subset of them (of a given size) will turn out to be faulty, no critical point of the domain will be ever left unvisited by some reliable agent longer than the allowed *idle time*.

The problem proposed above has been studied in [16] for patrolmen with identical speeds. Patrolling with agents that do not necessarily have identical speeds has been initiated in [15]. As shown in [23, 26] this case offers several surprises both in terms of the difficulty of the problem as well as in terms of the algorithmic results obtained. In particular, no optimal patrolling strategy involving more than three agents has yet been found. Recently, [39] studied the distributed coordination of a set of moving cameras monitoring a line segment to detect moving intruders. Optimal patrolling involving same-speed agents in mixed domains, where the regions to be traversed are fragmented by portions that do not need to be monitored, is studied in [13].

3 Sensor Coverage & Interference

Mobile sensors are being used in many application areas to enable easier access and information retrieval in diverse communication environments, such as habitat monitoring, sensing and diagnostics and critical infrastructure monitoring. Recent reductions in manufacturing costs make deployments of such sensors even more attractive. Since existing sensor deployment scenarios cannot always ensure precise placement of sensors, their initial deployment may be arbitrary. In some cases the sensors were originally randomly scattered over the region according to some (potentially unknown) distribution or they may have drifted to new positions over time. Even initially deterministically placed sensors may create arbitrary patterns of effectiveness due to random failures. Therefore in order to improve the coverage provided by the set of sensors it is necessary to redeploy them by displacing them more evenly throughout a domain (see Figure 2).

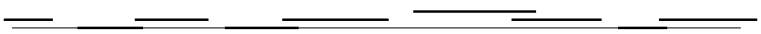

Fig. 2. A set of sensors with respective ranges depicted as closed intervals are initially placed on a barrier. What is the minimum sum of displacements (or maximum displacement) of the sensors required so that every point on the barrier is within the range of a sensor?

By displacing the sensors to new positions one can improve the overall coverage of a given region. Thus, a basic instance of the problem being considered is the following.

Sensor Coverage. What is the cost (expected, if sensor arrangement is random) of moving mobile sensors with a given circular (but bounded)

sensing range from their original positions to new positions so as to achieve full coverage of a region, i.e., every point of the region is within the range of at least one sensor.

Given a geometric region in the plane there are two basic formulations of the problem: displace the sensors so as to either ensure 1) full coverage of the region, or 2) coverage of the perimeter of the region. The first problem is referred as *area coverage* and the second as *perimeter or barrier coverage*.

The problem has been investigated in [28] for the uniform random setting. In both instances it is assumed the sensors are deployed initially in the domain uniformly and independently at random. Since such a random deployment does not necessarily guarantee full coverage it is important to displace the sensors so as to ensure all points are covered while at the same time minimizing the transportation cost. The two cost parameters we choose to optimize are the expected sum and maximum of the sensor's displacements, the former being an approximation of the total energy consumed while the latter of the time required to complete the task by the entire system of deployed sensors.

There is also extensive literature on area and barrier or perimeter coverage by a set of sensors (e.g., see [31, 41]). The deterministic sensor movement problem for planar domains with pre-existing anchor (or destination) points was introduced in [8] and for a linear domain (or interval) in [17]. Interestingly enough, the complexity of the problem (i.e., finding an algorithm that optimizes the total or maximum displacement) depends on the types of the sensors, the type of the domain and whether one is minimizing the sum or maximum of the sensor movements. For example, for the unit interval the problem of minimizing the sum is NP-complete if the sensors may have different sensing ranges but is polynomial time in the case where all the ranges are the same [18]. The problem of minimizing the maximum is NP-complete if the region consists of two intervals [17] but is polynomial time for a single interval even when the sensors may have different ranges [11]. Related work on deterministic algorithms for minimizing the total and maximum movement of sensors for barrier coverage of a planar region may be found in [8]. Different metrics for the complexity of barrier coverage are also possible: one is based on robot assisted restoration and is analyzed in [19] and another on the power of the displacement and is analyzed in [25].

A related problem studied in [29] is sensor interference. Assume that for a given parameter $s > 0$ two sensors' signals interfere with each other during communication if their distance is $\leq s$. We are allowed to move the sensors on the line, if needed, so as to avoid interference. We call total movement the sum of displacements that the sensors have to move so that the distance between any two sensors is $> s$.

Sensor Interference. Assume that n sensors are thrown randomly and independently with the Poisson distribution having arrival rate $\lambda = n$ in the interval $[0, +\infty)$. What is the expected minimum total distance that the sensors have to move from their initial position to a new destination so that any two sensors are at a distance more than s apart?

Finally, it is worth mentioning [30] where sensor movement for both coverage and interference at the same time is being studied.

4 Evacuation

The goal of traditional search problems is to find an object which is located in a specific domain. This subject of research has a long history and there is a plethora of models investigated in the mathematical and theoretical computer science literature with emphasis on probabilistic search in [42], game theoretic applications in [3], cops and robbers in [10], classical pursuit and evasion in [36], search problems and group testing in [1], plus many more.

We investigate the problem of searching for an *exit* at an unknown location using k agents, $k \geq 1$. We are interested in minimizing the time it takes until the *last agent* finds the exit. (Note: the case $k = 1$ is the same as the traditional search problem.) The agents need to evacuate the region but the location of the exit is unknown to them; they can cooperate to search for the exit, but it is not enough for one agent to find the exit, we require all agents to reach the exit as soon as possible (see Figure 3). A canonical example of our problem restricts the

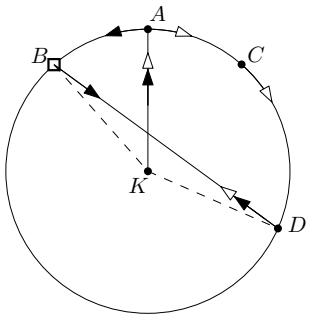

Fig. 3. Evacuation of two agents starting at point K from an unknown exit (at B) in the face-to-face model. The agents move together towards the perimeter (point A) and in opposite direction along the perimeter. The first agent to find the exit moves to meet the second agent (at point D) and bring it to the exit.

domain to be a disk of radius 1:

> $k > 1$ agents are located within a unit disk. At any time the agents can move anywhere they choose within the disk with maximum speed 1. The agents can communicate with each other either only if they are at the same point at the same time (we call this communication model *face-to-face communication*) or at any time by wireless communication. Our goal is to schedule the trajectories of the agents so as to minimize the *evacuation time*, which is the time it takes all agents to reach the exit

(for the worst case location of the exit). The time is generally reported as the worst case ratio of the evacuation time to actual distance to the exit.

The version of the above problem where all agents start at the centre of the disk was first studied in [14]. The same paper introduced the two communication models discussed above. Baeza-Yates *et al* [4] posed the question of minimizing the worst-case trajectory of a single agent searching for a target point at an unknown location in the plane. This was generalized to multiple agents in [34], and more recently has been studied in [24, 32]. However the agents cannot communicate, and moreover, the objective is only for the first agent to find the target. Two seminal and influential papers (that appeared almost at the same time) on probabilistic search are [5], and [6] and concern minimizing the *expected time* for the agent to find the target. Useful surveys on search theory can also be found in [7] and [21]. In addition, the latter citation has an interesting classification of search problems by search objectives, distribution of effort, point target (stationary, large, moving), two-sided search, etc. The evacuation problem considered is related to searching on a line, in that we are searching on the boundary of a disk but with the additional ability to make short-cuts in order to enable the agents to meet sooner and thus evacuate faster. In [12] evacuation algorithms are proposed for agents with different speeds on a line in the face-to-face communication model. Domains other than the disc or line have also been studied. For example, [20] considers evacuation from an equilateral triangle and a square.

5 Domain Protection & Blocking

Consider a set of impenetrable buildings located axis-aligned on a square or rectangular region (see Figure 4). We are interested in detecting intruders attempting to pass through the region by placing sensors at regularly spaced intervals over the region forming a grid. If an intruder steps within the sensing range of a sensor he or she will be detected. It is desired to prevent potential attacks in either one dimension or two dimensions. A one-dimensional attack succeeds when an intruder enters from the top (North) side and exits out the bottom (South) side of the domain without being detected. Preventing attacks in two dimensions requires that we simultaneously prevent the intruder from either entering North and exiting South or entering East (left side) and exiting West (right side) undetected.

Protection & Blocking. Assume that initially all of the sensors are working properly and the domain is fully protected, i.e., all attacks will be detected, in both dimensions (assuming the grid points are such that neighboring sensors have overlapping sensing ranges and include all four boundaries of the domain). Over time, some of the sensors may fail and we are left with a subset of working sensors. We wish to determine if one- or two-dimensional attack detection still persists and if not, restore

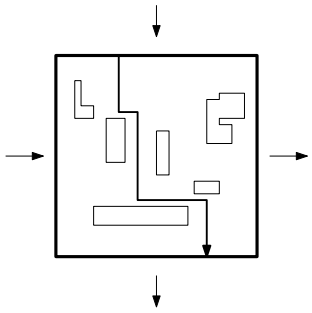

Fig. 4. A geometric region (square) containing impenetrable buildings and structures. An intruder may penetrate the region either from north to south or east to west by following a possibly rectilinear path through the available free space in the region. How should the adversary be blocked using the minimum number of sensors placed on grid points?

protection by adding the least number of sensors required to ensure detection in either one or two dimensions.

Ideally, the set of currently working sensors would provide some amount of fault-tolerance. In particular, it would be advantageous if for a given k, the set of sensors maintains protection (in one or two dimensions) even if up to k of the sensors fail. This leads to the problems of deciding if a subset of the sensors provides protection with up to k faults and if not, finding the minimum number of grid points to add sensors to in order to achieve k fault-tolerance. In [27], algorithms are provided for deciding if a set sensors provides k-fault tolerant protection against attacks in both one and two dimensions, for optimally restoring k-fault tolerant protection in one dimension and for restoring protection in two dimensions (optimally for $k = 0$ and approximately otherwise). A closely related work is that of [38] where the authors look at how to best randomly distribute additional sensors in order to maintain barrier coverage under the potential for faults

In the above version of the problem, sensors are added in order to restore protection. Alternatively, we could consider a version of the problem where we may move the existing sensors rather than add new sensors (assuming the number of existing sensors is sufficient to provide a solution). Can the rectangular grid be protected with the existing and/or the addition of new mobile sensors? If yes, provide an algorithm displacing the sensors so as to provide protection for the grid and which minimizes the sum (or maximum) of distances of the sensors displaced. What is the minimum number of new sensors which in combination with the previously existing sensors could protect the grid? Concerning this version of the problem, in [43] the authors introduce the problem of how to efficiently heal coverage holes in hybrid Wireless Sensor Networks (WSNs) by relocating mobile nodes (this is effectively the *moving sensor* version of the 1D

blocking problem introduced above), and propose a hole recovery strategy called Minimal Patching Barrier Healing Strategy (MPBHS).

The paths taken by an intruder in the above model are arbitrary rectilinear paths. In some instances it may only be necessary to protect against attackers traveling along orthogonal straight line paths. Such an attacker has been considered before in the case of barrier coverage [31]. Obviously, it is much easier to defend against the straight line type of adversary, referred to as *weak* protection, and optimal strategies are usually rather straightforward to identify when deciding where to add (immovable) sensors. Interestingly, even this weaker version becomes NP-complete when we consider mobile sensors and the problem of minimizing the maximum movement required [22].

.

6 Conclusion

In this survey we have discussed several "mobile agent" based optimization problems inspired by infrastructure security. For each of the four problems discussed, the optimization aspect was emphasized and we tried to indicate how efficient algorithms can be used to make security solutions more effective. In all cases considered agent mobility was crucial in obtaining optimal solutions.

However, it is important to take into account the fact that this is only the "tip of the iceberg" since security is a very complex task involving the coordination several layers of the communication process from physical infrastructure to network systems. We hope this presentation will initiate more research on optimization problems arising in infrastructure security in particular and security in general.

References

1. R. Ahlswede and I. Wegener. *Search problems*. Wiley-Interscience, 1987.
2. A. Almeida, G. Ramalho, H. Santana, P. Azevedo Tedesco, T. Menezes, V. Corruble, and Y. Chevaleyre. Recent advances on multi-agent patrolling. In *SBIA*, pages 474–483, 2004.
3. S. Alpern and S. Gal. *The theory of search games and rendezvous*, volume 55. Springer, 2003.
4. R. Baeza Yates, J. Culberson, and G. Rawlins. Searching in the plane. *Information and Computation*, 106(2):234–252, 1993.
5. A. Beck. On the linear search problem. *Israel Journal of Mathematics*, 2(4):221–228, 1964.
6. R. Bellman. An optimal search. *Siam Review*, 5(3):274–274, 1963.
7. S. Benkoski, M. Monticino, and J. Weisinger. A survey of the search theory literature. *Naval Research Logistics (NRL)*, 38(4):469–494, 1991.
8. B. Bhattacharya, M. Burmester, Y. Hu, E. Kranakis, Q. Shi, and A. Wiese. Optimal movement of mobile sensors for barrier coverage of a planar region. *TCS*, 410(52):5515–5528, 2009.

9. B. Biringer, E. Vugrin, and D. Warren. *Critical infrastructure system security and resiliency*. CRC press, 2013.
10. A. Bonato and R. Nowakowski. *The game of cops and robbers on graphs*. American Mathematical Soc., 2011.
11. D. Chen, Y. Gu, J. Li, and H. Wang. Algorithms on minimizing the maximum sensor movement for barrier coverage of a linear domain. *Algorithm Theory–SWAT 2012*, pages 177–188, 2012.
12. M. Chrobak, L. Gasieniec, T. Gorry, and R. Martin. Group search on the line. In *SOFSEM 2015: Theory and Practice of Computer Science*, pages 164–176. Springer, 2015.
13. A. Collins, J. Czyzowicz, L. Gasieniec, A. Kosowski, E. Kranakis, D. Krizanc, R. Martin, and O. Morales Ponce. Optimal patrolling of fragmented boundaries. In *Proceedings of SPAA*, 2013.
14. J. Czyzowicz, L. Gasieniec, T. Gorry, E. Kranakis, R. Martin, and D. Pajak. Evacuating robots from an unknown exit located on the perimeter of a disc. In *DISC 2014*. Springer, Austin, Texas, 2014.
15. J. Czyzowicz, L. Gasieniec, A. Kosowski, and E. Kranakis. Boundary patrolling by mobile agents with distinct maximal speeds. *Algorithms–ESA 2011*, pages 701–712, 2011.
16. J. Czyzowicz, L. Gasieniec, A. Kosowski, E. Kranakis, D. Krizanc, and N. Taleb. When patrolmen become corrupted: Monitoring a graph using faulty mobile robots. In *Proceedings of ISAAC*, 2015.
17. J. Czyzowicz, E. Kranakis, D. Krizanc, I. Lambadaris, L. Narayanan, J. Opatrny, L. Stacho, J. Urrutia, and M. Yazdani. On minimizing the maximum sensor movement for barrier coverage of a line segment. *ADHOCNOW*, pages 194–212, 2009.
18. J. Czyzowicz, E. Kranakis, D. Krizanc, I. Lambadaris, L. Narayanan, J. Opatrny, L. Stacho, J. Urrutia, and M. Yazdani. On minimizing the sum of sensor movements for barrier coverage of a line segment. *ADHOCNOW*, pages 29–42, 2010.
19. J. Czyzowicz, E. Kranakis, D. Krizanc, L. Narayanan, and J. Opatrny. Robot-assisted restoration of barrier coverage. In *Workshop on Approximation and Online Algorithms*, pages 119–131. Springer, 2014.
20. J. Czyzowicz, E. Kranakis, D. Krizanc, L. Narayanan, J. Opatrny, and S. Shende. Wireless autonomous robot evacuation from equilateral triangles and squares. *ADHOCNOW*, 2015.
21. J. Dobbie. A survey of search theory. *Operations Research*, 16(3):525–537, 1968.
22. S. Dobrev. personal communication.
23. A. Dumitrescu, A. Ghosh, and C. D. Tóth. On fence patrolling by mobile agents. *Electr. J. Comb.*, 21(3):P3.4, 2014.
24. Y. Emek, T. Langner, J. Uitto, and R. Wattenhofer. Solving the ants problem with asynchronous finite state machines. In *Proceedings of ICALP, LNCS 8573*, pages 471–482, 2014.
25. R. Kapelko and E. Kranakis. On the displacement for covering a square with randomly placed sensors. In *Ad-hoc, Mobile, and Wireless Networks - 14th International Conference, ADHOCNOW 2015, Athens, Greece, June 29 - July 1, 2015, Proceedings*, pages 148–162, 2015.
26. A. Kawamura and Y. Kobayashi. Fence patrolling by mobile agents with distinct speeds. In *Proceedings of ISAAC 2012*, December 19-21, 2012.
27. E. Kranakis, D. Krizanc, F. Luccio, and B. Smith. Maintaining intruder detection capability in a rectangular domain with sensors. In *Algosensors 2015, Patras, Greece*, 2015.

28. E. Kranakis, D. Krizanc, O. Morales-Ponce, L. Narayanan, J. Opatrny, and S. Shende. Expected sum and maximum of displacement of random sensors for coverage of a domain. In *Proceedings of the twenty-fifth annual ACM symposium on Parallelism in algorithms and architectures*, pages 73–82. ACM, 2013.
29. E. Kranakis and G. Shaikhet. Displacing random sensors to avoid interference. In *Computing and Combinatorics*, pages 501–512. Springer, 2014.
30. E. Kranakis and G. Shaikhet. Sensor allocation problems on the real line (to appear), 2015.
31. S. Kumar, T. H. Lai, and A. Arora. Barrier coverage with wireless sensors. In *Proceedings of the 11th annual International Conference on Mobile Computing and Networking*, pages 284–298. ACM, 2005.
32. C. Lenzen, N. Lynch, C. Newport, and T. Radeva. Trade-offs between selection complexity and performance when searching the plane without communication. In *Proceedings of PODC*, pages 252–261, 2014.
33. T. G. Lewis. *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons, 2014.
34. A. López-Ortiz and G. Sweet. Parallel searching on a lattice. In *Proceedings of CCCG*, pages 125–128, 2001.
35. A. Machado, G. Ramalho, J.-D. Zucker, and A. Drogoul. Multi-agent patrolling: An empirical analysis of alternative architectures. In *MABS*, pages 155–170, 2002.
36. P. Nahin. *Chases and Escapes: The Mathematics of Pursuit and Evasion*. Princeton University Press, 2012.
37. J. O'Rourke. *Art gallery theorems and algorithms*, volume 57. Oxford University Press, Oxford, 1987.
38. T. Park and H. Shi. Extending the lifetime of barrier coverage by adding sensors to a bottleneck region. In *12th IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 2015.
39. F. Pasqualetti, F. Zanella, Peters J. R., Spindler M., R. Carli, and F. Bullo. Camera network coordination for intruder detection. *IEEE Trans. Contr. Sys. Techn.*, 22(5):1669–1683, 2014.
40. R. S. Radvanovsky and A. McDougall. *Critical infrastructure: homeland security and emergency preparedness*. CRC Press, 2009.
41. A. Saipulla, C. Westphal, B. Liu, and J. Wang. Barrier coverage of line-based deployed wireless sensor networks. In *INFOCOM*, pages 127–135. IEEE, 2009.
42. L. Stone. *Theory of optimal search*. Academic Press New York, 1975.
43. H. Xie, M. Li, W. Wang, C. Wang, X. Li, and Y. Zhang. Minimal patching barrier healing strategy for barrier coverage in hybrid wsns. In *Personal, Indoor, and Mobile Radio Communication (PIMRC), 2014 IEEE 25th Annual International Symposium on*, pages 1558–1563. IEEE, 2014.