Dynamic Barrier Coverage Algorithm Using Coordinator Sensor Patrolling For Wireless Sensor

M.Arivazhagan\(^1\), Mr.T.Krishnakaarthik\(^2\)
\(^1\)P.G Scholar, Department of CSE, Nandha College of Technology, Erode
\(^2\)Assistant Professor, Department of IT, Nandha College of Technology, Erode

Abstract. Operational limitations such as human inaccessibility, sensors are usually deployed randomly, e.g., dropped by an airplane, in or near a region of interest (ROI). Random sensor dropping causes the WSNs to have topological weaknesses such as sensing holes, communication bottlenecks and network partitions. In this paper, consider a particular scenario, where sensors are not designated to monitor events inside the ROI but to detect intruders that attempt to penetrate the ROI. Consider the barrier coverage problem where \(m\) sensors are needed to guarantee full barrier coverage and there are only \(n\) mobile sensors available \((n < m)\). Formulate the problem as a dynamic programming problem and propose two sensor patrolling algorithms to solve this problem: periodic monitoring scheduling (PMS) and coordinated sensor patrolling. Work offers a radically new cost-effective barrier coverage solution. The barrier coverage performance is characterized by average intruder detection probability. Design two algorithms, S-DCSP and G-DCSP, to guide the sensor movement in order to detect intruders as many as possible. In this paper the dynamic k-barrier coverage problem in wireless sensor network in which each sensor has \(L+1\) sensing power levels is proposed. First, the proposed method transforms the dynamic k-barrier coverage problem work for different intruders’ arrival models. The performance of the proposed scheme was evaluated using the ns-2 network simulator.

1. INTRODUCTION

A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance.

However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The size a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

The barrier coverage problem where \(m\) sensors are needed to guarantee full barrier coverage and there are only \(n\) mobile sensors available \((n < m)\). First model the arrival of intruders at a specific location as are new process, in which the next intruder’s arrival time is correlated with the current one. The barrier coverage performance is characterized by average intruder detection probability. Formulate the problem as a dynamic programming problem where the movement strategy of all

Over the past few years, wireless sensor networks and their various applications is evolving quickly and known to be an important area of research. Wireless sensor networks have numerous applications such as in environmental, ecological, agricultural, military and medical treatment. Security has become the most important issue in worldwide nowadays. Meanwhile, real-time detection of border intrusion is becoming a tough
factor of any country. Monitoring borders requires large amount of equipments and labor power. So wireless sensor networks could be an intelligent manner to solve these problems. One important observation is the linearity of sensors’ energy consumption which means that the death of sensors could be predicted. So the research must pay more attention to the sink nodes to which indicate the weak zone. Discuss the methods to guarantee the quality of coverage and the new coverage model which could be more energy efficient. Consider the barrier coverage problem where \( m \) sensors are needed to guarantee full barrier coverage and there are only \( n \) mobile sensors available. First model the arrival of intruders at a specific location as a renew process, in which the next intruder’s arrival time is correlated with the current one.

2. RELATED WORKS

In this section, Barrier coverage of wireless sensor networks provides sensor barriers guarding boundaries of critical infrastructures or assets, such as country borders, coastal lines, and boundaries of battle fields.

1. Barrier Coverage of Wireless Sensor Networks

A. Saipulla, B. Liu, G. Xing, X. Fu et all Barrier coverage is a critical issue in wireless sensor networks for various battlefield and homeland security applications. The goal is to effectively detect intruders that attempt to penetrate the region of interest. A sensor barrier is formed by a connected sensor cluster across the entire deployed region, acting as a “trip wire” to detect any crossing intruders. In this paper study about how to efficiently improve barrier coverage using mobile sensors with limited mobility. After the initial deployment, mobile sensors can move to desired locations and connect with other sensors in order to create new barriers.

To explore the fundamental limits of barrier coverage with sensors of limited mobility. There is no prior work which can directly compare our approach with. To demonstrate the performance of our proposed sensor mobility scheme, we consider a greedy approach and use it as a reference point. The greedy approach tries to assign the closest available mobile sensor to each grid point. Each time we randomly select a grid point that has not assigned a sensor, and assign the closest available mobile sensor to the grid point.

2. Intrusion Detection in Mobile Sensor

E. Amaldi, A. Capone, M. Cesana et all, Intrusion detection is a significant application in wireless sensor networks (WSNs). S. Kumar et al have introduced the concept of barrier coverage, which deploys sensors in an arrow belt region to guarantee that any intrusion across the region is to be detected. However, the practical issues have not been investigated such as scheduling sensors energy-efficiently while guaranteeing the detection probability of any intrusion across the region based on probabilistic sensing model, which is a more realistic sensing model. Besides, the intruders may be humans, animals, fighter planes or other things, which obviously have diverse moving speeds. In this paper, we analyse the detection probability of arbitrary path across the barrier of sensors theoretically and take the maximum speed of possible intruders into consideration since the sensor networks are designed for different intruders in different scenarios.

3. Mobile Element Scheduling

I. Dietrich and F. Dressler et all. In a wireless sensor network, intruders are detected when they enter the areas covered by sensors. The union of the covered areas of sensors forms a barrier. A barrier may contain gaps, allowing the intruder to pass through undetected. A strong barrier has no gaps, so that no intruders can cross the region undetected no matter what crossing paths the intruders would choose.
Constructing a strong barrier from sensors randomly deployed in a region is a challenging problem. Barrier coverage is affected by sensor deployment methods. In barrier coverage sensors are often deployed in regions of an irregular long belt shape. In certain applications sensors may be manually placed in desired locations and so barrier coverage can be achieved using a minimum number of sensors by aligning them in straight lines crossing the network region. In other applications, sensors may have to be deployed randomly. They may be, for example, dropped by airplanes or launched by artilleries. In random sensor deployments, barrier coverage depends on the spatial distribution of sensor locations.

Barrier coverage is affected by the crossing paths taken by the intruder. A crossing path is a path that crosses the complete width of the region from one side to the other side. If an intruder has no knowledge of the sensor locations (i.e., sensors are stealthy), it is proved in [1] that the optimal crossing paths that minimize the probability of being detected in a two-dimensional rectangular network (a.k.a. a strip network) are the orthogonal crossing paths. Recently, Kumar, Lai, and Arora [2] defend two types of barrier coverage. They are weak barrier coverage, which guarantees to detect intruders moving along congruent paths; and strong barrier coverage, which guarantees to detect intruders no matter what crossing paths they take.

4. Mobile Target Detection

Edoardo Amaldi, Antonio Capone et al. Surveillance applications through wireless sensor networks (WSNs) where the areas to be monitored are fully accessible and the WSN topology can be planned a priority maximize application efficiency. We propose an optimization framework for selecting the positions of wireless sensors to detect mobile targets traversing a given area. By leveraging the concept of path exposure as a measure of detection quality, we propose two problem versions: the minimization of the sensors installation cost while guaranteeing a minimum exposure, and the maximization of the exposure of the least-exposed path subject to a budget on the sensors installation cost. We present compact mixed-integer linear programming formulations for these problems that can be solved to optimality for reasonable-sized network instances. Moreover, we develop Tabu Search heuristics that are able to provide near-optimal solutions of the same instances in short computing time and also tackle large size instances. The basic versions are extended to account for constraints on the wireless connectivity as well as heterogeneous devices and non-uniform sensing. Finally, we analyze an enhanced exposure definition based on mobile target detection probability.

3. PROBLEM FORMULATION

Existing solutions are mainly concerned with deciding one-time movement for individual sensors to construct as many barriers as possible, which may not be suitable when there are no sufficient sensors to form a single barrier. In this paper, we aim to achieve barrier coverage in the sensor scarcity scenario by dynamic sensor patrolling. Specifically, we design a periodic monitoring scheduling (PMS) algorithm in which each point along the barrier line is monitored periodically by mobile sensors. Based on the insight from PMS, we then propose a coordinated sensor patrolling (CSP) algorithm to further improve the barrier coverage, where each sensor’s current movement strategy is derived from the information of intruder arrivals in the past. Existing solutions to barrier coverage in mobile sensor networks implicitly assume the availability of sufficient sensors. They focus on how to move the available sensors one time to construct as many barriers as possible with a minimum aggregate moving distance. A drawback of Existing System in Traceability is not
supported and Data Dynamism sequence is not managed from High computational overhead.

The main Objective of the Project To develop the system for cost-effective barrier coverage problem for the case of sensor scarcity. First designed periodic monitoring scheduling (PMS) algorithm. Based on the insight gained from PMS, we then proposed to jointly exploit sensor mobility and intruder arrival information to improve barrier coverage. Then proposed to jointly exploit sensor mobility and intruder arrival information to improve barrier coverage. Proposed a new scheduling protocol 2D k-barrier

4. PROPOSED SYSTEM

Sensors are moving on two barriers and propose two heuristic algorithms to guide the movement of sensors. Finally, we generalize our results to work for different intruder arrival models. Through extensive simulations, the proposed algorithms have desired barrier coverage performances. Defined the notion of k-barrier coverage, and proposed algorithms to decide whether a belt region is k-barrier covered or not after sensor deployment. Introduced two probabilistic barrier coverage concepts: weak barrier coverage and strong barrier coverage. The minimum number of sensors required to ensure weak barrier coverage with high probability has been derived, while the issue of strong barrier coverage is still open. Based on the insight gained from PMS, in sensor networks for intruder detection, which constructs The general k-barriers coverage by mobile sensor networks in the future work. The one future research direction is to add some mobile sensors and consider their integrated movement strategy. Another future research direction is to realize the detection in reality, which will consider the network performance in 3D environment. The objective is not only to guarantee coverage quality but also to improve network lifetime, data report timeliness and reliability at the same time.

Advantages of Proposed System

- Privacy ensured data verification is performed.
- Simultaneous data verification scheme.
- Computational and communication cost is reduced.
- Data dynamism is supported by the system.

5. SOFTWARE DESCRIPTION

Front End

Red Hat Enterprise Linux (RHEL) is a Linux distribution produced by Red Hat and targeted toward the commercial market, including mainframes. Red Hat Enterprise Linux is released in server versions for x86, x86-64, Itanium, PowerPC and IBM System z, and desktop versions for x86 and x86-64. All of Red Hat's official support and training, and the Red Hat Certification Program center around the Red Hat Enterprise Linux platform. Red Hat Enterprise Linux is often abbreviated to RHEL, although this is not an official designation.

The first version of Red Hat Enterprise Linux to bear the name originally came onto the market as "Red Hat Linux Advanced Server". In 2003 Red Hat rebranded Red Hat Linux Advanced Server to "Red Hat Enterprise Linux AS", and added two more variants, Red Hat Enterprise Linux ES and Red Hat Enterprise Linux WS.

Real Time Strategy

New strategy game play allows players to Command from overhead. Build structures anywhere, collect resources and research upgrades. The marines can build phase gates, sentry turrets and siege cannons to assault the enemy. Aliens can build upgrade chambers, evolve special abilities, lay eggs and plant traps.

Dynamic Environment

Levels change as you play. Spreading alien infestation deforms
hallways and causes space station power failure, halting all lifts. Destroying a catwalk's supports causes it to fall, revealing a new route.

Unlimited Variations
Flexible game rules and scripting allow you to create your own unique scenarios like "Colonist Rescue", "Alien vs. Alien" or anything else you can dream up. Free automatic updates keep the game fresh by adding new levels and abilities. Trace file is one of the text-based results that the user gets from a simulation. It records the actions and relevant information of every discrete event in the simulation. There are varieties of forms for trace files. Simulations using different simulation networks or using different routing protocols could get trace files having different trace file formats.

Introduction to NAM
NAM is a Tcl/Tk based animation tool for viewing network simulation traces and real world packet trace data. The design theory behind NAM was to create an animator that is able to read large animation data sets and be extensible enough so that it could be used in different network visualization situations. Under this constraint NAM was designed to read simple animation event commands from a large trace file.

The first step to use NAM is to produce the trace file. The trace file contains topology information, e.g., nodes, links as well as packet traces. Usually, the trace file is generated by ns. When the trace file is generated, it is ready to be animated by NAM. Upon startup, NAM will read the trace file, pop up a window, do layout if necessary, and then pause at time 0. Through its user interface, NAM provides control over many aspects of animation as shown in figure 4.3.1.

Features of NS-2
- Protocols: TCP, UDP, HTTP, Routing algorithms etc
- Traffic Models: CBR, VBR, Web etc
- Error Models: Uniform, bursty etc
- Radio propagation, Mobility models
- Energy Models
- Topology Generation tools
- Visualization tools
- Extensibility
- Static Routing implemented for wireless nodes
- Co Channel interference added
- Adaptive data rate support for 802.11
- BPSK Modulation Scheme Added
- Directional Antenna support added (More radiation pattern added in TENS1.2)
6. SYSTEM IMPLEMENTATION

1. Single Barrier Case with Intruder Arrival Following Weibull Distribution:

For all the simulations, \( \lambda = 10 \) (Eqns. 1 and 2). An intruder is detected when it arrives at a point and a sensor is monitoring there. The average intruder detection probability \( \gamma \) is calculated by the ratio of the number of detected intruders to all arriving intruders. As there is no existing work on our problem, we use simulations to demonstrate the performance of the proposed algorithms.

In the simulation, initially \( n \) sensors are located at points \( 1 \sim n \). The total number of points \( m \) is set to be 10. For every \( T \) time slots, the sensor at point \( j \) will move to point \( \text{Mod}(j+n,m) \) for monitoring, regardless of the arrival of an intruder. We first fix \( n = 5 \) and \( \beta = 4 \), and vary \( T \) to show the impact of \( T \) on \( \gamma \). The results are plotted in Fig. 8. As stated in the Section 4, values of \( \gamma \) are equal to \( n/m \) for all different \( T \), reflecting the continuous monitoring time \( T \) at a point does not impact \( \gamma \). Then we vary the values of \( n \) to 4, 6, 7, and 8, and conduct the corresponding simulations. Values of \( \gamma \) in these cases are still equal to \( n/m \). At last, we set \( \beta = 5 \), \( n = 5 \) to investigate the impact of \( \beta \) on \( \gamma \) in the PMS algorithm. The results in Fig. 8 show that values of \( \gamma \) are the same as those in the case \( \beta = 4 \), \( n = 5 \). From the simulation results, we can conclude that PMS cannot improve the performance \( \gamma \) no matter what network settings are. This indicates that we have to include intruder arrival information for the sensor movement design in order to improve the performance \( \gamma \).

6.2 Single Barrier Case with Intruder Arrival Following Markov Chain

Adopt some real data collected from spectrum usage to show some practical implications of the proposed algorithms. The data record the channel states (i.e., occupancy and vacancy) of spectrum ranging from 300MHz to 3000MHz in Guangdong province, China. We note that barrier coverage approach can also be applied to the scenario where we want to estimate the specific channel usage of some discrete locations: viewing channel occupancy as an intruder, we use mobile sensors (such as sensing devices piggybacked on cars) to monitor specific channel states. As the resource is limited, we want to maximize the detection probability of channel occupancy by mobilizing these limited sensing devices. We adopt the Markov chain to model the real data, the barrier coverage performance of the modified CSP (MCSP). Again, we can see that MCSP can achieve a high barrier coverage performance with a small number of sensors, which is consistent with the results obtained in the previous subsection.

To show the impact of intruder arrival patterns on the barrier coverage performance, we then proceed to perform more simulations by setting different values of the parameters in Markov chain model. Note that there are two parameters in the Markov chain model: \( T11 \) and \( T00 \). We fix \( n = 8 \) and \( m = 12 \) and vary the values of \( T11 \) and \( T00 \) from 0.15 to 0.85 with an increment of 0.1, respectively. The barrier coverage performances for all cases are plotted in Fig. 15. In Markov chain model, \( T11 \) and \( T01 \) mean the probabilities that there is an intruder arriving in next slot if there is an intruder or no intruder arriving at the current slot, respectively. When \( T11 \) is close to \( T01 \), then we cannot know much about the intruder arrival based on the current state (as the intruder arrival probabilities are close no matter if there is an intruder arriving at current slot or not).

7. FUTURE WORK

Since the model of mobile barrier deployment for dynamic object is difficult to accurately evolve, there exist several open questions for further study. One of the future works is specific condition of sensors speed of movement for different movement.
and change modes of dynamic object sides, energy efficiency is critical for mobile sensors. The optimal moved path is another future work. For centralized algorithms, characterizing the situations when the feasibility of barrier coverage can be determined in polynomial time remains an interesting open problem. Considering perpendicular movement, existence of faster algorithms for parallel barriers is an open question. Also the existences of better approximation algorithms as well as study of different movement models are of interest. Furthermore, more realistic models where final positions of sensors are not required to be on the barriers can be considered. For distributed algorithms, we considered three different existing timing models for autonomous robots. However other models such as a model where sensors have almost but not fully synchronized clocks, is suggested as a future direction. Also with existing timing models, there are still many open problems such as: Is there any algorithm for barrier coverage with sensors that each have sense of orientation but do not necessarily agree on a global orientation, in the semi-synchronous/asynchronous models? Can our fully synchronous algorithms be extended for sensors that are not necessarily on grid positions? How about algorithms that do not terminate, but eventually sensors positions coverage to those in a covering assignment? What is the average-case performance of the algorithms? Also the question whether a visibility range larger than 2R can help with designing of algorithms for barrier coverage with un oriented sensors in SSYNC model remains unanswered.

8. CONCLUSION
The cost-effective barrier coverage problem for the case of sensor scarcity has been proposed. The first design is a periodic monitoring scheduling (PMS) algorithm. Based on the insight gained from PMS, jointly exploit sensor mobility and intruder arrival information to improve barrier coverage has been proposed. Here devise a coordinated sensor patrolling (CSP) algorithm, and demonstrated that the proposed CSP can significantly enhance the barrier coverage. This paper presented two distributed versions of CSP, S-DCSP and G-DCSP, to suit the decentralized nature of WSNs. It is considered 2-barriers case, where sensors can move on two different barriers, and proposed two sensor movement algorithms. In addition, CSP to work for different intruder arrival models is generalized. The simulation results indicated that the proposed algorithms can better improve the barrier coverage performance about the intruder arrival information. The solution thus has a great potential to reduce the application budget and provides a new cost-effective approach to achieve barrier coverage in large-scale mobile sensor networks.

REFERENCES

Wireless Sensor Networks Applications, San Diego, CA, USA.


