Sensors : general definition

Origin and usage

After humanity started to live in a fixed place, they try to secure the area around home using sentinels. Next they built barriers around homes in order to keep intruders outside.
So, over the time, humanity built more efficient barriers from castle to military restricted field. A couple of decades ago, main security system was composed of sensors linked to a central unit to monitor the information, at first with human then using algorithm.

With development of new technologies, especially miniaturization, an other solution came out, put embedded systems in these sensors and let them communicate with each others to secure an area. It's a huge benefit because this is no more a centralized structure, so the failure tolerance is much bigger, however this solution is not perfect and brings many issues including system limitations or NP-complete algorithms.

In this paper we will first define what is a sensor and a barrier, in particular a barrier coverage. Next we will see some algorithms about barrier coverage using sensor in a region, and analyze them. Finally we will analyze the algorithm of the paper, see in what it is good at, and what can be done to improve it maybe using ideas of previous algorithms.

Before explain anything more, lets see in details the concept of sensors and barriers.

Part 1 section 2: sensor definition The goal of this section is to define some terms we will use on this study. Fisrt we describe what a sensor is and what different kind of sensors it exists. Then we will introduce the concept of barrier, just before the next section where we present and categorize algorithms in barrier coverage.

A sensor is a small embedded system, designed for record physical signals using a specific device. The sensor this article considers is separated in 3 parts, one for the battery life, one for the communication unit and lastly the detection unit, which is the principal unit because with this, a sensor can detect intruders. It is important to notice that the battery life is something really critical as we don't assume there is a way to recharge these sensors.

In this paper, we consider all kind of sensors especially with different detection system such as thermic, visual, acoustic, etc
The reason we accept heterogeneous detectors is because all these sensors will detect differently but eventually they will all detect the intruder in their own way. So by combining all these sensors we obtain a barrier capable of detecting an enemy.

But sensors are not different only by their detection system.

Part 1 section 3 : type of sensors We previously introduce the concept of sensors and show they can be categorized using their detection type. But it exists other ways to describe a sensor.

We always assume sensor are static but as we can see in this paper [M:???] , it exists mobile sensors that can be used with statics. However only static sensors will be considered in this study. It is also possible to split sensors into categories using their detection area. It is obvious that an acoustic sensor or a thermic can detect in a disk area, but sensor like a camera has often a conic detection zone.

Structure of a sensor

A sensor is separated in 3 parts, one for the battery life, one for the communication unit, and lastly the detection unit which is the principal unit because with this a sensor can detect intruders.
In this paper we consider all kind of sensors especially with different detection system such as thermic, visual, acoustic, etc
The reason we accept heterogeneous detectors is because all these sensors will detect differently but eventually they will all detect the intruder in their own way. So by combining all these sensors we obtain a barrier capable of detecting an enemy.

Barrier of sensors

Classification

Barrier definition

A barrier is the concept that an ensemble of sensors will assure that no intrusion can go unnoticed. That is to say, if an intruder takes a path that goes from the unsecured to the secured zone, he has to pass through the detection area of at least one sensor.

Deterministic approach

The detection area has to have some rules : in this approach, it is considered that if an external object's distance to a sensor becomes smaller than the latter's detection range, it is detected. This means that if an intruder enters the detection area of a sensor, there is no possibility that it goes unnoticed.

Probabilitic approach

The deterministic approach is nice in that it simplifies the concept of barrier coverage, but it is unrealistic : it is highly improbable that a sensor with a detection range of 50 meters will have the same chances to detect an object five centimeters away and another object 49 meters away. To have a more evolved modelization, it is possible to introduce probabilities. Thus, the probability of an intruder to be detected can be seen as a decreasing function of the distance to the sensor.

Deterministic and probabilistic algorithms

0.0.1 CCANS : Coverage centric active nodes selection

A distributed algorithm that checks if the barrier is valid, by asking other nodes if they are awake.

0.0.2 LBCP : localized barrier coverage protocol

Another distributed algorithm where every node will check if the slice of the belt it is in is covered.

0.0.3 PCP : probabilistic coverage protocol

Chosen method : Minimum Weight ϵ-Barrier Problem

Main article

The method : Minimum Weight ϵ-Barrier Problem

The method created is based on a probabilistic sensing model, where an intrusion is not automatically detected like in a deterministic model, but is subjected to a probability. This way, the concept of an ϵ-barrier emerges : for any path taken by an intruder, an ϵ-barrier will detect it with a probability of at least ϵ. This implies that the closer the intruder is to the barrier, the more chances it has to be noticed.
Since a number of sensors deployed in a true random and equiprobable, the article proposes a mathematical and geometric formulation for the calculation of the detection capability of a network of at least k sensors.
The trajectories of the intruder are straight lines and all possible trajectories of the area covered has a probability in equiprobable way.
Among the elements defined in section the notion of "free path" seems interesting to us. This average remote driven by the target in the coverage area before being detected for the first time, will help us to calculate and predict the time at which the target will be detected based on velocity models intruder.
The article defines two models of detection, first called "Instant Detection Model", which allows to detect a target when its trajectory X interesecte with the area of sensor detection. The second model, "Sampling Detection Model" requires that a target X still some time in the area covered by a sensor to get detected.
In this study the probability of detecting a target does not depend on the shapes of the coverage areas but only depends of the perimeter of those area. This approach will allow the study of networks of heterogeneous sensors.

Advantages and shortcomings of the method