Location Discovery in Sensor Network

Pin Nie
Telecommunications Software and Multimedia Laboratory
Helsinki University of Technology
niepin@cc.hut.fi

Abstract

One established trend in electronics is micromation. Many digital devices are becoming smaller and many new functionalities are built up with various sensors. Sensors and sensor networks have been widely applied in monitoring, detecting and tracking, and are especially useful for applications in hazardous or hostile environments. Location discovery is a fundamental function in sensor networks. It is important for the upper level functionalities, such as location-based routing, information organization and management. This paper reviews different aspects on localization and analyzes the advantages and disadvantages of typical solutions for a clear view of this issue.

Keywords: security, ad hoc network, attacks, secure routing

1 Introduction

Emerging technology development and advances in embedded systems and wireless connection have made it more feasible and popular to design handy and low cost sensors to accomplish many tasks. When a group of sensors are connected, the networking system can extend its functionality and scope much further than a single sensor. For example, in a sensor network, tasks deployed on different sensors can be linked together to achieve a complicated task in either a parallel way or relay style. Home network, in which all digital appliances are connected, can do various housework from ordering food to making dishes. In the missions which have to look into a big region, the sensor network is able to extend tentacles to the wild open environments, where it is hard for human to explore or even impossible in some cases, like outer space exploration. Almost all the applications of sensor networks require the location awareness in every sensor, which is an important component in the coordinates of both deployment and tasks. Therefore, location discovery is a primary issue during the design the sensor network and application.

Unlike the location discovery in fixed network, sensor network is a type of ad hoc network, which has no infrastructure at the bottom. It lacks of central servers which have rich knowledge of the location in multi-dimensions, according to the missions or network division, such as DNS and subnet address. Location discovery in ad hoc network has to take many limits into the consideration. Computation intensity, power consumption and memory are imposed by the small devices. Mobility and security are predefined challenges set by the harsh working environments for sensor network.

In this paper, we review the location discovery techniques applied in sensor network, in the presence of relevant problems. The rest of the paper is organized as follows. Section 2 addresses the basic technologies used in the location discovery and two major solution categories. Section 3 looks into the mobility feature from the view of localization. Section 4 refers to security issues in localization, in light of attacks and vulnerabilities. In the Section **??**, location discovery technologies are analyzed and discussed with the applications. Section 5 gives a summary of this paper.

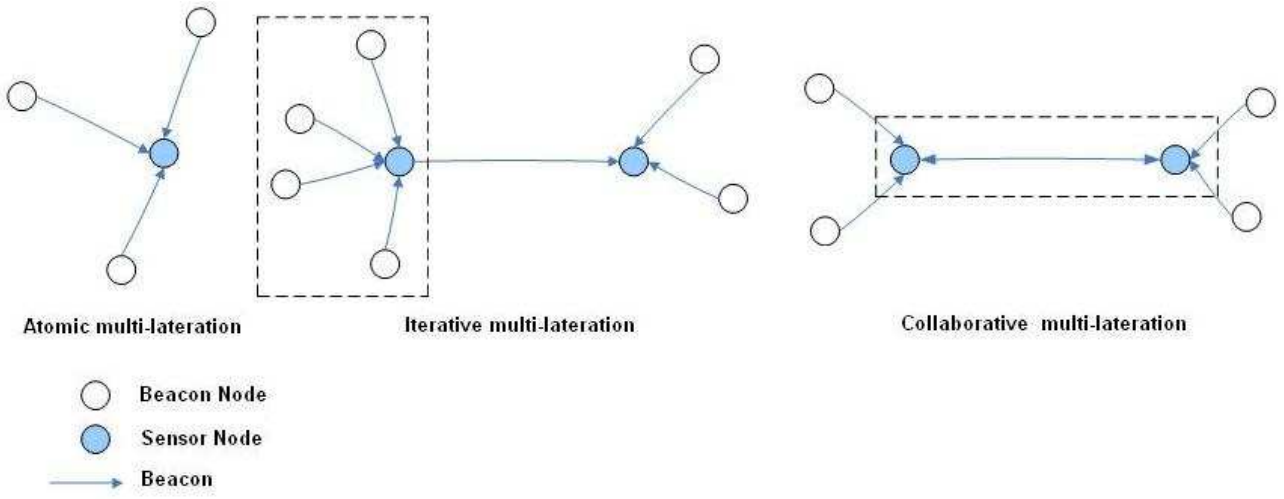

Figure 1: Three types of multi-laterations

2 Location Discovery Techniques Overview

Simply speaking, location discovery consists of two components: one is the reference points, whose coordinates are known; the other is the spatial relationship between sensors and the references point. For example, in the Global Positioning System (GPS), the GPS satellites are the reference points, and the time of arrival reveals the relationship between the GPS receiver and the satellites. In general, there are two kinds of localization based on the actor performing position computation. In the centralized localization techniques, sensor nodes transmit data to a central location, where computation is performed to determine the location of each node. On the other side, distributed localization methods rely on each node determining its location with only limited communication with nearby nodes. The latter style solutions predominate in the applications of sensor network, due to the better flexibility. There are two subtype techniques in the distributed localization, i.e. range-based and range-free. Range-based approaches exploit time of arrival (ToA), received signal strength indicator (RSSI), time difference of arrival (TDoA) and angle of arrival (AoA) to determine the distance and direction of the sensor nodes from the reference points, which is called *Beacon Nodes*. Range-free localization algorithms depends on the connectivity of the reference points, which is called *Seeds*. The connectivity parameters are denoted in the content of received messages. Solutions of this type is well known as beacon less solution.

No matter it is a beacon-based solution or beacon less solution, *multi-lateration* (ML) techniques is used as a basic procedure in the location discovery process. On the book [1], it explains three ML techniques, i.e. Atomic ML, Iterative ML and Collaborative ML. Figure 1 illustrates these three types of multi-laterations. Note that the elements in the dashed boxes can be taken as one integral part.

Both the beacon-based solution and beacon less solution have their advantages and disadvantages in the applications. We take a deep look over their principles in the following subsections.

2.1 Beacon-based solution

The first condition in the beacon-based solution is the presence of multiple beacon nodes, which know their locations. The location can be either obtained with GPS receiver or pre-configured. Based on the triangulation algorithm, at least three beacons MUST be available for the unknown sensor nodes. As aforementioned, four measurements (RSSI, ToA, DToA and AoA) are used to determine the distance and direction. From the attributes the these measurements, the synchronization of beacon is also

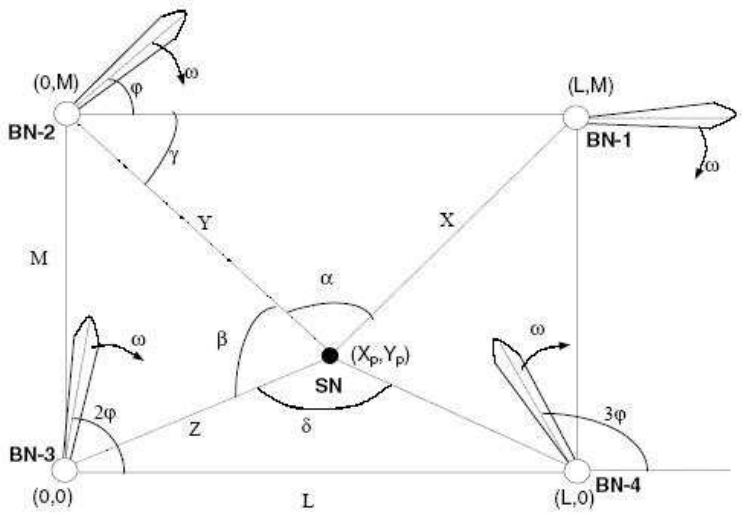

Figure 2: The model of directional beacon based location discovery scheme

required during the setup phase of sensor network. The beacon nodes broadcast the signal to cover a wide range, if not all, to connect to sensors. By listening to the beams from beacon nodes, sensors are able to calculate their positions based on the predefined algorithms. In the paper [6], a directional based location discovery scheme is proposed for wireless sensor networks. It utilizes the RSSI and ToA at the sensor side to compute the position. Figure 2 shows the general deployment of this solution.

Beacon-based solution can achieve high accuracy of the sensor location. It is also easy to adjust the radio scope and sensor deployment with the help of central administration on the beacon nodes. However, the drawbacks are obvious as well. Firstly, the beacon nodes are expensive, since they are usually equipped with GPS receivers and strong radio transmitters. Secondly, this centralized model is susceptible to attacks and errors. A single compromised BN can lead to severe degrade of the system or even failure. Thirdly, the sensor suffers intensive computation, which consumes a lot of battery. It is intolerable when the situation is too complex (e.g. too many reflections), or the sensor location changes too fast.

2.2 Beacon less solution

In contrast to the beacon-based location discovery, beacon less solutions circumvent the disadvantages by removing the beacons. They provide good alternatives for sensor networks when beacon-based solutions are infeasible. The functionality of the BN is taken in another way. Reference points is represented by the neighbors, other than beacon nodes. The neighbors obtain their locations from the deployment model. If the deployment point is predefined, sensors in the same group follow a probability distribution. In this case, location discovery is a statistical estimation problem. By using Maximum Likelihood Estimation, the sensor location can be estimated according to the observed neighbors. The more neighbors it observes, the more accurate position it gets. Usually, a grid map is applied to organize the sensors' deployment. The paper [5] designed a beacon less localization model. Figure 3 illustrates the idea of the model.

Beacon less location discovery overcome the single point failure at the beacon nodes. Sensors do not need assistance from other positioning systems, like GPS. Independence and distributed characteristic make it useful in unknown area or indoor space, where other location references is unavailable, but the division and sensor deployment can be pre-configured, e.g. outer space exploration and home network.

However, beacon less is based on static analysis. Mobility is not a feature. Deployment has direct

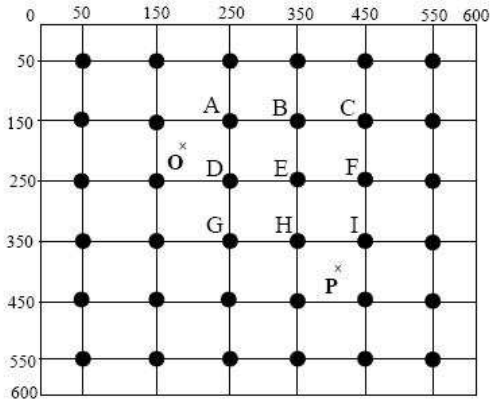

Figure 3: An Example of Group-based Deployment (each dot represents a deployment point) [5]

influence on the accuracy of localization. An accurate modeling of deployment knowledge is required. In other words, a coordinate of the target area and sensor deployment on it MUST be planned first.

3 Mobility in localization

By combining the beacon node and neighbor discovery in beacon less solution, localization for mobile sensor networks can be achieved. In the paper [4], an algorithm called Sequential Monte Carlo is used for localization. It defines three types of mobility in sensor networks as follows: (Nodes with unknown locations and Seeds with known locations)

1. *Nodes are static, seeds are moving.* For example, nodes are attached with the static buildings or objects and seeds are carried by people or moving vehicles.
2. *Nodes are moving, seeds are static.* For example, the base stations have the seeds and nodes are distributed to the wild area or carried by moving objects.
3. *Both nodes and seeds are moving.* This is the most general situation. In light of the mission, nodes and seeds may be carried by different moving objects, which wander in a big region and communicate with each other.

The key idea of Monte Carlo Localization (MCL) is to represent the posterior distribution of possible locations using a set of weighted samples. Each step is divided into a prediction phase and an update phase. Filtering is also performed by the node to remove impossible locations based on new observations. This algorithm was first developed for use in robotics localization. Therefore, a consistent learning process is involved as it appears. Simply say, the moving nodes *guess* their locations by observing surrounding seeds. The more it sees, the more location relevant knowledge it gets, and the more accurate positioning it can perform with rich inputs. In the paper [4], it claims 50 valid samples is sufficient to perform localization with good resolution. For details, please review the paper.

4 Security in localization

Security is always an important topic in any service on the computer systems and networks. It weighs heavier as the service functions at more fundamental level. Localization is an essential service in sensor network, which may provide information for upper applications. Furthermore, location refers

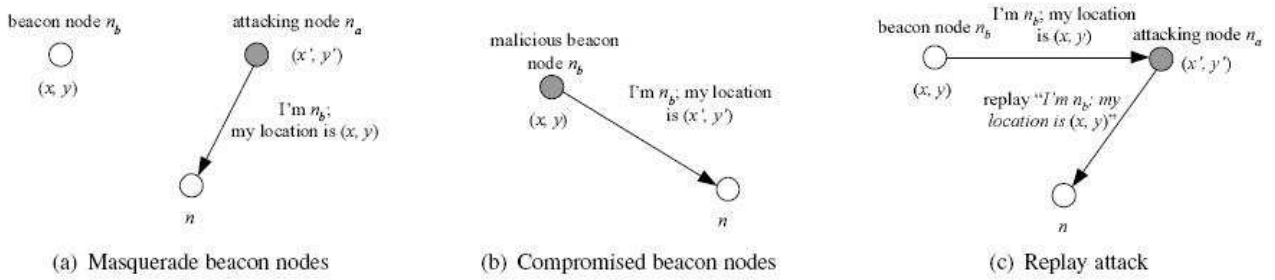

Figure 4: Attacks against location discovery schemes [2]

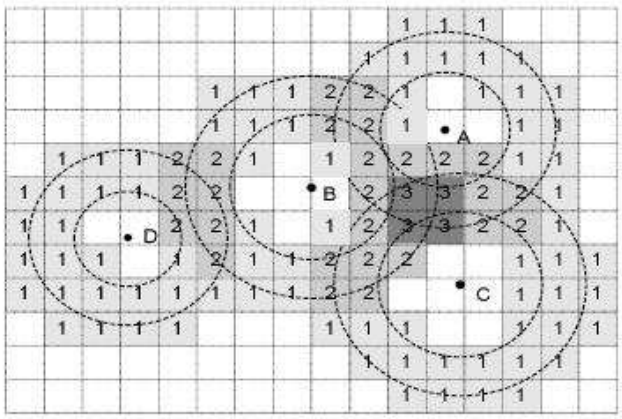

Figure 5: The voting-based location estimation [3]

to the privacy as well. Invalid disclosure of sensor's location may violate the privacy of its carrier. If the sensor network is deployed in hostile environment, attacks would be a common assumption. Basic security techniques are applied by default, for example, message authentication and digital signature.

The paper [2] provides several typical attacks on location discovery in beacon-based sensor network. Figure 4 presents the attack models. Based on the attack analysis, another paper [3] proposed two attack-resistant location estimation methods. One is called Minimum Mean Square Estimation (MMSE) and the other is a voting based scheme. Both methods explore the consistency of location information. It means few compromised beacon nodes can not cause big influence to the whole system, because the errors they inject will be detected in the consistency checking, and filtered out when under the threshold. The threshold value is determined based on the cumulative distribution of mean square error at the pre-study simulation. Unless the attacker can compromise more beacons than benign ones, it is unable to take over the localization system.

Voting-based scheme takes advantage of the radio overlapping area for location information filtering. A iterative refinement process is performed consistently to update location information. The sensor collects all location information from all candidates it can hear, and takes only the consistent values based on the algorithm calculation. Figure 5 gives an example of the voting design.

4.1 Sensor exposure

Concerning the privacy during location discovery, the less reference points the sensor exposes, the less risk it takes. Therefore, the Minimal Exposure Path (MEP) is the objective. The paper [7] designs a model based on Voronoi polygons and Delaunay triangulation. The idea is to Voronoi diagram to

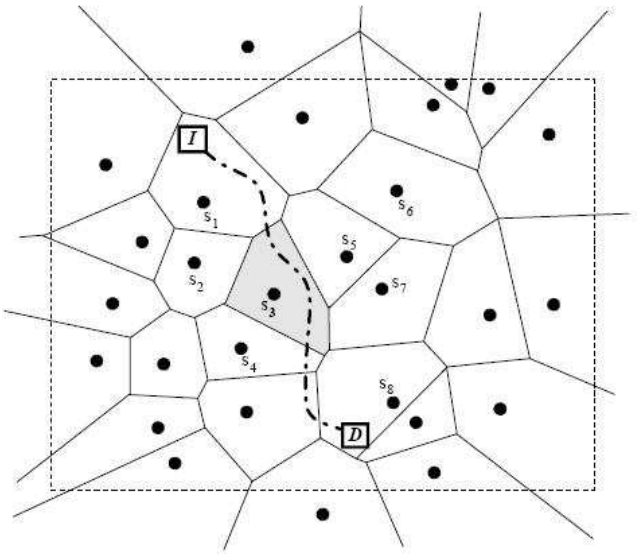

Figure 6: Overview of the Localized Minimal Exposure Path algorithm [7]

partition the plane into convex polygons by distance, and use Delaunay triangulation to get closest neighbors. Since the MEP is related to the source and destination, the partition and triangulation are computed every time for a new route. Figure 6 shows the MEP principles.

5 Conclusions

In this paper, materials on location discovery in sensor networks are reviewed for a general view of the state of art. Mobility and security are mentioned as well. In my opinion, the frameworks have been studied extensively. However, the application of localization still have big space to develop, for example, location-based routing, collaborative signal processing and optimization of communication tasks. These subjects involves many consideration on new protocol development and interoperability of existing protocols.

Location discovery relies on the coordinate, which is defined by the application. Absolute location may not be needed in many cases. Relative location is dependent on how to partition the area and how to use the location in the application. Thus, the localization study would be more meaningful when being bound with specific cases.

References

[1] C.Siva Ram Murthy and B.S.Manoj. *Ad Hoc Wireless Network: Architectures and Protocols.* Prentice Hall Ptr, 2004.

[2] P. N. Donggang Liu and W. Du. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, pages 609–619. ACM Press, 2005.

[3] P. N. Donggang Liu and W. K. Du. Attack-resistant location estimation in sensor network. In *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, 2005*, pages 99–106, Raleigh, NC, USA, 2005. IEEE.

[4] L. Hu and D. Evans. Localization for mobile sensor network. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 45–57, Philadelphia, PA, USA, 2004. ACM Press.

[5] W. D. Lei Fang and P. Ning. A beacon-less location discovery scheme for wireless sensor networks. In *Proceedings of IEEE INFOCOM*, pages 13–17, Miami, FL, USA, 2005. IEEE.

[6] A. Nasipuri and K. Li. A directionality based location discovery scheme for wireless sensor network. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 105–111, Atlanta, Georgia, USA, 2002. ACM Press.

[7] V. K. Seapahan Meguerdichian, Sasa Slijepcevic and M. Potkonjak. Localized algorithms in wireless ad-hoc network: Location discovery and sensor exposure. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 106–116, Long Beach, CA, USA, 2001. ACM Press.