Secure and Resilient Localization in Wireless Sensor Networks

Peng Ning¹, Donggang Liu², and Wenliang Du³

¹ Department of Computer Science, North Carolina State University pning@ncsu.edu
² Department of Computer Science and Engineering, University of Texas at Arlington dliu@cse.uta.edu
³ Department of Electrical Engineering and Computer Science, Syracuse University wedu@ecs.syr.edu

1 Introduction

Recent technological advances have made it possible to develop distributed sensor networks consisting of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate in short distances through wireless links [1]. Such sensor networks are ideal candidates for a wide range of applications such as health monitoring, data acquisition in hazardous environments, and military operations. The desirable features of distributed sensor networks have attracted many researchers to develop protocols and algorithms that can fulfill the requirements of these applications (e.g., [1, 12, 14, 17, 28, 29, 32]).

Sensors’ locations play a critical role in many sensor network applications. Not only do applications such as environment monitoring and target tracking require sensors’ location information to fulfill their tasks, but several fundamental techniques developed for wireless sensor networks also require sensor nodes’ locations. For example, in geographical routing (e.g., FACE [2, 3], GPSR [3, 4, 18]), sensor nodes make routing decisions at least partially based on their own and their neighbors’ locations. As another example, in some data-centric storage applications such as GHT [33, 36], storage and retrieval of sensor data highly depend on sensors’ locations. Indeed, many sensor network applications will not work without sensors’ location information.

The Global Positioning System (GPS) is a popular outdoor localization system for mobile devices. However, due to the cost reasons, it is highly undesirable to have a GPS receiver on every sensor node. Moreover, in some situations such as indoor sensor network applications, GPS cannot be used for localization because of interferences and obstacles. This creates a demand for efficient and cost-effective location discovery algorithms in sensor networks. In the past several years, a number of location discovery protocols have been proposed to reduce or completely remove the dependence on GPS in wireless sensor networks [4, 8, 13, 26, 27, 30, 31, 34, 35].
These protocols share a common feature: They all (with one exception [11]) use some special nodes, called beacon (or anchor) nodes, which are assumed to know their own locations (e.g., through GPS receivers or manual configuration). (For this reason, we call these location discovery techniques beacon-based location discovery.) These protocols work in two stages. In the first stage, non-beacon nodes receive radio signals called beacon signals from the beacon nodes. The packet carried by a beacon signal, which we call a beacon packet, usually includes the location of the beacon node. The non-beacon nodes then estimate certain measurements (e.g., distance between the beacon and the non-beacon nodes) based on features of the beacon signals. Features that may be used for location determination include Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), Time Difference of Arrival (TDoA), and Angle of Arrival (AoA). We refer to such a measurement (e.g., the distance) and the location of the corresponding beacon node collectively as a location reference. In the second stage, when a sensor has enough number of location references from different beacon nodes, it determines its own location in the network field. A typical approach is to consider the location references as constraints that a sensor node’s location must satisfy, and estimate it by finding a mathematical solution that satisfy these constraints with minimum estimation error. Existing approaches either employ range-based methods \([8,27,30,34,35]\), which use the exact measurements obtained in stage one, or range-free ones \([4,13,26,31]\), which only need the existences of beacon signals in stage one.

As a fundamental service critical to many sensor network applications, location discovery in hostile environments is certainly subject to attacks. As illustrated in Figure 1, an attacker may provide incorrect location reference information by pretending to be valid beacon nodes (Figure 1(a)), compromising beacon nodes (Figure 1(b)), or replaying the beacon packets that he/she intercepted in different locations (Figure 1(c)). In either of the above cases, non-beacon nodes will determine their locations incorrectly. As a result, the attacker can effectively disable or mislead the localization service, and none of the sensor network applications that require sensors’ locations will work as expected.

Both security and sensor network researchers have realized this problem. In the past two years, a number of techniques have been proposed for secure and resilient localization, from target localization (e.g., \([5]\)), where a number of trusted nodes determine the location of a potentially malicious node, to node localization (e.g., \([21,24]\)), where a non-beacon node determines its own location based on information provided by potential attackers. Some of these techniques target at range-based localization (e.g., \([21,24]\)), while some others focus on range-free localization (e.g., \([19,20]\)).

In this chapter, we would like to discuss two recent efforts for achieving secure and resilient localization in sensor networks: a suite of attack-resistant location estimation techniques \([24]\), and a mechanism for detecting malicious beacon nodes \([25]\). Other related techniques can be found in the other chapters of this edited volume.