Chapter 8
Preserving Security of Mobile Anchors Against Physical Layer Attacks:
A Resilient Scheme for Wireless Node Localization

Rathindra Nath Biswas
A. J. C. Bose Polytechnic, India

Swarup Kumar Mitra
MCKV Institute of Engineering, India

Mrinal Kanti Naskar
Jadavpur University, India

ABSTRACT

This chapter introduces a new security scheme for mobile anchors avoiding the physical layer attacks towards localization in wireless sensor networks (WSNs). In a network, anchors are made location-aware equipping them with GPS (global positioning system) receivers. Direction finding capabilities are also incorporated with smart antennas. The proposed algorithm is based on adaptive beamforming of smart array that always minimizes the probabilities of successful attacks, keeping the adversaries beyond its beam coverage. Particle swarm optimization (PSO) technique is used to compute array excitation coefficients, generating the desired pattern. Thus, anchors remain secured through pattern irregularities, deteriorating the information retrieval process even though chances of occurring adequate RSS (received signal strength)/AoA (angle of arrival) measurements may exist. Moreover, anchors are assumed to send pseudo references towards stationary nodes over private links, preserving data integrity for localization. Simulation results validate its effectiveness over the existing methods.

DOI: 10.4018/978-1-5225-5742-5.ch008

INTRODUCTION

During the last decades, continuous efforts were made to bring the diverse technologies in a common platform. The outcome can be viewed as an Internet of Things (IoT), an amalgamation of the Internet and smart sensors to ensure connectivity, computation and communications among the heterogeneous entities (Al-Gburi et al., 2018; Misra et al., 2017). Wireless sensor networks might be regarded as an example of such infrastructures. It inherently possesses numerous attractive features such as scalability, fault-tolerance capability, low power requirements, and less establishment cost, etc. Hence, such network architectures, comprising a considerable number of battery-driven tiny sensors, have now become much famous for data gathering applications under the hostile environments (Akyildiz et al., 2002; Biswas et al., 2014). For example, several essential services, both in civil and military sectors, often deploy such kind of network structures for various purposes like continuous monitoring of the environments, security surveillance, target detection, and tracking, etc. in the areas of interest. However, such applications frequently need location-based data to be relayed at the sink or base station (BS) for the realization of any event occurring within the networks. Usually, sensor devices are randomly deployed over the harsh fields from aircraft/ space vehicles to collect raw data from their surroundings. Accordingly, they remain scattered, unattended and unaware of their locations unless they are made location-aware by some system supports or being localized with the help of a localization system (Ou, 2011; Akter et al., 2018). In practice, a variety of network architectures are commonly existing. They are classified as (i) static networks consisting of stationary nodes only (ii) mobile networks comprised of mobile nodes only and (iii) quasi-static networks involving few mobile nodes along with the plentiful stationary nodes. However, random deployment causes some coverage problem in the first configurations because there is no provision of node relocations. Instead, the second arrangements could provide adequate coverage, but they seem to be much more energy inefficient. In this context, a more feasible solution might be obtained with the third configurations, and hence, it has now become the basis for the development of the state-of-the-art WSN architectures (Halder and Ghosal, 2016; Lin et al., 2017). Throughout the entire networks, mobile nodes can move freely, and they act as mobile data collectors (MDC) (Pazzi and Boukerche, 2008). For several location-based services (LBS), they also need to be location aware along their trajectories. Hence, they usually are made as embedded systems with GPS (Global Positioning System) receivers. Such nodes are referred to as the mobile anchors or beacons in WSNs literature. By employing suitable localization systems, on the other hand, stationary nodes are made capable of relaying location-based data to the base station in a cooperative manner. In most of the cases, anchors are also used as reference nodes for the localization process (Ssu et al., 2005; Naraghi-Pour