Chapter XXXVII
Localization Security in Wireless Sensor Networks

Yawen Wei
Iowa State University, USA

Zhen Yu
Iowa State University, USA

Yong Guan
Iowa State University, USA

ABSTRACT

Localization of sensor nodes is very important for many applications proposed for wireless sensor networks (WSN), such as environment monitoring, geographical routing, and target tracking. Because sensor networks may be deployed in hostile environments, localization approaches can be compromised by many malicious attacks. The adversaries can broadcast corrupted location information; they can jam or modify the transmitting signals between sensors to mislead them to obtain incorrect distance measurements or nonexistent connectivity links. All these malicious attacks will cause sensors not able to or wrongly estimate their locations. In this chapter, we summarize the threat models and provide a comprehensive survey and taxonomy of existing secure localization and verification schemes for wireless sensor networks.

INTRODUCTION

In recent years, the availability of low-cost, low-power, multifunctional, small-size autonomous devices equipped with various sensors has expedited the development of wireless sensor networks (WSN). Wireless sensor networks have both military applications (e.g., battlefield surveillance) and civilian applications (e.g., environment and habitat monitoring, target tracking, seismic detection, smart-home automation, and traffic control). To facilitate the cooperation between sensors and achieve different application goals, network and application protocols such as routing protocol, data

aggregation algorithm, and localization algorithm need to be properly designed.

Among these research issues, localization of sensor nodes is very important to some applications. For example, in environment surveillance applications, a sensor must report its location to the monitoring center when it detects some enemy force (e.g., a tank); in geographical routing protocol, a sensor should know the locations of its neighbors and forwards data packets to the neighbor who is closest to the destination.

Traditional localization approaches require the sensor nodes to equip with expensive global positioning system (GPS) devices, which are not affordable in some cases, especially in large-scale sensor networks. Hence, many localization schemes (Bahl & Padmanabhan, 2000; Bulusu, Heidemann, & Estrin, 2000; Doherty, Pister, & Ghaoui, 2001; Fang, Du, & Ning, 2005; Harter, Hopper, Steggles, Ward, & Webster, 1999; He, Huang, Blum, Stankovic, & Abdelzaher, 2003; Lazos & Poovendran, 2004; Nicolescu & Nath, 2001, 2003; Priyantha, Chakraborty, & Balakrishnan, 2000; Savvides, Han, & Srivastava, 2001; Shang, Ruml, Zhang, & Fromherz, 2003; Smith, Balakrishnan, Goraczko, & Priyantha, 2004) have been proposed. These schemes assume that some special sensor nodes (named anchors) can obtain their absolute locations through GPS device. Thus other sensors can use the measured distance or connectivity information between them and the beacon messages sent from the anchors to calculate their locations.

When sensor networks are deployed in hostile environments, localization approaches are vulnerable to many malicious attacks. For example, the adversaries can compromise a sensor node and send out false location information to disturb the localization of other nodes. Sensor nodes are constrained by limited energy resources, memory resource, computation ability, and communication bandwidth, therefore, traditional cryptography mechanisms such as a public key system cannot be applied to wireless sensor networks. Moreover, localization approaches utilize the physical features of the transmitting signals between sensors (e.g., transmitting time or signal strength), thus they are vulnerable to many localization-specific attacks (e.g., distance-modification attack) that cannot be prevented by traditional security mechanisms. All these attacks can cause the sensors to be not able to or wrongly estimate their locations.

In this chapter, we provide a comprehensive survey and taxonomy of existing countermeasures that secure the localization in wireless sensor networks. We classify the secure countermeasures into secure localization schemes, which enhance sensors' attack-resistant ability, and location verification schemes, which verify sensors' locations (accept the correct location estimations and discard the abnormal ones) after the sensors have obtained their locations. We also classify these secure localization (or verification) schemes on whether they use precise (with nanosecond precision) time-measuring hardware, sectored antenna, or not use any special hardware.

The rest of chapter is organized as following: In the following section, we take an overview and give a classification of current localization approaches. We describe the threat models, and we provide the taxonomy of existing secure localization approaches. Finally, we discuss some future trends and conclude the chapter.

BACKGROUND: LOCALIZATION IN WIRELESS SENSOR NETWORKS

In recent years, many localization approaches have been proposed for wireless sensor networks. Before we talk about the security issues, let us take an overview of the localization systems and the techniques involved in different localization approaches.

The most traditional and widely-used localization system is the global positioning system. The earth-based GPS receivers can provide users with location, speed, and time by calculating the distances from at least three satellites. However, it is not feasible to equip the relatively expensive GPS receiver on each node in large scale sensor networks. Most localization algorithms assume that only a fraction of sensor nodes in the field can obtain their locations through GPS receivers (or