Chapter 10
Enhancing Location Privacy in WSN: The iHide Case

Leonidas Kazatzopoulos
Athens University of Economics and Business, Greece

ABSTRACT

Wireless Sensor Networks (WSNs) receive significant attention due to the wide area of applications: environment monitoring, tracking, target detection, etc. At the same time, in some cases, the captured information from the WSN might be considered as private, for example, location of an important asset. Thus, security mechanisms might be essential to ensure the confidentiality of the location of the information source. In this chapter, the authors present an approach called iHIDE (information HIDing in Distributing Environments) to enable source-location privacy in WSNs. iHIDE adopts a non-geographical, overlay routing method for packet delivery. This chapter presents the architecture and assesses its performance through simulation experiments, providing comparisons with relative approaches.

INTRODUCTION

The WSNs technology aims to provide useful tools on monitoring and location-based applications. Contrary to stand-alone sensors, WSNs consist of cooperative nodes that forward, process, aggregate, route and disseminate information to other nodes, and finally to a central sensor, so called the sink, for further processing. From the sink, the information is passed to the users and service platforms. The WSN architecture that utilizes one or more sinks is considered as the most prevailing (Akyildiz et al., 2002; Heinzelman et al., 1999; Tilak et al., 2002), whilst other configurations have been designed, as well (Akyildiz et al., 2002). WSNs by default are not robust against
adversaries. An unauthorized opponent can gain access to classified data either by accessing aggregated information that is stored in sensors or by sensing and pilfering wireless transmissions. Thus, the deployment of WSNs arises privacy concerns. Privacy might not be a primary issue for several types of WSNs, such as environmental monitoring installations. On the other hand, it is crucial when WSNs are used by military applications, and especially for locating valuable assets or people. Lopez identifies two types of privacy in WSNs (Tilak et al., 2002): social and network privacy. Social privacy incorporates the concerns for collecting and manipulating our personal data. Network privacy is associated with the content that is stored, aggregated, and communicated between the WSN’s nodes. It also concerns the identity privacy, since the IDs of the nodes are subject to spoofing. Finally, it deals with the location privacy and the inferring of the physical position of a node, or of the asset that is monitored. This issue is addressed here, and the iHIDE architecture, which was originally introduced in (Kazatzopoulos et al., 2006), shields the position of the information source, i.e., the sensor that captures and reports the existence of an asset (i.e., target). iHIDE is applicable for WSNs deployed in a predefined geographical area to track a specific object with e.g., an embedded RF tag, or objects of a particular category, such as children, elderly, artifacts or even pandas (Lopez Munoz, 2005). In this type of WSNs the location information is eavesdropped either by monitoring the packet routing algorithm, or by intercepting the contents of the data packets. iHIDE uses a lightweight, end-to-end, cryptographic technique to protect the information content, and a hop-by-hop routing scheme to prevail the physical location of the source sensor.

The structure of this chapter is as follows. Firstly, next section introduces the iHIDE architecture and the mechanisms that enforce location privacy. The threats and security issues related to the iHIDE scheme are discussed in Section ‘Identifying Privacy Issues’. Subsequently, Section ‘Simulation Experiments’ provides the experimental setup and the evaluation of the scheme. Section ‘Exercises’ notes issues for further discussion and the chapter closes with some proposed exercises.

**iHIDE ARCHITECTURE AND ROUTING PLAN**

Before describing in details the iHIDE scheme, it is essential to define what we consider as Location Information (LocInfo). As LocInfo we use a variation of the definition introduced in (Kamat et al., 2005), i.e., we use the triple of the following form: \(\{\text{SensorID}, \text{RTargetID}, \text{Time}\}\). Thus, LocInfo is defined as a combination of the sensor that identifies the target, the identification of the target, and the time instance of the target existence.

iHIDE consists of the following functional elements and structures: Sensing Nodes (SEN), Bus Nodes (BUN), one Sink Node (SIN), one Bus and several Rings. We could visualize this through a configuration that consists of one rope with Rings attached to it (Figure 1). SENs organize the Ring structures, whilst BUNs construct the Bus struc-
Related Content

Quality-Oriented Mobility Management for Multimedia Content Delivery to Mobile Users
www.igi-global.com/chapter/quality-oriented-mobility-management-multimedia/56418?camid=4v1a

Enhancing Location Privacy in Location-Based Services: The STS Case
www.igi-global.com/chapter/enhancing-location-privacy-location-based/76791?camid=4v1a

Capacity and Service (CapServ) Adaptive Trust Computation by Territory Formation in Ubiquitous Environment

An Improved Connection Method for Multi-Core SoC
www.igi-global.com/article/improved-connection-method-multi-core/68805?camid=4v1a