Chapter XXVII
Privacy and Anonymity in Mobile Ad Hoc Networks

Christer Andersson
Combitech, Sweden

Leonardo A. Martucci
Karlstad University, Sweden

Simone Fischer-Hübner
Karlstad University, Sweden

ABSTRACT

Providing privacy is often considered a keystone factor for the ultimate take up and success of mobile ad hoc networking. Privacy can best be protected by enabling anonymous communication and, therefore, this chapter surveys existing anonymous communication mechanisms for mobile ad hoc networks. On the basis of the survey, we conclude that many open research challenges remain regarding anonymity provisioning in mobile ad hoc networks. Finally, we also discuss the notorious Sybil attack in the context of anonymous communication and mobile ad hoc networks.

INTRODUCTION

The quest for privacy in today's increasingly pervasive information society remains a fundamental research challenge. In the traditional (wired) Internet, one essential means for protecting privacy is *anonymous communication*. Being anonymous usually implies that a user remains unlinkable to a set of items of interest (e.g., communication partners, messages) from an attacker's perspective (Pfitzmann & Hansen, 2006). The capabilities of the attacker are usually modeled by an *attacker model*, which can, for instance, include a rogue communication partner or an observer tapping the communication lines. Further, more advanced applications can be deployed on top of anonymous

communication mechanisms, to, for instance, enable pseudonymous applications.

This chapter investigates how anonymous communication can be enabled in *mobile ad hoc networks* (Corson & Macker, 1999); networks constituted by mobile platforms that establish on-the-fly wireless connections among themselves and ephemera networks without central entities to control it. They are of great importance as they constitute a basic core functionality needed for deploying *ubiquitous computing*. In short, ubiquitous computing would allow for computational environments providing information instantaneously through "invisible interfaces," thus allowing unlimited spreading and sharing of information. If realized, ubiquitous computing could offer an invaluable support for many aspects of our society and its institutions. However, if privacy aspects are neglected, there is a great likelihood that the end product will resemble an Orwellian nightmare.

In this chapter, we study how privacy and anonymity issues are tackled today in mobile ad hoc networks by surveying existing anonymous communication mechanisms adapted for mobile ad hoc networks[1]. Only recently, a number of such proposals have been suggested. In the survey, we evaluate some of these approaches against a set of general requirements (Andersson, Martucci, & Fischer-Hübner, 2005), which assess to which degree these approaches are suitable for mobile ad hoc networks. We also discuss Sybil attacks (Douceur, 2002) in the context of anonymous communication and mobile ad hoc networks.

This chapter is structured as follows. First, an introduction to privacy, anonymity, and anonymity metrics is provided in "Background." Then, existing approaches for enabling anonymity in ad hoc networks are described in "Anonymous Communication in Mobile Ad Hoc Networks." In "Survey of Anonymous Communication Mechanisms for Ad Hoc Networks" these approaches are evaluated against the aforementioned requirements. Then, Sybil attacks in the context of anonymous communication and mobile ad hoc networks are discussed in "Future Trends." Finally, conclusions are drawn in "Conclusions."

BACKGROUND

In this section, the concepts of privacy and anonymity and their relation are introduced. Methods for quantifying anonymity are also discussed.

Definitions of Anonymity and Related Concepts

Pfitzmann and Hansen (2006) define *anonymity* as "the state of being not identifiable within a set of subjects, the *anonymity set*" (p. 6). The anonymity set includes all possible subjects in a given scenario, such as possible senders of a message.

Related to anonymity is *unlinkability*, where unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, events, actions, etc.) means that within the system (comprising these and pos-

Figure 1. Unlinkability between a user in the anonymity set and an item of interest