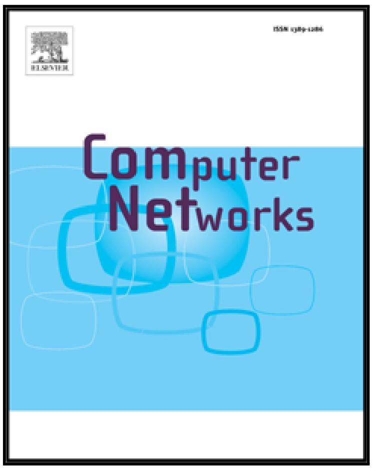

MSP: Providing Location Privacy in WLAN Networks with a MAC Swapping Protocol

O. Arana, F. Garcia, J. Gomez, V. Rangel

PII: S1389-1286(18)30150-6
DOI: 10.1016/j.comnet.2018.03.030
Reference: COMPNW 6457

To appear in: *Computer Networks*

Received date: 30 June 2017
Revised date: 15 December 2017
Accepted date: 27 March 2018

Please cite this article as: O. Arana, F. Garcia, J. Gomez, V. Rangel, MSP: Providing Location Privacy in WLAN Networks with a MAC Swapping Protocol, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.03.030

MSP: Providing Location Privacy in WLAN Networks with a MAC Swapping Protocol

O. Arana, F. Garcia, J. Gomez, V. Rangel

Department of Telecommunications Engineering, National Autonomous University of Mexico, 04510 Mexico City, Mexico

Abstract

Location privacy has been widely studied in the context of location-based services (LBS). However, a far more serious location privacy threat arises when malicious eavesdroppers listen to wireless transmissions from an unsuspecting mobile user in order to pinpoint his location and figure out his identity. This new scenario is known as *location estimation* (LE). While there are several strategies to mitigate the threats posed by LBS scenarios, only a few researchers deal with countermeasures for LE scenarios. This paper proposes MSP, a MAC swapping protocol that allows two mobile users to discreetly exchange their MAC addresses without malicious eavesdroppers being able to detect it. In this way, although potential eavesdroppers can still pinpoint the location of a transmitting node, they will get its identity wrong. Over time, MSP eliminates the eavesdroppers' ability to link the position and identity of a transmitting source. In contrast to related research, the identity exchange in MSP takes into account information from the mobile users' physical and MAC layers simultaneously, so an attack in one layer does not expose the identity exchange in the other layer. In order to provide location privacy, MSP uses two algorithms. The first algorithm works at the physical layer, allowing two mobile nodes to decide when and where to exchange their MAC addresses. The second algorithm uses virtual interfaces to guarantee that the identity exchange does not exhibit any abnormal behavior at the MAC layer. Test-bed and simulation experiments demonstrate that MSP is able to guarantee location privacy even with attackers eavesdropping at the physical and MAC layers simultaneously.

Keywords:
Location privacy, MAC exchange, anonymity, location estimation

1. Introduction

Location-based services (LBS) are becoming more and more popular because of the exponential use of mobile devices. Nowadays, most of these devices are equipped with multiple embedded sensors (e.g., accelerometer, GPS, and so on), facilitating the development of a variety of applications based on location information. Interacting with LBS usually requires mobile users to provide their current location (typically acquired by GPS) to obtain information such as specific directions to reach a destination, or request services from a taxi company, for example. However, this type of transaction creates location privacy concerns for mobile users since their location could be used by LBS for other purposes not authorized by the user. In [1], the authors defined the location privacy problem as *"the ability to prevent other parties from learning one's current or past location."* To mitigate the location privacy problem, several techniques have been proposed in recent years in the context of LBS. Most of these techniques can be grouped into obfuscation and anonymity categories. Obfuscation techniques require mobile users to provide a non-accurate location to the LBS while still being able to receive meaningful information. Anonymity techniques, on the other hand, consider *"the*

Email addresses: arana.h.oscar@comunidad.unam.mx (O. Arana), fgarcia@fi-b.unam.mx (F. Garcia), javierg@fi-b.unam.mx (J. Gomez), victor@fi-b.unam.mx (V. Rangel)