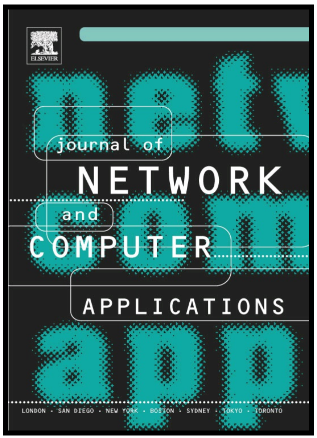
ELSEVIER
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

On Location-Privacy in Opportunistic Mobile Networks, A Survey

Sameh Zakhary, Abderrahim Benslimane

PII: S1084-8045(17)30355-7
DOI: https://doi.org/10.1016/j.jnca.2017.10.022
Reference: YJNCA2002

To appear in: *Journal of Network and Computer Applications*

Received date: 26 May 2017
Revised date: 4 October 2017
Accepted date: 28 October 2017

Cite this article as: Sameh Zakhary and Abderrahim Benslimane, On Location-Privacy in Opportunistic Mobile Networks, A Survey, *Journal of Network and Computer Applications,* https://doi.org/10.1016/j.jnca.2017.10.022

On Location-Privacy in Opportunistic Mobile Networks, A Survey

Sameh Zakhary[a,1,*], Abderrahim Benslimane[b,2]

[a] University of Nottingham, UK

[b] University of Avignon, France

Abstract

In recent years, networked devices spread into different activities in our daily lives enabling many innovative applications. These applications were not only computationally-intelligent on their own, but also enabled collection and sharing of users' information via opportunistic and pervasive communications. This omnipresence of devices capable of continuously tracking sensitive contexts and whereabouts raised users' concerns about their own privacy. In this paper, we present a survey of privacy-protection solutions proposed for Opportunistic Networks. Firstly, we provide a detailed study of the privacy problem and major privacy-related attacks. Secondly, we present contemporary research efforts aiming to protect users' privacy with special focus on location-privacy problem, while discussing the applicability of each solution in Opportunistic Networks (OppNets). Thirdly, a taxonomy of privacy-preserving approaches is proposed showing the major trends in addressing this challenging problem. A systematic evaluation of the advantages and disadvantages is presented. Using this study, we present various design space elements (criteria and factors) required to successfully offer better location-privacy. Moreover, we propose a unified framework that addresses these design space elements while enabling opportunistic communications between users. To illustrate our purpose, we apply this framework to a protocol that offers location-privacy through obfuscation in mobile opportunistic networks. This illustration shows the feasibility and effectiveness of our proposed framework. We explore key design space elements: criteria (such as scalability) and factors (such as social-awareness of ties, and location-awareness) to achieve the highest possible privacy level under different network conditions and nodes' requirements.

Keywords: Mobile opportunistic network, Distributed computing, Anonymity, Location privacy

[*] Corresponding author

Email addresses: `sameh.zakhary@nottingham.ac.uk` (Sameh Zakhary), `abderrahim.benslimane@univ-avignon.fr` (Abderrahim Benslimane)

[1] S. Zakhary is with the School of Computer Science

[2] A. Benslimane is with the Computer Science Laboratory of Avignon (LIA)