

Accepted Manuscript

Privacy-Preserving Mobile Crowd Sensing in Ad Hoc Networks

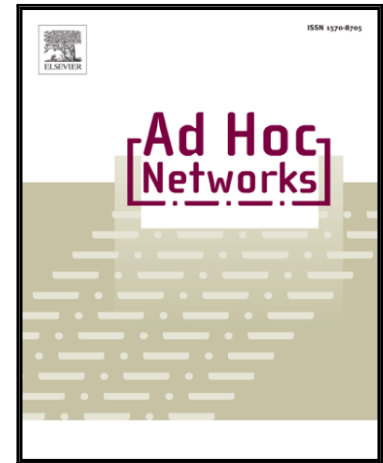
Zhijie Wang, Dijiang Huang

PII: S1570-8705(18)30033-7
DOI: [10.1016/j.adhoc.2018.02.003](https://doi.org/10.1016/j.adhoc.2018.02.003)
Reference: ADHOC 1637

To appear in: *Ad Hoc Networks*

Received date: 25 October 2016
Revised date: 1 July 2017
Accepted date: 7 February 2018

Please cite this article as: Zhijie Wang, Dijiang Huang, Privacy-Preserving Mobile Crowd Sensing in Ad Hoc Networks, *Ad Hoc Networks* (2018), doi: [10.1016/j.adhoc.2018.02.003](https://doi.org/10.1016/j.adhoc.2018.02.003)



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Privacy-Preserving Mobile Crowd Sensing in Ad Hoc Networks

Zhijie Wang, Dijiang Huang

Department of Computer Science and Engineering, Arizona State University, 699 S Mill Avenue, Tempe, AZ 85281, United States

Abstract

The presence of a rich set of embedded sensors on mobile devices has been propelling various sensing applications regarding individual activities and their surrounding environment, and these persuasive sensing-capable mobile devices are pushing the new paradigm of Mobile Crowd Sensing (MCS) from sketch to reality. MCS aims to outsource sensing data collection to Mobile Device Owner (MDO) and it could revolutionize the conventional ways of sensing data collection and processing. Nonetheless, the widespread deployment of MCS gives rise to the privacy concerns from both the MDOs and the Sensing Service Consumers (SSC), especially in the case where MCS relies on untrustworthy third-party infrastructures. This paper proposes three protocols to address the privacy issues of MCS in ad hoc network without depending on any third-parties. It first presents Privacy-Preserving Summation (PPS) protocol to protect the privacy of the SSCs. Next, it puts forward Privacy-Preserving Difference Rank Computation (PPDRC) protocol to ensure the privacy of the MDOs. Finally, it proposes Approximate K-Nearest Neighbor with Privacy Preservation (AKN2P2) to approximately identify the k-nearest neighbors without privacy leaks of both the MDOs and the SSCs. The performance evaluations demonstrate the computation overhead in different settings.

Keywords: Mobile Crowd Sensing, Ad Hoc Network, Privacy Preservation

Email addresses: zwang134@asu.edu (Zhijie Wang), dijiang@asu.edu (Dijiang Huang)

Download English Version:

<https://daneshyari.com/en/article/6878518>

Download Persian Version:

<https://daneshyari.com/article/6878518>

[Daneshyari.com](https://daneshyari.com)