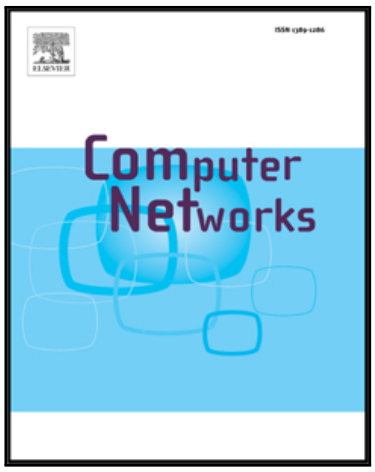

Trust Management and Reputation Systems in Mobile Participatory Sensing Applications: A Survey

Hayam Mousa, Sonia Ben Mokhtar, Omar Hasan, Osama Younes, Mohiy Hadhoud, Lionel Brunie

PII: S1389-1286(15)00234-0
DOI: 10.1016/j.comnet.2015.07.011
Reference: COMPNW 5613

To appear in: *Computer Networks*

Received date: 30 October 2014
Revised date: 13 June 2015
Accepted date: 3 July 2015

Please cite this article as: Hayam Mousa, Sonia Ben Mokhtar, Omar Hasan, Osama Younes, Mohiy Hadhoud, Lionel Brunie, Trust Management and Reputation Systems in Mobile Participatory Sensing Applications: A Survey, *Computer Networks* (2015), doi: 10.1016/j.comnet.2015.07.011

Trust Management and Reputation Systems in Mobile Participatory Sensing Applications: A Survey

Hayam Mousa[a,b,*], Sonia Ben Mokhtar[a], Omar Hasan[a], Osama Younes[b], Mohiy Hadhoud[b], Lionel Brunie[a]

[a] *LIRIS, INSA de Lyon, France, {Hayam.Kafaky; Omar.Hasan; Sonia.Benmokhtar; Lionel.Brunie}@insa-lyon.fr*
[b] *Faculty of Computers & Information, Menoufia University, Egypt, {osama.younes; mmhadhoud}@ci.menofia.edu.eg*

Abstract

Participatory sensing is an emerging paradigm in which citizens everywhere voluntarily use their computational devices to capture and share sensed data from their surrounding environments in order to monitor and analyze some phenomenon (e.g., weather, road traffic, pollution, etc.). Interest in participatory sensing systems has risen since a large mobile sensor network can now be opportunistically constructed with much less cost and effort than it was the case a decade ago. However, relying on citizens who share their contributions raises many challenges. Participants can disrupt the system by contributing corrupted, fabricated, or erroneous data. Consequently, monitoring the participants' behavior in order to estimate their honesty is an essential requirement. This enables to evaluate the veracity and accuracy of participants' contributions and therefore, to build robust and reliable participatory sensing systems. Recently, several trust and reputation systems have been proposed to trace participants' behavior in these systems. This survey presents a study and analysis of existing trust systems in participatory sensing applications. First, we study the nature of participatory sensing applications by surveying existing systems and outlining their common features. We then analyze the main vulnerabilities and attacks that can be launched in these systems. Furthermore, we discuss the concept of trust and we introduce a classification of existing trust systems. The two main classes of trust assessment methods for participatory sensing (i.e. Trusted Platform Module and reputation) are discussed. In addition, we analyze the merits as well as the limitations of each of them. We then derive a comparative study of several existing trust systems for participatory sensing. From this study, we identify many trust problems that have not been solved and many attacks have not been addressed yet in the literature. Finally, we list future research directions regarding trust management in participatory sensing systems.

Keywords: Participatory sensing, vulnerabilities, trust systems, TPM, reputation, challenges

1. Introduction

Everyday, millions of people move around carrying a variety of handheld devices equipped with sensing, computing, and networking capabilities (e.g., smartphones, tablets, music players, GPS watches, in-vehicle sensors, etc.) [1]. The advancement and widespread use of such devices have contributed toward the emergence of a new kind of application called *participatory sensing* [2]. These applications exploit both the mobility of participants and the sensing capabilities of their devices to construct opportunistic mobile sensor networks [3].

In participatory sensing, participants capture sensed data from their surrounding environment using a variety of sensors (e.g., GPS, camera, microphone, accelerometer, gyroscope, digital compass, etc.) embedded in their devices. Then, they share their collected observations with a backend server, which processes the received data to monitor, map, or analyze some incidents or phenomena of common interest.

Participatory sensing systems can be applied to serve many of our daily life needs, including health monitoring (e.g., [4, 5, 6, 7, 8]), traffic monitoring (e.g., [9, 10, 11, 12]), noise monitoring (e.g., [6, 13, 14]), weather monitoring (e.g., [15, 6]), activities monitoring [16, 17, 18, 19, 20], commerce [21, 22], sports monitoring [23], as well as other applications [24].

In these applications, no restrictions are usually imposed about the participants' experience, concern, trustworthiness, and interest. In addition, they are not usually paid for their participation in the sensing campaign. Thus, they usually do not have strong motivations to comply with the tasks' requirements. That is, they are not concerned about some parameters which may improve the quality of their contributions (e.g. time, location and/or the position of the device during the sensing process). As a consequence, participatory sensing applications are vulnerable to *erroneous* and *malicious* participants. We define erroneous and malicious participants as those who mislead and disrupt the system measurements by reporting false, corrupted or fabricated contributions either intentionally or non-intentionally. Non-intentional (i.e. erroneous) corruption may originate from a malfunctioning sensor while intended (i.e. malicious) corruption is deliberately committed to alter the system measurements in a specific location. For instance, an adversary can put his device in a non-appropriate position. Alternatively, the participant can modify a contribution before sharing it. Malicious participants may further launch various types of attacks such as Sybil, collusion, on-off attack, etc. These attacks are discussed in Section 3. Consequently, the need arises for ap-

*Corresponding author:hayam910@gmail.com