USER PRIVACY AND DATATRUSTWORTHINESS INMOBILE CROWD SENSING

ABSTRACT

Smartphones and other trendy mobile wearable devices are rapidly becoming the dominant sensing, computing and communication devices in peoples’ daily lives. Mobile crowd sensing is an emerging technology based on the sensing and networking capabilities of such mobile wearable devices. MCS has shown great potential in improving peoples’ quality of life, including healthcare and transportation, and thus has found a wide range of novel applications. However, user privacy and data trustworthiness are two critical challenges faced by MCS. In this project, we introduce the architecture of MCS and discuss its unique characteristics and advantages over traditional wireless sensor networks, which result in inapplicability of most existing WSN security solutions. Furthermore, we summarize recent advances in these areas and suggest some future research directions.

INTRODUCTION

Since the introduction of Apple’s iPhone, mobile phones have evolved into smartphones. Supported by advances in mobile and wireless communication technologies such as third/fourth generation (3G/4G) and Wi-Fi, smartphones have better networking capabilities, allowing them to transmit data at higher rates. Moreover, they are equipped with more processing power and storage capacities. More important, they are programmable. A myriad of paid or free applications (often referred to as apps) are available to be downloaded in a convenient manner. Overall, this evolution makes mobile phones so powerful that many novel applications can be executed on them. Moreover, recently, devices equipped with
similar capabilities are emerging as wearable accessories (e.g., Google Glass and Galaxy Gear). All together, they are referred to as mobile wearable devices.

**EXISTING SYSTEM**

This imposes possible threats to user privacy because the collected data may disclose their locations and trajectories. Other possible privacy invasions include recording intimate discussions and capturing private scenes. Such threats would discourage people from becoming participants in MCS. Since altruistic data collection is a critical element of MCS, this issue of privacy invasion needs to be addressed immediately before the success of MCS is explored further. Another security issue of MCS is the reliability of the uploaded data. As data are reported by participants, they could possibly be falsified. Hence, this raises the issue of data trustworthiness. Furthermore, this issue inherently conflicts with the privacy issue. This is because if participants’ identities are not disclosed, those participants reporting falsified or even fabricated data cannot be identified and eliminated. In other words, if full anonymity is provided to MCS participants, guaranteeing the trustworthiness of reported data is difficult. Hence, data trustworthiness in MCS becomes more crucial than in traditional wireless sensor networks (WSNs), which deploy a large number of wireless sensor devices managed by the network owner.

In the remainder of this article, we first give an overview of MCS, and discuss its unique characteristics and advantages over traditional WSNs. Then we discuss how adversaries can invade user privacy and corrupt the reported data. Subsequently, we review some recent works that address these two issues, and suggest some future research directions.

**DRAWBACK OF EXISTING SYSTEM**

- Data may disclose their locations and trajectories.
- Recording intimate discussions and capturing private scenes.

Copyright © 2015 LeMeniz Infotech. All rights reserved
Do Your Projects With Domain Experts...

- Possible for data falsified.
- Fabricated data cannot be identified and eliminated.

Proposed System

MCS is an innovative computing paradigm that bears great potential and can lead to a wide range of novel applications relating to, for example, environmental monitoring, transportation, and entertainment. In this article, we have presented the advantages of MCS over traditional WSNs. At the same time, we have also identified two important challenges of MCS, user privacy and data trustworthiness. They are the two major barriers to the success and massive deployment of MCS systems. It is important to overcome these challenges in order to move this field forward.

ADVANTAGE OF PROPOSED SYSTEM

- Privacy and data trustworthiness.
- Reliability of the uploaded data.

Hardware Requirement

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech
- Ram: 512 Mb.
- MOBILE: ANDROID
Software Requirement

- Coding Language : Java 1.7
- Tool Kit : Android 2.3 ABOVE
- IDE : Eclipse