The Sybil Attack in Participatory Sensing: Detection and Analysis

Shih-Hao Chang[1], Kuo-Kun Tseng[2], and Shin-Ming Cheng[3]

[1] Department of Computer Science and Information Engineering,
Tamkang University, New Taipei City, Taiwan
sh.chang@ieee.org

[2] Department of Computer Science and Technology, Harbin Institute of Technology,
Shenzhen, China
kktseng@hitsz.edu.cn

[3] Department of Computer Science and Information Engineering,
National Taiwan University of Science and Technology,
Taipei City, Taiwan
smcheng@mail.ntust.edu.tw

Abstract. Participatory sensing is a revolutionary paradigm in which volunteers collect and share information from their local environment using mobile phones. Nevertheless, one of the most important issues and misgiving about participatory sensing applications is security. Different from other participatory sensing application challenges who consider user privacy and data trustworthiness, we consider network trustworthiness problem namely Sybil attacks in participatory sensing. Sybil attacks is a particularly harmful attack against participatory sensing application, where Sybil attacks focus on creating multiple online user identities called Sybil identities and try to achieve malicious results through these identities. In this paper, we proposed a Hybrid Trust Management (HTM) framework for detecting and analyze Sybil attacks in participatory sensing network. Our HTM was proposed for performing Sybil attack characteristic check and trustworthiness management system to verify coverage nodes in the participatory sensing. To verify the proposed framework, we are currently developing the proposed scheme on OMNeT++ network simulator in multiple scenarios to achieve Sybil identities detection in our simulation environment.

1 Introduction

In recent years, participatory sensing become a very popular and promising new technology to enable economically urban data sharing solution to a variety of application. Different from last century, the mobile phone of today, namely smartphone, have usually come with multiple embedded sensors, such as camera, microphone, GPS, accelerometer, digital compass and gyroscope. These technologies empowered smartphone users to collect data from their surrounding environment and upload them to an application server using existing communication infrastructure (e.g., 3G service or WiFi access points). Smartphones

J.-S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*,
Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_30, © Springer International Publishing Switzerland 2014

provide an excellent platform for participatory sensing application [1]. Hence, a requester of data can create tasks that uses the general public to capture geotagged images, videos, or audio snippets. Participants who have installed the client APPs on their smart phones can submit their data and get rewarded. For example, Panoramic 3-D photosynthesis of businesses and restaurants photos from Gigwalk has been collected by Microsoft Bing Map.

Participatory sensing provides a very openness which allows anyone to contribute data, however, also exposes the applications to malicious and erroneous attack. Security in participatory sensing is complicated by the data sharing nature and the lack of tamper-resistant mechanism. In addition, due to the broadcast nature of the participatory sensing, it is impractical to rendering public key cryptography in distributed network environment. Sharing sensed data tagged with spatial-temporal information could reveal a lot of personal information, such as user's identity, personal activities, political views, health status, etc., which poses threats to the participating users. Hence, an attacker can have many identities to act maliciously, by either stealing information or provide incorrect data in participatory sensing environment, namely Sybil Attack. The Sybil attack was first introduced by Microsoft researcher J. R. Douceur [6]. A Sybil attack relies on the fact that a participatory sensing network data server cannot ensure that each unknown data collecting element is a distinct, mobile phone. Therefore, any malicious participatory sensing network attack can try to inject false information into the network to confuse or even collapse the network applications.

In cloud computing , everything is treated as a service (i.e. XaaS), e.g. SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) and these services define a layered system structure for cloud computing. However, trust management is one of the most challenging issues in the emerging cloud computing. Although many approaches have been proposed recently for trust management in cloud environments, not much attention has been given to determining the credibility of trust feedbacks. To solve this problem, we propose a Hybrid Trust Management (HTM) framework for evaluating the trustworthiness of volunteer networks in participatory sensing applications. Our HTM framework allows a credit calculator associate with mobile devices that reflects the level of trust perceived over a period of time. A high credit score is an indication that a particular mobile device has been reporting reliable communication in the past. Moreover, in analyzing Sybil attacks data, we applied a fuzzy logic approach that can analyze detected Sybil attack features with these learning patterns in production time. To verify our idea, we utilizing OMNeT++ simulation to show its effectiveness against Sybil attacks.

The rest of this paper is organized as follows. Section 2 presents related works and summarized. Section 3 provides the detection factors to motivate the need for a reputation system in the context of participatory sensing and presents an overview of the system architecture respectively. In Section 4, we describe the experimental setup. Section 5 concludes the paper.