

SONATA: Social Network Assisted Trustworthiness Assurance in Smart City Crowdsensing

Burak Kantarci, Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA

Kevin G. Carr, Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA

Connor D. Pearsall, Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA

ABSTRACT

With the advent of mobile cloud computing paradigm, mobile social networks (MSNs) have become attractive tools to share, publish and analyze data regarding everyday behavior of mobile users. Besides revealing information about social interactions between individuals, MSNs can assist smart city applications through crowdsensing services. In presence of malicious users who aim at misinformation through manipulation of their sensing data, trustworthiness arises as a crucial issue for the users who receive service from smart city applications. In this paper, the authors propose a new crowdsensing framework, namely Social Network Assisted Trustworthiness Assurance (SONATA) which aims at maximizing crowdsensing platform utility and minimizing the manipulation probability through vote-based trustworthiness analysis in dynamic social network architecture. SONATA adopts existing Sybil detection techniques to identify malicious users who aim at misinformation/disinformation at the crowdsensing platform. The authors present performance evaluation of SONATA under various crowdsensing scenarios in a smart city setting. Performance results show that SONATA improves crowdsensing utility under light and moderate arrival rates of sensing task requests when less than 7% of the users are malicious whereas crowdsensing utility is significantly improved under all task arrival rates if the ratio of malicious users to the entire population is at least 7%. Furthermore, under each scenario, manipulation ratio is close to zero under SONATA while trustworthiness unaware recruitment of social network users leads to a manipulation probability of 2.5% which cannot be tolerated in critical smart city applications such as disaster management or public safety.

KEYWORDS

Cloud-Centric Internet of Things, Crowdsensing, Mobile Social Networks, Sensing-as-a-Service, Smart City

INTRODUCTION

The smart city concept denotes an intelligent platform consisting of interconnected sensors, embedded devices, decision making systems that process real time data (Chourabi, et al., 2012) (Meier & Lee, 2011) (Batty, 2014). Innovations in smart city design and applications can be accelerated by the integration of cloud computing into several smart city services such as transport, education, energy and water monitoring, healthcare, public safety and other ICT-based applications (Clohessy, Acton, & Morgan, 2014). A promising solution that would improve the benefits of smart city applications can be the integration of built-in sensors in mobile devices and providing the sensing resources as a service to particular smart city applications when needed (Kantarci & Mouftah, Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things, 2014). This concept is defined as Sensing as a Service (S²aaS) in the literature (Sheng, Xiao, Tang, & Xue, 2013). In S²aaS, distributed smart mobile devices participate in crowdsensing tasks that are requested by end users that are using either fixed computers or smart mobile devices. A comprehensive survey of S²aaS in the context of cloud-centric Internet of Things has been presented in (Kantarci & Mouftah, Sensing as a Service in Cloud-Centric Internet of Things Architecture, 2015).

Trustworthiness of crowdsensed data is a crucial challenge in S²aaS applications (French, Bessis, Maple, & Asimakopoulou, 2012). Kantarci and Mouftah have raised the trustworthiness issue in the recruitment process through user centric incentives (Kantarci & Mouftah, Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things, 2014). Trustworthiness of crowdsensed data has been improved by applying a user reputation system that uses statistical accuracy of the crowdsensed data per mobile device. This approach has later been improved by incorporating mobility-awareness (Kantarci & Mouftah, Mobility-aware trustworthy crowdsourcing in cloud-centric Internet of Things, 2014) and social interaction-awareness (Kantarci & Mouftah, Trustworthy crowdsourcing via mobile social networks, 2014). In order to address trustworthiness issue, there have been studies which take social ties into consideration, and some mobile devices are defined as social sensors denoting the trusted crowdsensing nodes (Hao, Mingjie, Geyong, & Yang, 2014). Furthermore, social trust and reciprocity have been combined to maximize the crowdsensing utility by modeling the problem as maximizing utility of a circulation flow (Gong, Chen, Zhang, & Poor, 2014).

As known by everyone, social networks have become inseparable part of every life (Dingli & Seychell, 2012). Related works point out mobile social networks as a smart ecosystem to harvest data from smart mobile devices in a participatory manner (Hu, Li, Ngai, Leung, & Kruchten, 2014). In (Sheng, Xiao, Tang, & Xue, 2013), integration of mobile social network into mobile S²aaS has been pointed as an important challenge. Mobile social network denotes a geo-social model that connects all users based on interests, location, context and interaction (Cardone, et al., 2013). Mobile social network-aware crowdsensing has been shown to improve the platform utility as mobile device trajectories can be estimated based on user interaction (Kantarci & Mouftah, Trustworthy crowdsourcing via mobile social networks, 2014). Research findings of the same study report that trustworthiness-aware recruitment of mobile devices is crucial since in presence of malicious activity, recruitment of mobile devices with high reputation can avoid degradation in crowdsensing utility due to the payments made to malicious users and manipulation probability in the harvested data. Incorporating social behavior and social trust dimensions into S²aaS by assigning social credits to users has been shown to improve the effectiveness of crowdsensing (Gong, Chen, Zhang, & Poor, 2014).

In this paper, we aim at addressing the trustworthiness challenge in smart city crowdsensing by combining social network theory and S²aaS. A minimalist illustration of the scenario is seen in Figure 1.a where crowdsensing for crisis management is depicted in the context of a smart city. The information is collected at the cloud platform, aggregated, analyzed and visualized for the end user. We adopt a Sybil detection approach (Yhang, Xue, Yang, Wang, & Dai, 2015) to detect the users who are in malicious activity. We propose Social Network-Assisted Trustworthiness Assurance (SONATA) as an effective and trustworthy recruitment framework for mobile devices sharing their built-in sensors

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/sonata/143903

Related Content

Integrating Production Automation Expert Knowledge Across Engineering Domains

Thomas Moser, Stefan Biffel, Wikan Danar Sunindyo and Dietmar Winkler (2013). *Development of Distributed Systems from Design to Application and Maintenance* (pp. 152-167).

www.irma-international.org/chapter/integrating-production-automation-expert-knowledge/72251

Grid Access Control Models and Architectures

Antonios Gouglidis and Ioannis Mavridis (2012). *Grid and Cloud Computing: Concepts, Methodologies, Tools and Applications* (pp. 349-365).

www.irma-international.org/chapter/grid-access-control-models-architectures/64491

Discovering Complex Relationships of Drugs over Distributed Knowledgebases

Juan Li, Ranjana Sharma and Yan Bai (2014). *International Journal of Distributed Systems and Technologies* (pp. 22-39).

www.irma-international.org/article/discovering-complex-relationships-of-drugs-over-distributed-knowledgebases/104762

Persistence and Communication State Transfer in an Asynchronous Pipe Mechanism

Philip Chan and David Abramson (2009). *International Journal of Grid and High Performance Computing* (pp. 18-36).

www.irma-international.org/article/persistence-communication-state-transfer-asynchronous/3968

Service Oriented Storage System Grid

Yuhui Deng, Frank Zhigang Wang and Na Helian (2009). *Handbook of Research on Grid Technologies and Utility Computing: Concepts for Managing Large-Scale Applications* (pp. 126-135).

www.irma-international.org/chapter/service-oriented-storage-system-grid/20515