Accepted Manuscript

Location and trajectory privacy preservation in 5G-Enabled vehicle social network services

Dan Liao, Hui Li, Gang Sun, Ming Zhang, Victor Chang

PII: S1084-8045(18)30039-0

DOI: 10.1016/j.jnca.2018.02.002

Reference: YJNCA 2061

To appear in: *Journal of Network and Computer Applications*

Received Date: 10 April 2017

Revised Date: 16 January 2018

Accepted Date: 2 February 2018

Please cite this article as: Liao, D., Li, H., Sun, G., Zhang, M., Chang, V., Location and trajectory privacy preservation in 5G-Enabled vehicle social network services, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.02.002.

Location and Trajectory Privacy Preservation in 5G-Enabled Vehicle Social Network Services

Dan Liao[1], Hui Li[1,2], Gang Sun[1,3], Ming Zhang[2], Victor Chang[4]

[1]Key Lab of Optical Fiber Sensing and Communications (Ministry of Education), University of Electronic Science and Technology of China, Chengdu, China
[2]Chendu Research Institute of UESTC, Chengdu, China
[3]Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu, China
[4]Xi'an Jiaotong Liverpool University, Suzhou, China

Abstract: 5G-based Vehicular Social Networks (VSNs) demand an advanced location and trajectory privacy preserving scheme for vehicles. Because VSNs present the characteristics of high mobility and multiple hop relays, we design a 5G-based VSN framework that incorporates Mobile Femtocell (MFemtocell) technology. Then, we propose the Dynamic Group Division algorithm (DGD), which is suitable for the dynamic properties of 5G and meets the real-time demands of VSN. To preserve privacy, the DGD algorithm increases the likelihood of exchanging pseudonyms via the proposed Group Generating Protocol and Pseudonym Exchanging Protocol. Then, we adopt the composite metric KDT (where *K* is the average anonymity set size, *D* is the average distance deviation, and *T* is the anonymity duration) and pseudonym entropy to quantify the degree of privacy. We evaluate and validate the effectiveness of our proposed algorithm based on the following three aspects: anonymity set size, distance deviation and pseudonym entropy. The simulation results show that our DGD algorithm better protects the location and trajectory privacy of VSNs while sustaining higher real-time demand than current approaches.

Key words: Location privacy; Trajectory privacy; 5G; Mobile Femtocell; VSN

1. INTRODUCTION

Vehicles now represent "the biggest mobile terminal" in the context of the Internet. The 5GAA committee (5G Automotive Alliance) has published research on the Internet of Cars in 2017 [1], and with the development of cloud computing [2-7] and big data [8-13], vehicles represent intelligent devices that can connect to the Internet and present sensing and computing abilities. Thus, vehicles are now the main carriers for mobile social networks. The Vehicular Social Network (VSN) has emerged, and vehicles can now be connected to wireless networks to improve traffic safety and promote the development of smart cars. However, the convenience of VSNs may lead to privacy concerns. The problem of privacy disclosure primarily stems from two aspects. First, for the users, certain data transmitted over the VSN are highly sensitive, such as location, trajectory, and identity information. If these sensitive data are revealed, the location privacy, trajectory privacy and identity privacy can be leaked [14]. Second, the topology of the VSN changes quickly because of the vehicle's high-speed mobility. Thus, data transmission exploits the multiple hop relay method. However, multiple hop relays are prone to data leakage risks, which may lead to the leakage of private information. Furthermore, people are paying increasing attention to their own privacy and data security [15-21]. Therefore, this paper addresses the problem of privacy leakage in VSNs. Combined with modern communication technology (5G), the method in this paper effectively protects the vehicles' location and trajectory privacy in the VSN.

With the increasing number of connected devices and demand for data rate, the 5G wireless communication system has been a popular research area in recent years [22-23]. The next 5G can serve all types of applications/systems with extremely high user rates anytime and anywhere [24]. As a Wireless Sensor Network (WSN), VSNs will inevitably lead to extraordinary developments with the application of 5G. Compared with other WSNs, VSNs realize the modern Intelligent Transport System (ITS). However, VSNs have inherent characteristics, such as high mobility and multiple hop relays. Thus, Mobile Femtocell (MFemtocell) has been introduced for 5G technology [25]. The use of MFemtocell can significantly maximize performance, such as by realizing dynamic linking, enhancing user throughput, and reducing response times and signal overhead [26-27].

To reduce traffic accidents, vehicles send safety message periodically. The safety message includes information about the location, speed and direction of the vehicles. Although the VSN can be plugged into the 5G network seamlessly, the 5G-based VSN does not consider privacy preservation. If a malicious attacker continuously eavesdrops on the safety message, the location and trajectory privacy may be leaked. To address this problem, researchers have proposed efficient schemes that include K-anonymity [28], Mix-zone [29], MixGroup [30], and Encryption [31-32]. The basic ideas behind these schemes are consistent. Each vehicle is assigned a pseudonym in the VSN, and then vehicles exchange the