Chapter 76
A Trust Based Secure and Privacy Aware Framework for Efficient Taxi and Car Sharing System

Oladayo Olakanmi
University of Ibadan, Ibadan, Nigeria

Sekoni Oluwaseun
University of Ibadan, Ibadan, Nigeria

ABSTRACT

This article describes how taxi service is an essential means of mobility in many cities. Recent findings show that average automobile owners utilize their vehicles for only 5% of its time in a day. Therefore, the advent of autonomous vehicles and car sharing will make it possible for owners to engage their vehicles as taxis when not in use by utilizing its 95% free time for income generation. Sensitive private information is required to be released during a taxi service delivery, which may bring certain security and privacy issues and challenges. This may hinder the prospect of using autonomous vehicles as a form of taxi. As a result of these, the authors propose a secure and privacy-preserving taxi service framework for car sharing, which ensures protection of car owner and passengers personal details, e.g. identity, location, destination, etc. The authors developed a decay-based trust model for a framework in order to monitor and improve the quality of service rendered to passengers by vehicles. The decay-based trust model was simulated on the framework. The simulation of the decay-based trust model shows that it is a perfect model for rewarding vehicles which render good quality of service and blacklisting vehicles with frequent poor service delivery.

DOI: 10.4018/978-1-7998-8954-0.ch076

1. INTRODUCTION

It is not a gainsaying that advent of autonomous vehicles would have notable impacts on the operation of car sharing and taxi services. Meanwhile, advent of autonomous vehicles does not imply that non-autonomous vehicles would suddenly be out of the transport system. It will take time before it fizzles out, therefore, a good car sharing or taxi system framework must be able to accommodate both vehicles. Apart from this kind of heterogeneity required in taxi system framework, sensitive information needs to be exchanged between passengers and drivers in case of non-autonomous or between passengers and vehicles in the case of autonomous vehicles. This brings security and privacy issues. Recent findings have shown that adversaries could intercept the requests of passengers in order to track the whereabouts of the vehicles as well as passengers (Liu, Au, Susilo, & Zhou, 2012) (Boukerche, Oliveira, Nakamura, & Loureiro, 2008) (Li, Dan, & Nahrstedt, 2015). Also, mischievous passenger or vehicle can collude with adversary to obtain the personal details of the other entities in the taxi system. In most of the taxi or car sharing systems, drivers do not know the destination of passengers before accepting their ride requests, thereby putting drivers at disadvantage position especially in a fixed price system. Example of taxi-service system with this kind of lapses is Uber; a popular taxi-service system which allows non-autonomous car sharing, it does not allow driver to know the destination before accepting the ride sharing request from passenger. Also, Uber's rating model is susceptible to bad mouthing attacks. Apart from this, almost all the existing taxi-service systems are non-autonomous vehicles based, that is, they do not accommodate AVs.

2. RELATED WORKS

Examples of the major works done on taxi systems can be seen in the work of Chim et al. (2013). They proposed a VANET-based secure taxi service framework where driver- passenger authentication is mandatory through a centralised trusted party. To preserve privacy, both driver and passenger make use of pseudonyms for all their transactions. Another related research effort is in Wei et al. (2012), where authors proposed a lightweight Prediction Based Greedy Routing (PBGR) protocol for taxi call system. This protocol works well in low node density areas. In the predicted protocol, the taxi and passenger locations are treated as nodes; passenger node is treated as the stationary node while the taxi node is the moving node. Their routing protocol predicts and updates the routing information and uses the greedy algorithm based on hop distance to find routes to destination quickly. The protocol adopts broadcast technique in which the passenger broadcasts his location and destination, and the vehicle is expected to reply within a particular time frame in order to minimise delay. However, the future position of the passenger and the taxi is predictable which makes them traceable for adversaries. Furthermore, due to the broadcast nature of the protocol, adversaries can easily launch their attacks. Also, authors in Ahmed et al. (2016), proposed the use of AVs as taxis through ride sharing. The ride matching mechanisms proposed in (Kleiner, Nebel, & Ziparo, 2011) and (Wang, 2013), made use of a control center as the determinant of the route plied by the taxis. In Lu et al., (2008), a conditional privacy preservation protocol for secure vehicular communication was proposed to solve the problem of the growing revocation list of blacklisted vehicles in VANET. Their protocol adopted a faster safety message verification scheme as the revocation list to reduce the required storage needed for storing revocation list, unlike the existing schemes which rely on the huge storage space in the onboard unit (OBU). However, a very large computational overhead is involved in