International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

PARKNET: A Parking Network with Payment Scheme

T. Veermani[1], V. Vignesh[2], D. Rajini Girinath[3], A. Mathan Gopi[4], S. P. Audline Beena[5]
[1,2]*UG Student, Dept. of Computer Science Engg., Sri Muthukumaran Institute of Technology, Chennai, India*
[3]*Professor, Dept. of Computer Science Engg., Sri Muthukumaran Institute of Technology, Chennai, India*
[4,5]*Assistant Professor, Dept. of Computer Science Engg., Sri Muthukumaran Institute of Tech., Chennai, India*

***Abstract*: Cruising for a vacant and economical parking spot causes not only time consuming and frustrating driving experiences, but fuel waste and air pollution. Public parking spots in crowded cities are scarce and expensive. Given this situation, it is imperative to call for a smart parking system that collects and provides private parking spots (e.g., around home or workplace) to ease public parking concerns. However, when the suppliers (drivers) are providing (querying for) parking spots, their privacy (e.g., location, identity) is inevitable to be disclosed and existing parking schemes cannot achieve anonymous authentication and anonymous payment simultaneously. To tackle these problems, we propose an anonymous smart parking and payment (PARKNET) scheme in vehicular networks. Specifically, we use short randomizable signature to provide anonymity and conditional privacy. We achieve quick result matching with hash map and anonymous payment with E-cash.**

***Keywords*: Vehicular networks, Smart parking, Security and privacy, Anonymous payment.**

1. Introduction

The parking in downtown areas has been a problem for years. Reports show that nearly 1.3 million out of 5.7 million motor vehicles regularly struggle to find parking places and by 2014 there were 2.9 million spaces were in need at night when Shanghai's 3 million registered car owners get off work. Meanwhile, a study shows that there are 30% of the traffic congestion is caused by the drivers who are cruising for parking spots. Another record shows that cars cruising for parking spots traveled 945, 000 extra miles, burned 47,000 gallons of gasoline and produced 728 tons of carbon dioxide in a Los Angeles district for over a year. The situation is getting even worse in developing countries where the number of vehicles has been increasing without sufficient investment in parking facilities. Some governments try to mitigate these problems through building extra parking lots, deploying road-side sensors, and establishing parking guidance systems. While the effect of such centralized approach is obvious and immediate, the limited construction space, expensive investment, and the consequent maintenance cost inhibit a widespread adoption. Therefore, the parking problem cannot be solved efficiently only through public infrastructure or management. Different from the traditional solutions, we have observed that a large proportion of parking spot is owned by the private sector and beyond the direct control of local transport authority. Such parking spots in private sector (e.g., residential space, workplace) always remain vacant when spot suppliers (we will use supplier for short) are on a trip or off duty. In addition, suppliers usually spend much money on buying and maintaining these private spots. Hence, they are willing to offer their parking spots for a parking fee as an economical compensation for their expenses. These motivate us to think how much time will be saved for cruising drivers and how much traffic congestion will be relieved and if the information of private parking spots can be initiatively provided by suppliers the public, especially the cruising drivers.

The recent increase in the development and use of smart phones has provided the opportunity to collaboratively sense and share information for the common good. Individuals with sensing, storing and computing devices are now able to collect and contribute valuable data (usually in a form of a report) to a server for different applications, such as finding parking spots. Therefore, we can utilize the people to help improve smart-parking with timely and accurate parking information.

However, security and privacy issues are preliminary concerns for users (including suppliers and drivers) participating in the data collecting and sharing task, since the system is faced with various cyber-attacks and the private information of users is put at risk. If the private parking spots are published online or a driver continues to upload information (e.g., current location, visit to a hospital, dinner list in a restaurant) without any security protection, the untrustworthy server or an adversary can infer sensitive information such as home/work address, health condition, insurance status, salary level, diet preference and even identity by analyzing transmitting messages along with background knowledge. If these issues cannot be well addressed, the system's functionality and durability will be endangered. To prevent illegal suppliers or drivers from submitting invalid messages to the server, registration is necessary for all entities which will be authenticated in each report and query to make sure that they are the registers. Data confidentiality and integrity are also important security issues. A supplier does not want the server or people nearby to learn the spot status by eavesdropping on the reports and a driver does not want the server or people

nearby to learn his cruising need for a parking spot. The messages sent to the server have to be signed to guarantee that they are not forged. Location privacy is another concern for users. Nevertheless, the server has to know a user' location in order to return the location related result. Therefore, we use cloaking to inhabit users' area with other locations and further satisfy anonymity constraint.

While providing private parking spots to unacquainted drivers, neighbors or colleagues of the parking spot supplier will have various concerns about the inconvenience or threat from an outsider who may have huge interest for their privacy. On the other hand, a maliciously behaved supplier may abuse the privacy preserving mechanism by providing inaccurate or others' parking spots to gain profits. These potential situations particularly happen when there is a dispute or accident. Therefore, we should provide anonymous authentication to protect users' privacy as well as traceability meaning a trusted authority can track a targeted supplier or driver. After the server has collected enough supplying reports, it should provide an accurate and quick service which in this case is the parking spot, to drivers. Here, we constructed a hashmap storing all parking locations with pertinent information and since we used binary tree in the hashmap, the average matching time is O (log2N um) which is the same for deleting and inserting time, where N um is the number of users.

Since the parking spot is private, supplier will charge a parking fee for using the private resource but anonymous authentication makes it difficult to complete the transaction. In summary, the key challenges are:

- We need to design a system to encourage the suppliers to willingly offer their parking spots to the public because different from public parking spots, private parking spots are hidden from the public;
- We need to protect the drivers' and suppliers' privacy because if these private parking spots as well as drivers' queries are published online without any protection, an adversary with background knowledge will acquire the suppliers' and drivers' privacy, such as home/work address, health condition, insurance status, salary level, diet preference and even identity;
- We need to achieve payment process after drivers finishing parking even when suppliers and drivers are anonymous to the server.

Existing public parking schemes do not work in our scenario for several reasons:

- They do not possess the functionality to utilize private parking spots;
- They cannot enable spot suppliers to have requirements for vehicles to be parked in their spots, such as the parking duration and the size of the vehicle;
- They cannot enable drivers to have preferences for private parking spots, such as location and price.

2. Related work

Existing work has been focusing on parking or parking related problem in VANET, on-street parking and navigation. Lu et al. proposed a secure navigation scheme SPARK to provide drivers with accurate and convenient parking services in large parking lots, including real-time parking navigation service, intelligent antitheft protection, and friendly parking information dissemination. Lu et al. presented a new intelligent and secure privacy-preserving parking scheme by employing parking lot RSUs to manage the whole parking lot. ParkNet is a system that estimates street parking availability by using vehicles equipped with a GPS receiver and a passenger-side-facing ultrasonic rangefinder. The data is then aggregated at central server, building a real-time map of parking availability and providing this information to drivers in search of parking. Park sense is another system that leverages the ubiquity of Wi-Fi beacons to monitor on street parking availability. It utilizes a robust Wi-Fi signature matching approach to detect a driver's return to the parked vehicle and it uses a novel approach based on the rate of change of Wi-Fi beacons to sense if the user has started driving.

3. System model

A. *System model*

The system model mainly consists of four entities: trusted authority, server, driver, and supplier, as shown in Fig. 1. The key notations are listed in Table 1.

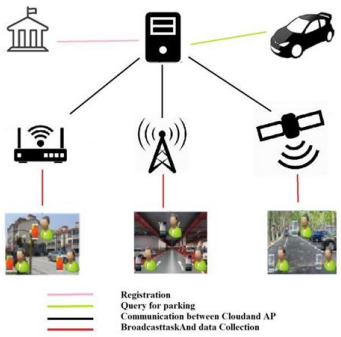

Fig. 1. System model

Trust Authority (TA) is a powerful entity whose responsibility is initializing the whole system which includes registering drivers and suppliers, generating public parameters, and distributing keys. TA will be offline unless a dispute arises where it can trace a targeted user's identities. Server receives the supplying reports from suppliers and parking queries from drivers, then it searches the database and returns matching results to drivers. The server generates electric coupons to complete anonymous payment and help suppliers verify the validity of coupons. Supplier is willing to contribute her private parking spot to the driver and she will charge the driver a certain amount of parking fee for the extra parking resources. We denote both supplier and driver as "user" in this paper. Driver

cruises around to find a parking spot in a public parking lot or waits for a private parking spot for which he is willing to pay a parking fee.

B. Thread model

The trusted authority is fully trusted and will not be breached by any adversary. We assume that drivers, suppliers, and the server are honest-but curious, meaning that they will strictly follow the predesigned scheme, but may also try to pry into others' privacy from available information. location to a supplier, links a location to a driver, and links one user's different messages. Supplier may try to obtain the identities of drivers who park in her spot. She may also report inaccurate parking spot information to collect an extra parking fee. We note that if the identity and supplying report of a supplier are not protected, then her neighbors will know the status of this spot and the supplier (whether she is home or not) which leads to a serious privacy violation. Similarly, the drivers can find out which drivers around her are querying for a parking spot. We do not consider the physical attack from recording users and their behaviors with private cameras which are not obfuscated because anyone with a smartphone can take a picture anytime and anywhere without being detected and it cannot be prevented. Driver may try to obtain the identities of suppliers, park in other drivers' matched parking spots, refuse to pay a negotiated parking fee, or damage a parking spot on purpose.

C. Design objectives

- *User Authentication:* A user should be authenticated before sending a supplying report/parking query, such that no adversary can impersonate a legal user.
- *User Privacy:* Users' identities are protected from the server, other users and external adversaries. Users' locations are protected from the server, other users and external adversaries, except the matched user. Given two supplying reports/parking queries from one user, no one can link them to the same user.
- *Data Confidentiality and Integrity:* The contents of sup-plying reports and protected from the server, other users and external adversaries. All accepted messages should be transmitted without being altered.
- *Traceability:* TA can trace the real identity of a misbehaved user in case a dispute happens.
- *Anonymous payment:* The driver's real identity is not disclosed when paying coupons to a supplier and the supplier's real identity is not disclosed when verifying the coupons with the help of the server and cashing coupons at the server. In addition, unlink ability must be protected, meaning any user's coupons cannot be linked together.
- *Quick result retrieval:* After storing enough information about private parking spots from different suppliers and parking queries from drivers, the server should efficiently match parking queries with supplying reports.

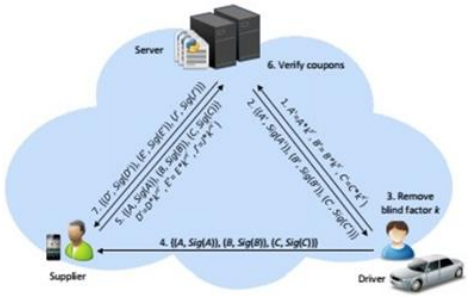

Fig. 2. Anonymous payment

4. Discussion

- *Supplier motivation:* In a typical data collecting and sharing platform, the workers or reporters have incentives to participate because they will get rewards from the system man-ager for valid contributions. In PARKNET, suppliers earn parking fees which is the incentive by providing private parking spots. Therefore, in order to recruit more suppliers, the system can provide extra benefits (e. g., gas coupons) to suppliers and the drivers can behave according to the negotiation result such that the system will enter a healthy circulation and assist society in trust establishment. In addition, if more than one spots are available for one driver, the suppliers can compete to be selected by the driver according to a bidding system.
- *Combining techniques:* It is difficult to combine the techniques in PARKNET. Imagine that when the system attempts to achieve payment process between suppliers and drivers, an intuitive method is that drivers pay by e-cash. A digital signature can be added to protect the integrity of the e-cash. However, when a driver buys an e-cash with his credit card or debit card, his real identity is exposed at the same time. The privacy cannot be preserved because the system can record the card number and the e-cash ID in its database. Another alternative method is to use anonymous payment technology. However, if we use anonymous payment such as Bit coin and TOR, there will be disadvantages: for the Bit coin approach, the suppliers and drivers have to register a Bit coin account in the first place; the driver must wait for at least 1 hour (6 blocks) to be found in order to gain high confidence that the transaction with a driver is actually acknowledged in the network. Therefore, it is not practicable for the supplier to actually receive the payment. For the TOR approach, it will raise more communication overhead since layers of encryption and decryption are required in transmission.
- *Securing parking spots:* One supplier's renting out neighbor's parking spots be prevented by using a remote control ground parking lock. Only after the

supplier agrees to lend her paring spot to a driver, she will unlock the parking lock for the driver, or tells the driver how to unlock it. Furthermore, this behavior will incur legal sanction because private parking spots are personal property as well.

- *Other considerations:* If a driver does not pay the parking fee, the supplier can file a complaint to the TA, if the driver cannot provide the payment proof received from the supplier, the TA deems the driver as a violator, recovers his real identity, and inserts the driver into a blacklist. The parking duration time can be calculated by a camera at the private area entrance/exit gate. There are two types of cameras: ones installed by the government and ones installed by residents. For the first type, we trust the administrative personnel which has professional ethics and their regular monitoring through cameras is not considered as a privacy violation to the residents (PARKNET users) whether the cameras are obfuscated. Even if someone misuses the camera and violates users' privacy, he/she will be punished by the law. Meanwhile, some cameras only aim at detecting certain users, such as the roadside cameras only take pictures of over speeding vehicles. For the second type, the cameras which are obfuscated can be used in PARKNET, since the face and plate number will not be clearly recorded; we do not consider the physical attack from cameras which are not obfuscated because anyone with a smartphone can take a picture anytime and anywhere without being detected and it cannot be prevented. Meanwhile, not all private parking spots have a secret camera.

5. Conclusion

In this paper, we proposed PARKNET to enable the cruising driver to find a parking spot and supplier to make a profit from providing private parking resources. The parking spots are better utilized and traffic congestion is further reduced. A supplier and driver can anonymously send a supplying report and a parking query to the server. Meanwhile, a trusted authority is able to disclose a user's identity if a dispute occurs and users achieve anonymous payment with E-cash. Our scheme also supports finding public parking spot which only needs to add a counting item in the hash map. For the future work, first, we will consider detecting location attack from drivers in advance, meaning a driver may send a parking query to the server long he arrives at the destination area, and the system should be able to filter out this query and guarantee system fairness since other drivers in this areas now need parking spots more. Second, we will design a privacy preserving smart-parking and payment scheme based on fog computing to achieve a more efficient, smart parking and payment scheme for suppliers and drivers. In this way, the suppliers and drivers will be matched locally by fog nodes, and the reports and queries will not be uploaded to a remote server, such that the response time, network bandwidth and public traffic congestion caused by cruising vehicles will be further reduced.

References

[1] S. Mathur, T. Jin, N. Kasturirangan, J. Chandrashekharan, W. Z. Xue, M. Gruteser, and W. Trappe, "Drive-by sensing of road-side parking statistics," Proc. ACM Mobi. Sys, 2010, pp. 123-136

[2] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," IEEE

[3] M. Mahmoud, K. Rabieh, A. Sherif, E. Oriero, M. Ismail, E. Serpedin, and K. Qaraqe, "Privacy preserving fine-grained data retrieval schemes for mobile social networks," IEEE Trans. Dependable and Secure Computing, no. 99, 2017.

[4] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," Proc. IEEE INFOCOM, 2008, pp. 1903-1911.

[5] K. Wei, A. J. Smith, Y. F. R. Chen, and B. Vo, "WhoPay: A scalable and anonymous payment system for peer-to-peer environments," Proc. IEEE ICDCS, 2006, pp. 1-10.

[6] S. Rahaman, L. Cheng, D. F. Yao, H. Li, and J. -M. Park, "Provably secure anonymous-yet-accountable crowd sensing with Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772- 2784, 2010. scalable sublinear revocation," Proc. Privacy Enhancing Technologies, vol. 2017, iss. 4, 2017, pp: 384-403.

[7] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR: Security & privacy-preserving architecture for participatory-sensing applications," Proc. ACM Wi Sec, 2014, pp. 39-50.