Vehicle Theft Identification RIFD Based Vehicle ID Detection in a Wireless Charging Applications

Basit Sayeed Qadri[1], Faiq Basu[2], N. Priya[3]

[1, 2]Department of Computer Science and Engineering, Bharath University Chennai-600073, India

[3]Assistant Professor, Department of Computer Science, Bharath University Chennai-600073

Abstract: ***There is not any suitable payment system for the electric rechargeable automobiles. Additionally there is not any effective system to track the theft vehicles; still police's job of finding the lost vehicle is very difficult. The electric chargeable vehicle will be monitored by the server if the vehicle will be stolen. The owner will give the request to the server when the stolen vehicle get charged it will send request to the police station and send alert to the vehicle owner. Stolen Request is given via Android Application or through System to the Server. We also include Wireless Power Transmission (WPT) in this Project to charge the Vehicle. We use RFID for Vehicle Number Authentication.***

Keywords: Location Privacy, Electric Vehicles, RIFD, Wireless power transmission.

1. Introduction

An electric vehicle (EV) is a vehicle that does not rely on gasoline or liquefied petroleum gas as fuel but only uses electricity stored inside the battery of car as the source of kinetic energy; hence, it offers emission-free urban transportation. It uses an electric motor as an alternative of a gasoline engine to get started. Its battery can be simply recharged by the shared domestic electricity for standard charging (slow charging) or by the explicitly designed charging station for fast charging. There are many benefits of using electric vehicles. For example, EVs do not produce toxic tailpipe contaminants from the on-board source of power at the point of operation (zero tailpipe emissions). If renewable energy (such as solar or hydroelectricity) is used, the EV becomes a renewable form of transportation. Future EVs may support a vehicle-to-grid (V2G) system. This idea lets vehicles to provide power (vend electricity) to the grid. This can be achieved if an EV is equipped with a solar panel and is parked outside in sunshine. In this way, the EV can help to balance loads by "valley filling" (charging at night when the need is little) and "peak shaving" (transmitting power back to the grid when the demand is high). It can enable utilizing different means to offer regulation services (keeping voltage and frequency constant) and spinning reserves (meeting un expected demands for power). In the U.S., EVs have started to become popular due to the advantages that it can offer. On average, fuelling a gasoline-based car will cost roughly three times extra than fuelling it with electricity, i.e., in the case of EVs. In addition to saving money, EVs also offer significant environmental benefits, which makes the adoption of EVs very attractive. Regardless of their potential advantages, extensive adoption of EVs faces numerous difficulties and restrictions limitations. One of themain glitches is the driving limit. Most EVs can go only about 100 to 150 km before recharging, whereas gasoline vehicles can go over 500 km before refuelling. This may be sufficient for city trips or other short hauls. Nevertheless, individuals can be apprehensive that they would run off of energy from their battery prior to reaching their terminus, which is a concern known as the range anxiety. One of the explanations is to set up more fast-charging stations with high-speed charging capability so that customers could recharge the 100-km battery of their electric vehicles up to 80% in about 30 min. EV drivers may then charge their automobiles at their homes, offices, shopping malls, or car parks outside restaurants while they are having dinner. Location privacy concern: Theamenity of charging EVs at the drivers' ease also comes with few drawbacks. In practice, EVs need to travel at a certain time between two charging stations. As stated previously, since the distance is relatively much shorter compared with gasoline-based cars, this will lead to some issues that are related to location privacy [1]. These locations include the drivers' homes, places of employment, places of amusement places where they usually go, etc. Leaking privacy will directly produce negative impacts [2], [3], [4], such as location-based "spam," which means that the location information could be used by malicious businesses to strike down an person with unsought promotion for products or services related to the location of that individual.

Additional undesirable result is that the location can be used to deduce an individual's radical views, state of health, or personal partialities. Furthermore, the disclosure of location privacy may also result in safety problems. For example, it may be used by unprincipled people, such as robbers, for stalking or corporeal attacks. Therefore, location privacy issues must be carefully addressed before EVs can be adopted everywhere in practice. It is interesting to note that this location privacy problem does not exist in gasoline cars. Gasoline cars will not require to be refilled within a short distance; therefore simply tracking the distance between the last gas station and the next gas station will reveal no useful information. In practice, drivers may need to refill the gasoline once a week. There will be many activities within that week that will be untraceable. When drivers pay for the gasoline in the gas station using a credit card, then this information will be known. Nevertheless, many drivers still choose to pay with cash, which is imperceptible. Furthermore, even credit card payment will not disclose excessive information since the gasoline refilling events will not be very recurrent, and as highlighted earlier, the activities after the car has been refilled will remain unknown. This is in contrast to EVs. Moreover, since EVs can support vehicle to grid charging, the location of the last refill can even be easily noted. Revocation of location privacy at the "right" time: It is clear that EVs require protection against location privacy.

2. Existing Payment Systems

There are many different forms of existing payment systems. We examine some of the most practical forms and explain why they are not suitable for EVs.

1) **Paper cash:** Unlike gas stations, charging stations for EVs are all machine operated. Ifthey allow cash payment, the installation costs will be very high due to the high security requirement of cash machines [similar to those for automatic teller machines (ATMs)]. Note that, currently, there are many ticketing machinesset up in car parks or automatic selling machines (e.g., selling soft drinks), which can take paper cash or coins. However, as the cost for car park or soft drinks is far less than charging EVs, the physical security prerequisite can be considerable lower. Thus, even though paper cash can offer anonymity, the high installation and running cost are the main obstacles that are disfavoured by suppliers to adopt. Paper cash as a kind of a payment system in the charging station.

2) E-cash: Alternatively, e-cash [5], [6], [7], [8], [9] is the form of electronic paper cash, which also provides privacy. However, e-cash is mainly used in small amount Transactions (e.g., a few dollars) instead of large amount transactions (e.g., a few hundred dollars) due to security and efficiency concerns. To support two-way payments, transferable e-cash [10], [11], [12] is needed, and it has been shown that the complexity of transferable e-cash linearly grows in the number of transfers that are supported [22]. Apart from that, offline e-cash cannot provide double-spending prevention. It can only perceive doubleoutlay and reveal the identity of the doublepayer when the electronic coins are credited back to the bank. If a corrupt user double-spends several times before going bankrupt, the double-crossed shops cannot get back the money that they deserved to have. Furthermore, different from credit cards, e-cash does not provide lost protection. No one will put a few thousand or even a few hundred dollars in the e-wallet. Thus, e-cash is only suitable for small-amount transactions. Charging for an EV does not definitely belong to the small-amount transaction category.

3) Micropayment: Micropayment [13], [14], [15], [16], [17] is another form of an electronic payment system. Compared with e-cash, it is usually more efficient. However, there are some trade-offs for the advantage of efficiency. The security of micropayment may not be as strong as e-cash. Some of them may require trusted hardware. In addition, privacy is sometimes not considered an essential requirement in a micropayment system. Thus, it is only suitable for payment with a small amount.

4) Prepaid cash card or cash coupon: Prepaid cash card or cash coupon (e.g., EZ link in Singapore [18], Octopus in Hong Kong [19], and Oyster in London [20]) is another common way of anonymous e-payment. However, similar to e-cash, it does not support lost protection. Executing a large-amount transaction may bring inconvenience to user, i.e., they may neither want to bring many coupons together nor buy the coupons or top up every day. In addition, it also does not fully support two-way transactions, which is a necessary requirement for the future V2G system.

5) PayPal: PayPal [21] is a kind of the most commonly used electronic prepayment system. However, it requires a third party (the PayPal Company). If the authority colludes with the PayPal company (e.g., by telling the PayPal company the exact time and location of a particular transaction), the user can be traced. Thus, we regard PayPal providing partial location privacy only.

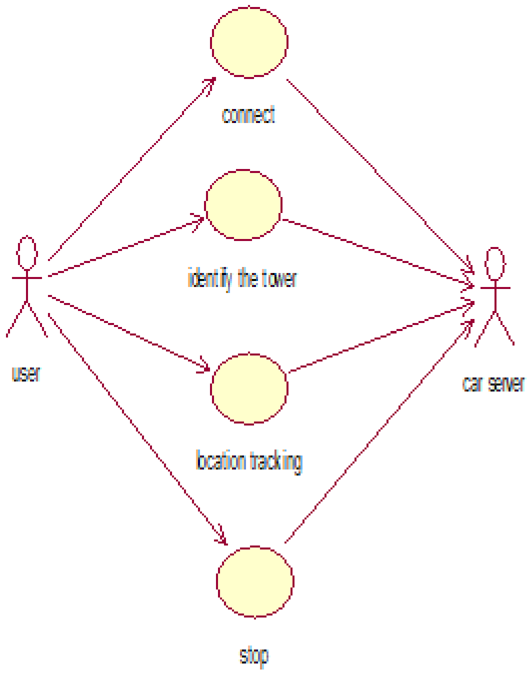
3. Existing System

There is no proper payment system for the electric chargeable vehicles. Also there is no very effective system to track the stolen vehicles; still police job is finding the lost vehicle is very difficult.

4. Proposed System

The electric chargeable vehicle will be monitored by the server if the vehicle will be stolen. The owner will give the request to the server when the stolen vehicle get charged it will send request to the police station and send alert to the vehicle owner.

Modification of the Project is Stolen Request is given via Android Application or through System to the Serve. We also include Wireless Power Transmission (WPT) in this Project to charge the Vehicle. We use RFID for Vehicle Number Authentication.



5. Modules

1) Android Deployment
2) Stolen Server

3) RFID Authentication
4) Wireless Power Transfer Embedded Hardware Fabrication
5) Vehicle Tracking

Android Deployment or Java deployment

Mobile Client is an Android application which created and installed in the User's Android Mobile Phone. So that we can perform the activities. The Application First Page Consist of the User registration Process. We'll create the User Login Page by Button with Text Field Class in the Android. While creating the Android Application, we have to design the page by dragging the tools like Button, Text field, and Radio Button. Once we designed the page we have to write the codes for each. Once we create the full mobile application, it will generated as Android Platform Kit (APK) file. This APK file will be installed in the User's Mobile Phone an Application. We can also use the java terminal to create the registration page for submitting the vehicle theft request to the server.

Stolen Server:

A server is a computer program operating to assist therequirements of other programs, the "clients". Thus, the "server" is used to perform some computational assignment on behalf of "clients". The clients bothrun on the same system or connect through the network.

Here the server will store all the user's information in the database. In the server, the detection sensors are connected, so that they can control the vehicles. Also the server will monitor all the user access. The server will also store the user access details in the database.

RFID Authentication:

The user reader enquiries tags by disseminating an RF signal, and the tag reacts to the reader with a vehicle number or other identifying information. The reader forwards the tag response to a back-end server. The server has a database of tags and can retrieve detailed information regarding the tag (or the item attached to the tag) from the tag response. If the tag doesn't match then user invalid user

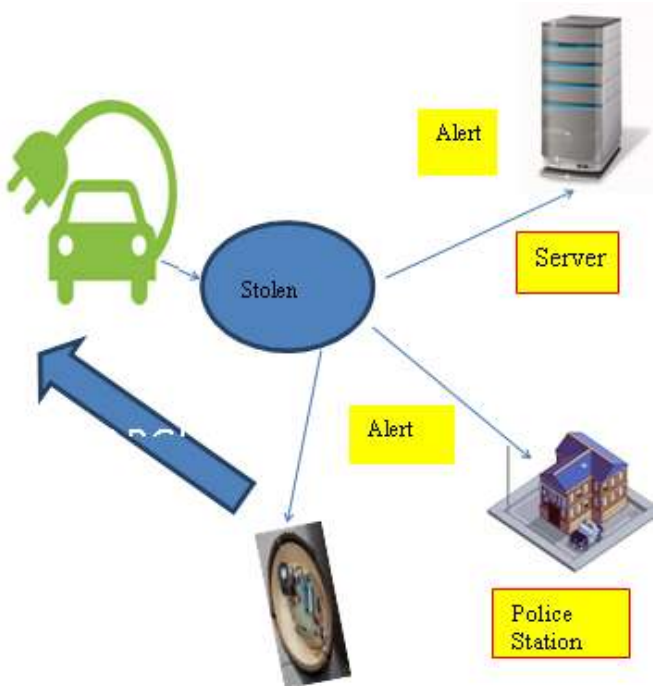
Wireless Power Transfer Embedded Hardware Fabrication

In this module we implemented a technique of Wireless power transmission; it is used to charge the vehicles. That is, the power transmitting unit has visibility of the car for certain meters and can charge the on-board energy storage unit for amount of seconds. The amount of energy that can be transferred via wireless power transmission. Fee status, Paid through the RFID tag

Vehicle Tracking

Radio frequency identification is a wireless technology that uses radio signals to track the vehicle. RFID system is RFID tags, RFID readers and a back-end server. A tag is an identification apparatus attached to an item, which uses radio frequency (RF) to communicate to server. If the user gives Stolen request is given via Android Application or through system to the server. In such conditions ,when the stolen vehicle try to get charged it will send request to the police station and send alert to the vehicle owner

6. System Architecture



7. Conclusion

In this paper, we have presented a mechanism to enhance location privacy for EVs. Our proposed solution provides an anonymous payment system with privacy protection support. In the case where traceability is required, such as when the EV is stolen, this feature is also provided by sending the stolen vehicle request to the server through the system or smartphone. Hence, our solution provides location privacy enhancement at the right time, which will make the adoption of EVs practical. It can also trace a user for all his previous and future transactions while keeping the transactions from other users unopened. We also note that the scheme described in this paper is specifically designed for EVs. However, we do not eliminate the possibility to apply our scheme (or modified version) in other environments whenever it is deemed suitable.

References

[1] M. Chia, S. Krishnan, and J. Zhou, "Challenges and opportunities in infrastructure support for electric vehicles and smart grid in a dense urban environment," in Proc. IEEE Int. Elect. Veh. Conf., 2012,pp. 1–6.

[2] I. Bilogrevic, M. Jadliwala, K. Kalkan, J.-P. Hubaux, and I. Aad, "Privacy in mobile computing for location-sharing-based services," in Proc. PETS, vol. 6794, Lecture Notes in Computer Science, 2011, pp. 77–96.

[3] M. Duckham, "Moving forward: Location privacy and location awareness," in Proc. SPRINGL, 2010, pp. 1–3.

[4] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the privacy risk of location-based services," in Proc. Financial Cryptogr., vol. 7035, Lecture Notes in Computer Science, 2012, pp. 31–46.

[5] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in Proc. CRYPTO, vol. 403, Lecture Notes in Computer Science, 1988, pp. 319–327.

[6] A. die Solages and J. Traoré, "An efficient fair off-line electronic cash system with extensions to checks and wallets with observers," in Proc. Financial Cryptogr., vol. 1465, Lecture Notes in Computer Science, 1998, pp. 275–295.

[7] C.-I. Fan and V. S.-M. Huang, "Provably secure integrated on/off-line electronic cash for flexible and efficient payment," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 40, no. 5, pp. 567–579, Sep. 2010.

[8] T. Okamoto, "An efficient divisible electronic cash scheme," in Proc. CRYPTO, vol. 963, Lecture Notes in Computer Science, 1995, pp. 438–451.

[9] T. Okamoto and K. Ohta, "Universal electronic cash," in Proc. CRYPTO, vol. 576, Lecture Notes in Computer Science, 1992, pp. 324–337.

[10] R. S. Anand and C. E. V. Madhavan, "An online, transferable E-cash payment system," in Proc. INDOCRYPT, vol. 1977, Lecture Notes in Computer Science, 2000, pp. 93–103.

[11] S. Canard, A. Gouget, and J. Traoré, "Improvement of efficiency in (unconditional) Anonymous transferable e-cash," in Proc. Financial Cryptogr., vol. 5143, Lecture Notes in Computer Science, 2008, pp. 202–214.

[12] I. R. Jeong, D. H. Lee, and J. I. Lim, "Efficient transferable cash with group signatures," in Proc. ISC, vol. 2200, Lecture Notes in Computer Science, 2001, pp. 462–474.

[13] S. N. Foley, "Using trust management to support transferable hash-based micropayments," in Proc. Financial Cryptogr., vol. 2742, Lecture Notes in Computer Science, 2003, pp. 1–14.

[14] S. Jarecki and A. M. Odlyzko, "An efficient micropayment system based on probabilistic polling," in Proc. Financial Cryptogr., vol. 1318, Lecture Notes in Computer Science, 1997, pp. 173–192.

[15] M. Lesk, "Micropayments: An idea whose time has passed twice?" IEEE Security Privacy, vol. 2, no. 1, pp. 61–63, Jan./Feb. 2004.

[16] R. J. Lipton and R. Ostrovsky, "Micropayments via efficient coinflipping,"in Proc. Financial Cryptogr., vol. 1465, Lecture Notes in Computer Science, 1998, pp. 1–15.

[17] S.-M. Yen, K.-Z. Chiou, J. Zhang, and P.-H. Lee, "A new peer-to-peer micropayment protocol based on transferable debt token," in Transactions on Computational Science X. New York, NY, USA: Springer-Verlag, 2010, pp. 352–363.

[18] EZ-link. [Online]. Available: http://www.ezlink.com.sg

[19] Octopus Hong Kong. [Online]. Available: http://www.octopus.com.hk

[20] Oyster online. [Online]. Available: https://oyster.tfl.gov.uk/oyster/entry.do

[21] Send Mondy, Pay Online and Merchant Accounts. [Online].