Structure Free Highway Toll Collection Using Non-Repudiated Tickets

Nol Premasathian[a] and Somying Thainimit[b]

[a]*Department of Mathematics, King Mongkut's University of Technology Thonburi, Bangkok 10140, Thailand*

[b]*Department of Electrical Engineering, Kasetsart University, Bangkok 10900, Thailand*

Abstract

This paper proposes a concept of how to collect toll on highways. Unlike any existing method, the proposed approach requires no structure to be built on highways for the toll collection purpose and drivers are not required to stop or even slow down to pay toll. Toll must be prepaid in advance and a driver must keep a toll ticket as proof of payment. We apply public key cryptographic operations to the ticket issuing system to prevent forgery as well as repudiation from the seller. This paper explains the mechanism of the system: the details of toll tickets issuance, the detection and penalization of drivers without a toll ticket, the prevention of toll ticket reproduction by involved parties, and the detection of an agent selling toll ticket for his own benefit.

1. Introduction

Poor highway condition, especially poor surfaces, causes automobile tires and other components to wear out faster and there is increased fuel consumption on account of traffic congestion [5]. To keep highways in good condition, the government needs fund, which can be obtained from the tax payer money and/or from toll collection. Using money from tax alone is not a justifiable solution since people use highways at different capacities. Vehicle tolling is a more logical way to finance transportation maintenance system since only people who use toll-way pay for its upkeep and improvement. Collecting toll using man-operated toll booth not only cause traffic delay [2] but also affect the health of the booth attendants [7]. There are other methods to collect toll without using human. In many cases there are both electronic toll booths and man-operated toll booths with the attempt to optimize the toll collection systems [3]. An example of electronic toll booth is FasTrak [1], which requires drivers to have a transponder installed on the windshield inside their cars. When passing through the designated lane, an overhead antenna reads the transponder and automatically deducts the appropriate toll from the prepaid account. The car doesn't have to stop but cannot move faster than 25 miles per hour. Raytheon, a more advanced technique allows cars to pass at speed exceeding 100 miles per hour [4]. Vehicle without transponders are spied by digital license plate cameras that photograph the rear license plates and send the information to a computerized data center for revenue management and billing through the mail.

All techniques mentioned above require permanent structures to be constructed on highways. The number of structures depends on the method of toll calculation and is normally proportional to the length of highways, the number of entrances and the number of exits if toll is calculated from the distance traveled on highways. Roads must be expanded to accommodate the toll booths or the electronic toll collecting lanes. All of these must be maintained with expenses. For this reason, we

propose a new system that requires no structure or road expansion. The new system also allows flexible toll pricing structure.

Our ticketing system is first described in the following section. Detail of generating a non-repudiated ticket is explained in section 3. The highway monitoring system is discussed in section 4 and some conclusions are drawn in section 5.

2. Ticketing System

To eliminate the traffic congestion due to toll collection and enhance drivers' convenience, we propose a prepaid ticketing system. Drivers should obtain a ticket that will authorize them to use a particular portion of highways. Tickets can be purchased from a convenient place, such as post offices, banks, convenient stores, ATM machines or even from the internet. Drivers must give the license plate number of their vehicles and specify the date and a portion of highways on which they intend to drive. This allows a fair toll pricing system because drivers pay for only the portion of highways on which they will drive. Since processing fee must be paid to vendors, this overhead can be reduced if drivers buy a ticket that is valid for several days at the same time. Drivers can obtain a weekly, a monthly or a yearly pass that will allow them to drive on highways for one week, one month or one year respectively. The system is capable of issuing a pass tailored to the requirement of any driver; for example, a driver may need a pass that is valid on Monday morning and Friday evening excluding non-holiday. Besides issuing tickets, vendors are required to daily report the sales to the central unit, which is responsible for collecting tolls. The central unit therefore has a list of vehicles allowed to use highways on each day. The list is not up to date since a driver may purchase a ticket and drive on the same day. This problem will be mentioned in a later section.

3. Non-Repudiated Ticket

As mentioned above, drivers are required to purchase a ticket from vendors prior to the journey. Ticket forgery is a major concern in any ticketing system and causes revenue loss. Only authorized vendors should be the only parties that can issue tickets. Using special paper for ticket printing is costly and involves some serious problems. Tickets of different prices must be printed on different papers, or vendors can sell high-priced tickets and claim to have sold lower-priced ones. Second, a vendor can print the name of another vendor on tickets and keep the money for himself. Third, the special paper can be lost or stolen. To eliminate all of these problems, we introduce the use of the Non-Repudiated Ticket, which is produced using some public key cryptographic operation [6]. The procedure is as follows.

1. The central unit publishes its public key.

2. The central unit sends its private key to the vendors.

3. Each vendor publishes their public key.

4. When a driver wants to purchase a ticket, the vendor acquires from him information about the vehicle type, the license plate number, the entrance

and exit of the highway on which he will drive, the type of the ticket (single day, several days, etc.), and the starting date. The information is combined with the vendor's name, arranged in a specific format, encrypted using the vendor's private key and encrypted again using the private key of the central unit.

5. The vendor prints the ticket, which includes the information in step 4 as well as the encrypted ciphertext.

Since the encryption is performed first with the vendor's private key, if RSA encryption is used, n in the vendor's private key must always be smaller than the n of the key of the central unit. Tickets can be printed on ordinary papers and can be reprinted if lost or stolen. A stolen ticket cannot be used unless the vehicle corresponding with the ticket is also stolen. Tickets can even be printed by drivers, which is convenient especially when purchasing is made on the internet.

The double keys encryption and decryption is introduced into our system to verify the authenticity of purchasing and selling, and to validate the tolls. Vendors who issue tickets cannot deny that a ticket was not sold by them since it is encrypted with the vendor's private key. Drivers can verify the validity of tickets since both the central unit's public key and the vendor's public key are made public. To heighten security, key can also be changed regularly. The central unit may use different keys on tickets starting on different days and publish all keys in advance.

At the end of each day, vendors must report all sales, which include the information of the ticket and the corresponding encrypted ciphertext as proof of sale. Failure to make such report may cause the vendor a hefty fine if an unreported ticket is used and inspected by an inspector, which will be explained in a later section.

Sales can be reported as batch transactions or can be updated online when a sale is made and will affect the monitoring system. Selecting the type of transaction depends on the communication cost and/or any other relating factor. Batch or online transactions can be made through insecure channel such as telephone line or the internet. A message containing the number of transactions encrypted with the vendor's private key and the central unit's public key must be sent along. No one can add a false transaction since the central unit knows number of transactions. A transaction cannot be substituted since the hacker cannot produce the ciphertext that corresponds with the information of the transaction. If a transaction is lost, intentionally deleted or modified during the transmission, it can be detected for the same reasons. Note that the message containing the number of transactions cannot be modified and is a signed message from vendors.

4. Highway Monitoring

When using this system, highways should be randomly monitored and the central unit should impose a heavy penalty for driving without a valid ticket. The central unit can send inspectors to patrol and check if vehicles on highways have proper tickets. Inspectors should have read-only access to the database of the central unit so that inspectors will not stop a vehicle that is in the list that contains the license numbers of vehicles that are authorized to drive on that portion of highways on that day. Drivers who purchased tickets less than 24 hours in advance may be asked to stop for ticket

verification. In this case, tickets can be verified by decryption with the central unit's public key and the vendor's public key. If the ticket is valid, the ticket information is recorded by the inspector and will be verified with the sale transaction at the end of the day.

Drivers without a valid ticket will be penalized. Since vehicles not listed in the database are randomly stopped, the penalty of driving without a ticket must be high enough so that drivers will find it's not worth risking. If ticket is valid (the information is correct and was produced with the correct public keys) and has been issued before the time when the database was last updated, it means that the vendor has sold the ticket without reporting to the central unit and kept all the money. In this case, it's not the driver's fault and the vendor is subject to a considerable fine. Inspectors or any other parties cannot produce any ticket since they don't know the keys.

An electronic monitoring system such as automatic license plate detector can be mechanized. However, this will require some structures to be built on highways. The decision about the monitoring method and policy should be made according to the geographical, economic or other factors, which may differ in various countries.

5. Conclusions

This paper proposed an alternative approach to collect toll on highways. Tickets are produced using public cryptographic operations and can be easily verified but not reproduced. The approach requires no construction of a structure of highways, allows flexible tolling options, and prevents some revenue leakages in toll collection.

References

[1] FasTrak, http;//www.dot.ca.gov/fastrak/index/htm

[2] Huang, D., and Huang, W., The influence of tollbooths on highway traffic, *Physica A: Statistical Mechanics and its Applications*, Vol. 312, Issues 3-4, 15 September 2002, p. 597-608.

[3] Levinson, D., and Chang, E., A model for optimizing electronic toll collection systems, *Transportation Research Part A: Policy and Practice*, Vol. 37, Issue 4, May 2003, p. 293-314.

[4] Raytheon, http://www.imperialtech.com/success_highway.htm

[5] Road Infrastructure, http://auto.indiamart.com/user-manual/roads.html

[6] Schneier, B., *Applied Cryptography*, Wiley, 1996.

[7] Tsai, P., Lee, C., Chen, C., Shih, T., Lai, C., and Liou, S., Predicting the content of BTEX and MTBE for the three types of tollbooth at a highway toll station via the direct and indirect approaches, *Atmospheric Environment*, Vol. 36, Issues 39-40, December 2002, p 5961-5969.