Privacy-Sensitive Congestion Charging

Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle

Computer Laboratory,
University of Cambridge,
15 J.J. Thomson Avenue,
Cambridge, UK. CB3 0FD
{arb33,jjd27,rkh23}@cam.ac.uk

Abstract. National-scale congestion charging schemes are increasingly viewed as the most viable long-term strategy for controlling congestion and maintaining the viability of the road network. In this paper we challenge the widely held belief that enforceable and economically viable congestion charging schemes require drivers to give up their location privacy to the government. Instead we explore an alternative scheme where privately-owned cars enforce congestion charge payments by using an on-board vehicle unit containing a camera and wireless communications. Our solution prevents centralised tracking of vehicle movements but raises an important issue: should we trust our neighbours with a little personal information in preference to entrusting it all to the government?

A 2003 study into the efficiency of transport [1] determined that the cost of traffic congestion to the United Kingdom economy is nearly £15bn p.a. (1998 prices), which constitutes 1.5% of the nation's GDP. Furthermore, the RAC Foundation claim that this is set to double within the next decade [2].

The UK Government has recently proposed [3, 4] the implementation of a nationwide congestion charging scheme and has conducted a study into its feasibility [5]. The study suggests that such a scheme will encourage people to consider more carefully how and when they travel, and will provide incentives for them to travel at off-peak times, thus reducing the peak volume of traffic on the roads.

Traditional congestion charging schemes have employed either toll booths accepting cash payment, or vehicle-mounted tags which identify pre-paid accounts, interrogated by custom systems installed on overhead gantries. Whilst both of these systems have attractive properties in terms of maintaining the privacy of their users, they cannot scale to a national level due to the high cost of their installation and maintenance. Similarly, camera-based systems like those deployed in London would be prohibitively costly to extend to all roads nationwide. An alternative is for vehicles to contain on-board units which automatically calculate the congestion charge and decrement an on-board balance, but similar systems have, in the past, proven difficult to make tamperproof. To avoid this potential pitfall, an on-board unit could regularly upload the host vehicle's location to the

congestion charging authority who then calculates the appropriate charge and issues a bill. This approach has particularly undesirable properties with respect to privacy.

In this paper, we propose a novel congestion charging scheme which, in our view, increases the privacy of its users, whilst still ensuring that enforcement of payment is possible. The scheme is particularly interesting because the vehicles form an important component in enforcement: without the support of the majority of drivers, its effectiveness would be severely diminished.

1 Threat model

There are three types of entity taking part in our protocol: vehicle units, payment authorities and enforcement agencies. Vehicle units consist of an outward-facing video camera, a short-range communications unit, a location sensor such as GPS, and a microprocessor. Payment authorities collect congestion charge payments from vehicle units and issue a signed digital certificate to the vehicle unit for any payment made. Enforcement agencies collect data from vehicle units and use this data to issue penalties for non-payment.

We assume that vehicle units have been programmed with the correct public key for each payment authority and enforcement authority. Further, we assume that digital certificates issued by any payment authority cannot be forged, and that the enforcement agencies trust the contents of any valid digital certificate signed by a payment authority. Finally, we assume that vehicle units have some way of communicating with other nearby vehicle units as well as with payment authorities and enforcement agencies. We do *not* assume that the equipment installed in vehicles or their number plates are tamperproof. Therefore vehicle owners may attempt to modify any vehicle under their control.

By assuming vehicle units can be tampered with, we reduce the implementation complexity of the units at the expense of the need for greater care in protocol design. The overall aim of the protocol is to ensure:

- *location privacy for honest users*: the whereabouts of individuals who have paid the congestion charge are not recorded by either the payment authority or enforcement agency; and
- *fare-dodgers are detected*: individuals who have not paid the congestion charge are tracked and sufficient evidence is collected to ensure an enforcement authority can invoke penalties for non-payment.

We will evaluate our proposal in light of these two requirements later.

2 Protocol description

The overall aim of the protocol is to allow the vehicle units to collect evidence of fare-dodgers and provide this information to the enforcement authorities. By doing this, movement data is processed in a decentralised fashion and therefore

the centralised collection of location data concerning honest drivers is minimised. Our proposed protocol can be separated into three main phases: payment, usage and enforcement. We will examine these three areas in turn.

2.1 Payment

A vehicle owner who wishes to make use of the public roads must pay a fee. The fee can be based on any number of criteria, including the time of day, type of road, etc. In order to preserve privacy, payments are made through an anonymous payment scheme such as digital cash [6], and in return the driver receives a digital certificate signed by a payment authority. There may be more than one payment authority, but only one payment authority can operate in a single geographical region.

Every payment authority segments all chargeable roads for its region into spatio-temporal units with a single fixed price; we call such units *chargeable zones*. The set of chargeable zones must be communicated to all vehicle units to enable effective enforcement. Example chargeable zones for a payment authority may include £1 for use of the M11 from Junction 10 to Junction 11 between 8am and 9am, and £1 for use of the M11 from Junction 9 to Junction 14 between 10am and 11am. By ensuring all zones have the same cost, the payment authority can sign journey details received from vehicle owners in return for payment *without needing to see the journey details*. Roads with higher potential levels of congestion would tend to have many more (shorter) zones so that the total cost of travelling along the road is higher. By using a blind signature scheme the vehicle owner can receive a digital certificate (containing details of the road segment, time of travel and vehicle registration plate number) signed by the payment authority, whilst maintaining location privacy. More formally, for a vehicle unit V, with registration plate R, wanting to purchase travel in zone Z from payment authority P, with digital cash D, the protocol operates as follows:

$$V \rightarrow P : \{\{Z, R\}_{K_V}, D\}_{K_P}$$
$$P \rightarrow V : \{\{Z, R\}_{K_V}\}_{K_P^{-1}}$$

If K_V and K_P^{-1} are commutative functions, V can retrieve $\{Z, R\}_{K_P^{-1}}$. The vehicle unit can present the certificate $\{Z, R\}_{K_P^{-1}}$ as proof of payment to anyone who requires it.

2.2 Usage

When travelling on a chargeable road, one vehicle unit, A, may encounter another vehicle unit, B. Our protocol requires some method by which A can determine the identity of B. For example, the registration plate of B may fall into the field of view of the on-board camera of A. In this scenario, unit A uses automatic number-plate recognition software to identify the presence and registration plate R_B of B, and a still photograph of B is taken using the camera on A's vehicle

unit and stored in temporary storage. The time of the sighting and the location of A is derived from the unit's location sensor, and is also recorded with the photograph. Then A, using its radio communications module, challenges B for a valid digital certificate which proves that B has paid the relevant congestion charge. Note that a ubiquitous radio network is not required for this—the two vehicles simply need to communicate directly with each other. Either one of two outcomes occurs:

- B responds by presenting a valid digital certificate $\{Z, R_B\}_{K_P^{-1}}$ to A, in which case A deduces that B is entitled to use the road, and so deletes the photograph of B and takes no further action; or
- B responds with an invalid digital certificate, or B does not respond at all, in which cases A stores the photo of B and the associated time and location in permanent storage.

2.3 Enforcement

Enforcement is carried out by one or more enforcement agencies. At a convenient moment when vehicle unit A receives a network connection via its radio module, A uploads all photos of vehicles which responded with invalid digital certificates, or did not respond at all, to an enforcement agency. This upload does not have to happen immediately, but a fairly prompt delivery of data (of the order of days) is useful for the final part of the protocol.

Every enforcement agency aggregates the reports received from vehicle units at regular (say weekly) intervals. If a particular vehicle has been reported a large number of times, this may indicate that the vehicle was travelling without paying the congestion charge. If the vehicle has indeed been travelling in that location but has paid the congestion charge, the vehicle owner can present the relevant digital certificates to prove payment. In other words, if a vehicle with registration plate R has been spotted travelling in zones Z_1, Z_2 and Z_3, the vehicle's owner should be able to present $\{Z_1, R\}_{K_A^{-1}}$, $\{Z_2, R\}_{K_A^{-1}}$, $\{Z_3, R\}_{K_A^{-1}}$.

In general we wish to avoid such false positives since they waste time and result in reduced location privacy for drivers. False negatives are also troublesome, since these occur when fare-dodgers travel for free, and remove the economic incentives intended to moderate road usage. But, if we assume that all vehicle units operate faithfully, the probability that a fare-dodger will be caught for non-payment is strongly positively correlated with the volume of traffic; thus, when the charge is highest, offenders are most likely to be detected. However, in our threat model we assumed that vehicle number plates and vehicle units are not tamperproof. Therefore unscrupulous individuals may attempt to modify either their registration plate or vehicle unit.

If a vehicle registration plate is modified, replaced or removed, determining the real identity of the vehicle is very difficult. Thus, using the registration plate in a congestion charging scheme provides an additional incentive for tampering with it and therefore we expect the frequency of this crime to increase. However, assuming the deployment of a national-scale scheme with a reasonable proportion

of vehicles equipped with vehicle units, the enforcement agency may be able to track the location and whereabouts of vehicles who do not have valid registration plates (or have none at all) by using vehicle unit cameras to track the movement of objects which are likely to represent cars. Such information may help the police trace vehicles without valid license plates and perhaps also the driver. Our scheme is open to one number plate modification attack: two or more vehicles can use the same registration plate in order to pay a single fee for the congestion charge. Such vehicles would then have to travel substantially along the same route at the same time if a moderate amount of saving is to be obtained. If two cars with the same number plate travel along different routes, then separate payments would have to be made in order to avoid an enforcement action.

Tampering with the vehicle unit itself leads to several further problems. Firstly an attacker can attempt to prevent one or more sensors on the nearby vehicle units from functioning. Examples include shining light at nearby cameras in order to prevent capture of photographic evidence [7], and jamming or altering GPS radio transmissions to prevent adjacent vehicle units from determining their correct current location. Communication interfaces to and from the vehicle unit could also be compromised. For example, care is required when a vehicle unit talks to the enforcement agency to ensure that the data is correctly transmitted: a man-in-the-middle attack may not be able to read the communication if data is encrypted with the public key of the authority, but a failure to forward all the relevant data must be detected and retransmitted, perhaps at a later point in time.

The enforcement agency may also receive erroneous data from modified vehicle units. For example, a malicious individual may upload a forged photograph, or attach an incorrect charging zone to a genuine photo. Such a modified submission may then lend credence to a vehicle owner being falsely accused of using a particular charging zone. Since the vehicle owner may have paid the congestion charge and driven elsewhere or even left the vehicle in a garage there will, in many cases, be no record of the vehicle's actual movements.

One solution to this problem is to attempt to detect the fake evidence and punish those who submit it. Digital watermarking of photographs is not suitable, since the vehicle unit is in the hands of a malicious user who may modify the vehicle unit to apply the watermark to the fake photograph. Statistical analysis of the digital image may help to indicate whether an image has been forged, even if it appears genuine to the human eye [8]. However, such techniques do not protect against forged charging zones.

We require better protection against forged evidence. The next two subsections explore whether we can protect against forgeries whilst still permitting anonymous reporting, or whether reports should only be accepted from certified entities.

Anonymous reporting. If enforcement agencies must rely on anonymous reports, forged data may be detected by examining evidence from many distinct vehicle units. This approach assumes that wide-spread collusion is not possible.

Using this approach, we require a method to ensure enforcement data has originated from different vehicles without compromising the identity of the vehicle's driver. One solution is to issue a unique public/private key pair with each vehicle unit, and to sign the public key using the private key of a payment authority. We can then use this certified vehicle unit key when data is submitted to the enforcement agency. More formally, for a photograph G of a car with registration plate R, taken in charging zone Z, the vehicle unit A (purchased from payment authority P) is equipped with public/private key pair K_A/K_A^{-1} and can submit the following evidence to an enforcement agency E:

$$A \rightarrow E : \{K_A\}_{K_P^{-1}}, \{G, R, Z\}_{K_A^{-1}}$$

By validating the key used by the vehicle unit, an enforcement agency can ensure that data used to determine whether a vehicle is travelling without paying is collected from many distinct vehicle units. Data from vehicle units which have in the past submitted evidence of questionable integrity can be ignored by the enforcement agency. If the reported data $(\{K_A\}_{K_P^{-1}}, \{G, R, Z\}_{K_A^{-1}})$ is found to be questionable, the offending vehicle unit keys can be communicated to payment authorities. The payment authorities can then prevent the offending vehicle unit from purchasing new congestion charging credit assuming, of course, that the payment protocol is modified so that keys must be presented to purchase congestion credit. An indirect fine for submitting fake evidence can then be imposed by charging for the issuance of a new public/private key pair.

Unfortunately such a scheme can lead to invasions of location privacy. The key pair represents a static pseudonym for the vehicle unit, and this enables the enforcement agency to correlate together all the places that the vehicle unit has reported potential offenders. Therefore charging zones must be large enough to prevent any zone from having a strong sense of identity attached to it. For example, we would not allow a section of road connecting a single house to the wider road network to act as an individual charging zone.

Even with this precaution, some privacy violations may continue to exist. For example, if charging zones were created at the granularity of postcodes or zipcodes, then the combination of reports from several zones may uniquely identify an individual. This is perhaps more likely if the released zones include those at the start and end of a long journey. The privacy risks posed can be reduced by limiting the number of reports and exchanging vehicle units (and therefore keys) at regular intervals. Interestingly, the greater the number of fare-dodgers, the less location privacy is afforded to honest participants who file reports with the enforcement agency.

In Section 2.1 we described how a blind signature scheme is used to prevent the payment authority from receiving any journey information associated with a purchase. This means the payment authority (unlike the enforcement agency) can only correlate financial expenditure and time of purchases with the vehicle unit public/private key pair. Intuitively, this appears to pose less risk of re-identification for the owner of a vehicle unit.

Certified reporting. Our solution for anonymous reporting assumes that widespread collusion between vehicle owners was not possible. An alternative scheme which does not rely on this assumption ties any report of bad behaviour to an explicit identity, and offers citizens the chance to submit a traceable report. This route to evidence collection may result in less reports, but allows a more traditional form of witness statement to be collected from a legal entity. This solution allows visual inspection of the vehicle unit to check for tampering—the usefulness of this approach depends on whether a tamper-evident package is easier to build than a tamperproof one.

It is also possible to make two versions of the vehicle unit: one with enforcement potential (i.e. with a camera) and one without. Less comprehensive enforcement may then be possible by only installing the enforcement version on public service vehicles. All vehicles still require a vehicle unit to confirm payment of the congestion charge and therefore maintain location privacy.

3 Discussion

Our congestion charging protocol places some trust in vehicle units to execute the protocol faithfully. If very few vehicle units function correctly, very little enforcement can be carried out. To be truly effective, the charging mechanism requires a critical mass of vehicles to support the scheme. In this paper we have only discussed the validation of congestion charge payments. However, the same scheme can also be used to check for valid digital equivalents of vehicle roadworthiness certificates, general road-tax payments and vehicle insurance.

We believe the system does achieve a greater overall degree of privacy than a centralised system which monitors the movement of all vehicles—our scheme only reveals movement data for those vehicles who have not paid, or do not respond when challenged. This provides an incentive for vehicle owners to ensure that their on-board units are operating correctly and discourages destructive tampering.

Road users would prefer neither the government nor other road users spy on them. However, assuming that a national congestion charging scheme is essential for the future viability of the UK road network, which is the lesser of the two evils? It is our belief that the system we propose is more desirable than a centralised one. In earlier work [9], we gave an overview of this protocol as an example of why privacy issues require greater attention when designing systems. Most responses we have received have been positive, but some were clearly negative, for example:

> "*[W]asn't the last time a population was coerced into spying and reporting on its neighbours assigned to the history books with the disbandment of the Stasi following the collapse of East Germany in 1989?*" [10]

This viewpoint may, in part, be due to the lack of belief in the need for congestion charging. Alternatively, some individuals may prefer to trust the government with their location data, rather than trust their neighbour to provide fair enforcement.

It is important to note that most of the technology to build a vehicle unit exists already. Drivers can install cameras in their cars today and report illegal behaviour to the police. Nevertheless our proposal does encourage wide-scale surveillance and stream-lines the reporting mechanism.

In the UK at least, the general public has a long history of reporting wrong-doing to the state; for example, there are presently mechanisms for citizens to report benefit fraud [11] and unlicensed vehicles [12]. Perhaps the difference between our proposal and current methods is that filing a complaint is voluntary rather than automated by technology (although our proposed protocol could be adjusted to provide users with an option to select when to report offences).

In summary, we believe that this scheme is worthy of study, as it challenges the opinion that user privacy can only be achieved in a large-scale congestion charging system at great cost. The nature of the scheme presented here differs radically from other proposals, particularly in that it relies on its participants to perform the enforcement of payment. Integral societal involvement in the protocol means that the efficacy of the system would depend heavily on the users' attitude toward it.

References

1. May, A., Allsop, R., Andrews, D., Betts, C., Bayliss, D., Cottell, M., Dick, A., Kemp, R., Lowson, M., Ridley, T., Tietz, S., Wootton, H.: Transport 2050: The route to sustainable wealth creation. Technical report, Royal Academy of Engineering, 29 Great Peter Street, London, SW1P 3LW (2005)
2. RAC Foundation: New government—new agenda for transport? (2005) `http://www.racfoundation.org/index.php?option=com_content&task=view&id=%66&Itemid=35`.
3. House of Commons Transport Committee: Road pricing: The next steps (2005)
4. Department for Transport: The Government's response to the Transport Select Committee's report, *Road Pricing: The Next Steps* (2005)
5. Department for Transport: Feasibility study of road pricing in the UK (2004)
6. Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: CRYPTO '88: Proceedings on advances in cryptology, New York, NY, USA, Springer-Verlag New York, Inc. (1990) 319–327
7. Truong, K.N., Patel, S.N., Summet, J., Abowd, G.D.: Preventing camera recording by designing a capture-resistant environment. In Beigl, M., Intille, S.S., Rekimoto, J., Tokuda, H., eds.: Ubicomp. Volume 3660 of Lecture Notes in Computer Science., Springer (2005) 73–86
8. Popescu, A.C., Farid, H.: Statistical tools for digital forensics. In: 6th International Workshop on Information Hiding, Toronto, Canada (2004)
9. Harle, R., Beresford, A.: Keeping big brother off the road. IEE Review **51**(10) (2005) 34–37
10. Brown, S.: Feedback: Big brother is back. IEE Review **51**(12) (2005) 6
11. Department for Work and Pensions: Website, "Report a cheat online form" (2006) `https://secure.dwp.gov.uk/benefitfraud/`.
12. Driver and Vehicle Licensing Agency: Website, "Reporting of unlicensed vehicles on the public highway" (2006) `http://www.dvla.gov.uk/public/unlic_veh/report_online.htm`.