A new approach to time, distance and place-dependent road pricing can offer, both with ‘thin’ and ‘fat’ on-board equipment (OBE), greater privacy protection and fraud-resistance. It allows the hiding of the amount of usage between two check-points and an enforcement approach that does not rely on physical protection of OBE against traffic data manipulation.

Most countries currently have a road tax for cars, involving a fixed charge or a toll based on the actual road use, but this system may depend, for example, on the car’s weight and engine category. Toll charges for roads, bridges or tunnels introduce a certain level of usage dependence, but only at a limited number of specific locations. In addition, these charges are performed by one step further and to replace these (road toll and toll) charges with a new wide area pricing system in which road charges depend on the actual distances driven and possibly also on the time of day and on location. Such time-distance-place road pricing is not only considered to be fairer than flat charges, but also allows targeted congestion and pollution reduction by applying a higher tariff per kilometre for busy areas or road segments and for environmentally unfriendly cars. Furthermore, it can solve the fine distribution problems associated with the transition to plug-in hybrid and fully electric vehicles.

Global navigation satellite systems, like GPS or Galileo, usually form the basis for such road pricing. The idea is that cars will be equipped with OBE for registering their consecutive locations and transferring relevant information to the traffic service provider (TSP) or traffic fee charger (TC) for billing and checking purposes.

Fraud-resistance and privacy

It is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race. Furthermore, it can solve the fine distribution problems associated with the transition to plug-in hybrid and fully electric vehicles.

Global navigation satellite systems, like GPS or Galileo, usually form the basis for such road pricing. The idea is that cars will be equipped with OBE for registering their consecutive locations and transferring relevant information to the traffic service provider (TSP) or traffic fee charger (TC) for billing and checking purposes.

Fraud-resistance and privacy

It is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race. Furthermore, it is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race.

It is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race. Furthermore, it is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race.

It is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race. Furthermore, it is obvious that fraud-resistance is important and also that the OBE resides in a possibly hostile environment. In general, it is rather unwise to fully rely on physical (ie, hardware) protection measures, since these are never perfect and are always subject to an arms race.
Data Protection

- and approved or trusted by - the traffic fee charger. Thus, this TSP receives all details of all trajectory parts travelled, including vehicle identity.

In our approach - and particularly also in its thin variety - this is different. Our approach uses ‘non-revealing commits’ and gives the user full freedom in choosing any party to commit. Further, these calculations do not require supply of absolute timestamps, nor of any identification. Therefore, the user may choose to ‘anonymise’ the location data before committing. Furthermore, it also offers more flexibility in designing and implementing fraud-resistance, since one can choose any combination (e.g., a cost-optimal one) between the extremes of ‘spot-checking only’ and of ‘physical protection only’.

Parallel protection offers much better operational continuity than serial protection. If parallel protection is breached, the spot-checking still works and can relatively easily be intensified temporarily until the physical protection problems are solved. Further, parallel protection offers at least twice as much fraud-resistance as serial protection (or the same level of fraud-resistance at lower costs). It also offers more flexibility in designing and implementing fraud-resistance, since one can choose any combination (e.g., a cost-optimal one) between the extremes of ‘spot-checking only’ and ‘physical protection only’.

In addition, it offers more operational flexibility, since intensifying spot-checking always raises the aggregate protection level (no limit is imposed by physical protection). Finally, only in the case of parallel protection can remote spot-checks be used to monitor the aggregate fraud-resistance level that is actually achieved, in terms of percentages of violations. For example, a traffic fee charger can monitor easily whether (and to what extent) various traffic fee service providers succeed in keeping traffic fraud below a level agreed upon.

Free competition and easier interoperability

Our approach allows for a minimal uniform infrastructure, dealing with the collection of hash values and requests for original data needed for spot-checks, on top of which many different (thin and fat) implementations may be offered by various commercial and non-commercial parties. Users can freely choose whether and, if so, to which parties - they are willing to reveal more information, such as (part of) their location data or other travel information.

Finally, we mention that our approach eases scaling up to an international setting due to its monitoring capability, its easy and robust observation-based enforcement and its hash values, which can be exchanged between different countries - or collected centrally - without endangering privacy. For example, for enforcement purposes one could set up one European hash value collector that after each legitimate request supplies a specific hash value to an enforcement unit. The important thing is that given a certain hash value (like “4f5...” as above): a) there is no feasible way to reconstruct its original input (also known as the ‘pre-image’) or any part of its input, while b) one can easily check whether some given sentence (e.g., “traffic pricing is hot” or ‘...hit”) must have been the original input, simply by checking whether the hash value of this given sentence is the same (e.g., “4f5...”). In short, hash values can work as ‘anonymous’ digital fingerprints of their input.

Data Protection

Figure 1. Hash values used as ‘anonymous’ fingerprints

Secure hash functions are basic operations in cryptography that transform an input text to completely garbled output. For instance the (MD5) hash value of the sentence “traffic pricing is hot” is “4f5688b38731cafe4ecb13e93f2d7f82”. By changing only one character in the input, the output is totally different: the hash value of “traffic price is hot” is “a7f73aa6a9d4007ac3e638c6b8d76852”. The important thing is that given a certain hash value (like “4f5...” as above) a) there is no feasible way to reconstruct its original input (also known as the ‘pre-image’) or any part of its input, while b) one can easily check whether some given sentence (e.g., “traffic pricing is hot” or ‘...hit”) must have been the original input, simply by checking whether the hash value of this given sentence is the same (e.g., “4f5...”). In short, hash values can work as ‘anonymous’ digital fingerprints of their input.

Figure 2. Observation-based spot-checks and non-revealing commits based on hash values

If OBE regularly sends hash values of its location data to the traffic fee charger, it commits itself to these location data without revealing any content (see Figure 1). Observation-based spot-checks then can be performed as follows. After a road-side observation and after receipt of the commit (i.e., hash value of the traffic data that correspond to the time of observation), one demands the ‘pre-image’, that is, the original traffic data committed to. Then one verifies whether the data returned indeed produce the correct hash value and also cover the location of the observation correctly.