Journey time monitoring through UTMC systems

A UTMC Technical Guide
Library reference ***UTMC-TR012.001***

31 March 2015

Cover + 5 pages

List of contents

1 Introduction

1.1 About this document

1.1.1 UTMC is a UK-led initiative which provides and maintains a technical framework for traffic management and related systems. It is geared to producing open specifications geared to the needs of real world projects, delivered through an efficient and innovative supply market. UTMC specifications are endorsed by the UK Department for Transport and are published on the UTMC website at: http://www.utmc.eu.

1.1.2 ANPR has for some time been used for journey time measurements, and there is an established UTMC protocol for ANPR systems. However, during 2014-15 it became clear that there were an increasing number of systems using non-ANPR sensor technologies to determine actual journey times of vehicle between two points on the network. In particular, the use of low-power sensors detecting and identifying devices (such as mobile phones) with a Bluetooth connection had reached the point where several commercial products were on the market, both in the UK and elsewhere in the world.

1.1.3 A Working Group was therefore convened, sponsored by Reading Borough Council, to consider how such systems might be incorporated into UTMC systems. This guidance note has been developed based on the conclusions of that WG.

2 Guidance

2.1 Architecture

2.1.1 Estimating the actual journey time on a link road is a complex process, involving several steps or data gathering, analysis and presentation. The nature of each step depends on the purpose to which the information will be put; for example, if the aim is to inform drivers just entering a congested area, it will need to take into account projections of traffic change in the near-term future. It also depends on the environment: in a motorway context, traffic is relatively uniform, whereas in the urban space there is often “clutter” (eg from buses and pedestrians) and a targeted algorithm is therefore required to tease apart the data.

2.1.2 The applications logic in journey time estimation is therefore sophisticated and it is not appropriate to determine a single simple standard. In common with many UTMC applications, this is an area where supplier innovation can be highly beneficial.

2.1.3 Similarly, the channels by which information is distributed are many and various, and the format is which information is presented. This is true even where journey time information is used relatively “raw”, for example by traffic managers monitoring the state of the network.

2.1.4 However what all of these architecture have in common is the need to identify a specific vehicle (or person) at one point of the network, and to match this with a subsequent detection of the same vehicle (or person) elsewhere. It is the focus of this document to focus on standardisation of this element.

2.1.5 Achieving this would make it easier to determine journey time in a wide array of contexts. In particular:

- If the two detectors are provided by different suppliers, a standard message means that the detections are more likely to be matchable;
- If the two detectors are operated in different geographical areas or by different traffic authorities, a standard message makes it easier to exchange operational data to monitor cross-boundary journey times.

2.1.6 The physical location of the open interface is less important: it could be over the air or between severs, depending on the design of the sensor, the communications available, and the operational procedures adopted. The actual architecture used would need to be determined locally in discussion with system suppliers.

2.1.7 *Note*: Some approaches to journey time estimation have totally different architectures, for example those that extract estimates from a network model based on detected (but not identified) vehicle flows. This document is not relevant for these approaches.

2.2 Interface specification

2.2.1 UTMC already has data structure geared to journey time estimation. These exist as a UML model, an XML schema, together with a guidance note on usage – all available on the UTMC website (respectively as **UTMC-TS004.0062 Objects - Addendum ANPR UML Mar15.pdf**, **utmc_anpr_schema_V1-2.zip** and **UTMC-TR007.002 ANPR.pdf**).

2.2.2 In fact, this is not logically dependent on the solution being based on ANPR – it provides the necessary structure for any journey time estimation method which is based on sensing individual vehicles.

2.2.3 Essentially the only feature that needs to be reinterpreted is the VRN field, which becomes a technology-dependent “unique” trackable identifier. For systems based on Bluetooth “sniffers”, it is recommended that this field should be interpreted as “device MAC address”. (This, or an equivalent device address, may be used for a range of other communications-capable devices, such as those based on WiFi detection.)

2.2.4 Associated interpretation will be necessary elsewhere within the protocol. Several other fields, while remaining relevant as they stand, are given names which assume an ANPR context – for example, the class **PlateRead** and the config commands SendVRNs and MaxPlatesToSend.

2.2.5 Other fields only make sense in an ANPR context, such as the diagnostic field MeanIlluminatorTemp. Still other fields may be relevant or not, depending on the detector used – for example vehicle parameters such as Make and Model or association parameters such as Country.

2.2.6 ANPR is also present elsewhere in UTMC: in the CCTV Package (Annex D Section 9 of the UTMC Data Object Registry UTMC-TS004.0061:2010) in the TL_ANPR components of the TransportLink Package (Annex D, Section 26 *ibid*). These are able to be used essentially unchanged, although there are some fields where the names imply ANPR and which will need to be interpreted suitably. For example, in the **TL_ANPR_Dynami**c class the field NumberPlateMatches should be read as “number of detected device matches”.

2.3 Security

2.3.1 ANPR data is subject to strict scrutiny under data protection legislation, and both users and systems developers are sensitive to the need to minimise the risk of personal data leakage. There are two ways of achieving this: non-lossy *encryption* of data when vulnerable – especially during transmission from device to centre and vice versa – and lossy *anonymisation* to remove the unique link.

Encryption

2.3.2 UTMC provides separate (high level) guidance on security architectures (UTMC-TR005). In the case of journey time systems, this generally indicates that (non-lossy) encryption is required only over the communications link, rather than in storage or in the application layer. The following approach has been suggested by the Working Group and will normally be sufficient:

- Open SSL V3 transport layer security;
- AES256 standard encryption;
- 2048 bit RSA keys.

Anonymisation

2.3.3 For some applications, for example in police surveillance, it may be necessary to keep the full MAC address through the system. However for journey time monitoring it is usually more convenient to anonymise the MAC address at source. This is in keeping with the guidance from the Information Commissioner’s Office, and will simplify operational processes and data management considerably by avoiding many of the requirements for handling “personal data”.

2.3.4 Because anonymised data loses global uniqueness, incorrect matching may occasionally occur. Generally this can be addressed through the use of statistical techniques for removing outliers, with minimal impact on system performance.

2.3.5 Three approaches to anonymisation are recommended – the selection of which will depend on local context:

- The simplest approach is to truncate the MAC address. This is computationally easy but least secure. The truncated MAC address should be sent in the VRN field; the truncation algorithm will determine the matching algorithm, and should be recorded in the system design documents.

- The UTMC ANPR protocol provides an existing hashing algorithm for ASCII VRN data that can be applied equally well to ASCII-Hex Bluetooth (or Wifi) MAC addresses. The resulting hashed value should be sent in the Tag field – this is a single byte and this makes for efficient communications.

- For some authorities – in particular Highways England – a higher grade of secure anonymisation is required. In this case, it is recommended to use the SHA-256 algorithm ("Secure Hash Algorithm on 256 bits"). This is a US Government algorithm and a series of references can be found at http://en.wikipedia.org/wiki/SHA-2. The resulting hash should be sent in a new field, SHATag, of length 32 bytes (256 bits).

2.3.6 There are pros and cons to each approach both in security and in system performance. Integration between systems using different anonymisation approaches will generally not be possible.