TAXIMETERS

Taximeters - solutions to combat fraud

CLAUDE RICARD, Gleike Inc. (USA) and MICHEL LE FAOU, ATA (France)

Introduction

In any major city, the words "taxi" and "taximeter" conjure up a variety of preconceptions. The taxi driver is unfortunately renowned for defrauding - sometimes accusations are exaggerated, but often the fraud is underestimated.

The fight against taximeter fraud is an international concern and both domestic and foreign customers must be protected, especially as the latter may form an initially negative opinion of a country on arrival if they experience over-charging by a taxi.

In the field, two kinds of fraud flourish:

- visible fraud (for example the application of a higher tariff), against which the domestic consumer can be on his guard; and
- invisible fraud (for example injection of extra distance pulses), which first appeared with the advent of electronic taximeters and the most recent generations of vehicles. Here, the consumer is defenseless. This second type is in fact impossible to detect and any omission in the applicable standard, regulation or type approval may have severe consequences since it is difficult (if not impossible) to remedy this kind of situation in the aftermath.

In this paper, the authors describe various types of fraud observed in the field (thousands of inaccurate taximeters are already in use on the market), especially those that concern the injection of abnormal signals. They will show that efficient solutions do exist to detect this problem.

The electronic taximeter

The taximeter is an instrument installed on public hire vehicles (taxis) which calculates and indicates the fare to be paid on the basis of distance traveled and journey duration.

A sensor (either one installed by the vehicle manufacturer for other purposes, or one especially installed for the taximeter) provides distance pulses and an internal clock gives time information.

In some countries, the meter also controls an illuminated unit mounted on the vehicle's roof which displays externally the tariff being applied.

The meter casing is generally mechanically sealed but neither the sensor nor the cable feeding the meter are protected, which is an issue for concern.

Main types of fraud that can be found in the field

The traditional targets for taximeter fraud are firstly the domestic customer who is not aware of local regulations and secondly the foreigner who is unfamiliar with the fares typically applied in the country he is visiting. The following can be noted:

- *use of a higher tariff*: particularly frequent in those countries in which the driver can manually modify the tariff position;
- *the meter starts counting before the journey begins*: it is not easy to differentiate between the official initial fare and another amount displayed; and
- *display of wrong data*: for instance a totalizer is displayed instead of the fare.

Table 1 gives an idea of the extent of each kind of fraud and the difficulty in detecting them. The solutions (generally) instigated to combat them are also presented.

But there is a more insidious and more serious form of fraud which concerns the taximeter system (taximeter device, sensor, peripherals, wiring) and the customer may not even imagine that a sealed instrument can be a

Table 1 Fraud detectable by the customer

Fraud	Extent	Detection difficulty	Solution
Wrong data displayed	Low	Easy	• Type approval: data displayed (totalizers, internal information) must be clearly and unambiguously identified
Meter starts counting before trip begins	Medium	Easy	• Display of the applied tariff on roof for police control; • Printed receipt mandatory
Use of a higher tariff	High	Easy	• Display of the applied tariff on roof for police control; • Tariff simplification and automatic changes; • Printed receipt mandatory; • Consumer information

potential source of cheating. This form of fraud consists in modifying the taximeter system to artificially increase the measurement of the journey distance (see Table 2). The following can be observed:

- injecting extra pulses into the sensor line by means of a small device called a "zapper" (also known as a "sugar" in the United Kingdom);
- changing the tires, which is an easy way to add extra meters to the actual journey distance; and
- modifying the taximeter itself by altering the software, using software available in another country, or changing the tariff table or the *k* constant.

The zapper

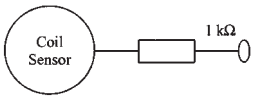
On a "parallel market", several kinds of zappers can be bought at prices varying from 50 to 500 Euros. Due to their small size (~ 2 cm^3), they can easily be concealed and are normally activated by a hidden switch situated near the driver, though some models are located behind the dashboard and controlled by a magnet.

Due to the large variety of sensors that exist on the market, many of which differ in impedance and in signal shape, the most widely-used anti-zapper may or may not function efficiently depending on the model of car and on the distance sensor installed in the vehicle. The authors have observed that defrauders tend to buy and use those models of cars on which it is easy to commit fraud.

To better understand how it is possible to "mislead" a taximeter, it is important to understand what kinds of signals the sensors and zappers generate.

The main features of the sensor line are the signal shape (square or sine) and the impedance level (low or high). Accordingly, one can group the sensor generators into three families:

1 Alternator type (**coil**) providing alternative or positive sine pulses. The signal amplitude depends on the rotation speed of the magnet facing the coil. Sensor impedance is roughly 1 kΩ, the same value for the high and low levels:



2 Hall effect sensor type, with open collector output (**HE/opc**) providing square pulses. The low level can vary from 0 V to 1.5 V and the high level from 5 V to 12 V. The sensor impedance is around 100 Ω (low level) and 10 kΩ (high level):

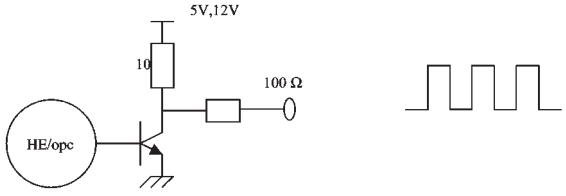
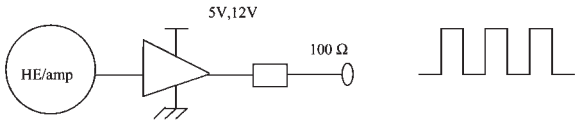


Table 2 Fraud not detectable by the customer

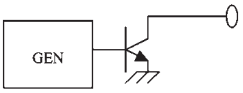
Fraud	Extent	Detection difficulty	Solution
Change of tires	Low	Easy	• Controls in the field; • Printed receipt mandatory
Internal modification of the taximeter (program memory, parameters change);	Low	Not very easy	• Mechanical and electronic sealing; • Software protections
Taximeter programming not compliant with regulation	Low	(Very) difficult	• Agreement and control of installers and meter shops
Injection of abnormal pulses	High	(Very) difficult	• Security device inside the meter able to detect any fraudulent injection; • Distance sensor devoted to the taximeter

3 Hall effect sensor with amplifier and current protection type (**HE/amp**) providing square pulses. The low level can vary from 0 V to 1.5 V and the high level from 5 V to 12 V. The sensor impedance is around 100 Ω for high and low levels:

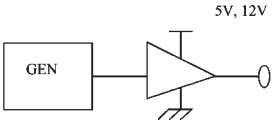


The zapper generators can be grouped into five types:

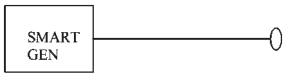
Zapper type 1: Fixed frequency generator with open collector output:



Zapper type 2: Fixed frequency generator with analog amplifier output:

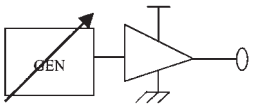


Zapper type 3: Smart zapper that generates 1 pulse (high level) every *n* pulses:



Zapper type 4: Smart zapper that generates 1 pulse (low level) every *n* pulses:

Zapper type 5: Smooth on frequency generator with open collector output:



It can be observed that a zapper is generally able to inject signals on the line due to the difference in impedance between the two generators (the sensor does generally not have a very low output impedance due to current protection).

The first security devices designed only verified whether the distance signal seemed to be perturbed. But very rapidly new zappers came onto the market with technology capable of taking control of the sensor line by injecting pulses with the same shape, at a very low impedance, and providing a smooth acceleration after

power-up. This kind of zapper is difficult to detect using rudimentary techniques.

This zapper (type 5 - see page 11) comes into action either when the speed of the car is low or when the car has stopped. Generally equipped with an amplifier output, it generates pulses at a frequency that increases until a fixed or adjustable medium speed is reached, at which time the frequency is stabilized at a predetermined speed or decreased slowly. The latest techniques designed by ATA are able to detect such zappers.

Anti-zapper solutions available: the Gleike Mini Generation

The Gleike Mini Generation is the first product line on the market which integrates a maximum number of powerful solutions to fight the zappers, basically through software signal and data processing. Its efficiency has been proved on over 15 000 instruments in the field.

The solutions implemented are based on the consideration that when a fraudulent signal is injected, this injection leads to the modification of various features of the sensor line or the sensor signal such as pulse width, amplitude modulation, impedance modification, frequency jump, etc.

The strategy can be resumed as follows:

- during the installation, the meter "takes a photograph" of the sensor line and the pulse characteristics and memorizes them;
- when running and periodically, the meter verifies that the measured characteristics fit with the initial ones;
- when abnormal characteristics are detected, the meter stops the price calculation based on distance, and stops working at the end of the trip, displaying an error message; and
- the meter has to be re-programmed (i.e. returned to the supplier).

To take a decision, the meter analyses the following criteria:

- the line impedance variation at the low and high signal levels (comparison with initial impedance);
- the amplitude modulation (comparison with average amplitude);
- the signal duty cycle variation (comparison with initial duty cycle);
- whether the speed limit is exceeded;
- whether the acceleration is too high for the car;
- sudden speed changes; and
- any abnormal stability of the speed.

The processor designed for the Gleike Mini Generation is able to detect a zapper in under 24 seconds. According to an average duration of 20 minutes for a trip, that duration represents less than 2 % of an average trip.

Note: The solutions presented here can be applied to other classes of instruments, especially any instrument that receives pulse signals from a sensor, such as industrial counters, fuel pumps, chronotachographs, etc.

Methodology used by ATA to accept or reject an anti-zapper system

The tests have to take into account the following parameters:

- diversity of sensor technologies (grouped into 3 families);
- diversity of zapper technologies (grouped into 5 families - today at least!); and
- speed of the car.

A practical way is to check all the possible combinations of sensor and zapper families, for three speeds:

- vehicle has stopped;
- low speed (the speed must be increased slowly from 0 to 20 km/h); and
- high speed (the speed must be increased slowly from 0 to 100 km/h).

When the vehicle has been stopped, two tables have to be checked:

- sensor output is low level; and
- sensor output is high level.

It is important to note that during the test the speed must be increased smoothly, as in an actual vehicle. Abnormal acceleration would be detected by the common acceleration process and would distort the test results. However, the fifth zapper is not detected by the acceleration control.

Speed =	Zapper 1	Zapper 2	Zapper 3	Zapper 4	Zapper 5
Coil	×	×	×	×	×
HE/opc	×	×	×	×	×
HE/amp	×	×	×	×	×
Sensor					

Consequently 4 × 15 tests have to be performed. For each square, the result is "OK" if the zapper has been detected after less than the target time (24 s for the Gleike Mini Generation) (see Annex: Examples of sensor line disturbances, pages 13 and 14).

Examples of legal clauses relative to fraud protection

- ***France: Decree of 17 February 1988 - art. 11 (extract and translation):***

The taximeter has to be supplied with an automatic control of the distance pulses enabling it to ensure that only the pulses corresponding to the effective traveled distance are taken into account.

- ***The proposal for a European Directive on measuring instruments, in the annex MI-007 (Taximeters) offers the following article:***

A taximeter and its installation instructions specified by the manufacturer shall be such that, if installed according to the manufacturer's instructions, fraudulent alterations of the measurement signal representing the distance traveled are impossible.

The European Directive is interesting because the requirement is expressed in terms of global result instead of imposed solution. This global result guarantees the consumer against "invisible" fraud and defines goals for the manufacturer - and therefore for the installer. Actually the installation operation is fundamental. In France, it happened that some instruments, 100 % compliant with the regulation, were installed in such a way that actually permitted fraud.

Conclusions

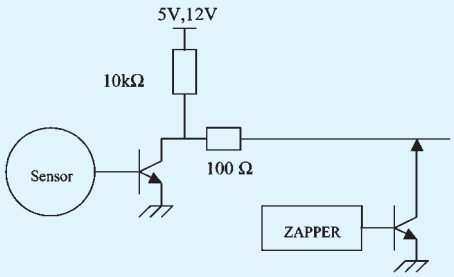
The alteration of the metrology chain (distance sensor - meter) is prevalent, invisible and pernicious. The injection of extra distance pulses is an easy operation using readily available technology (kits are available around the world in electronics shops). Controls in the field are inoperative due to the zapper's small size and because it can be plugged in anywhere along the sensor cable.

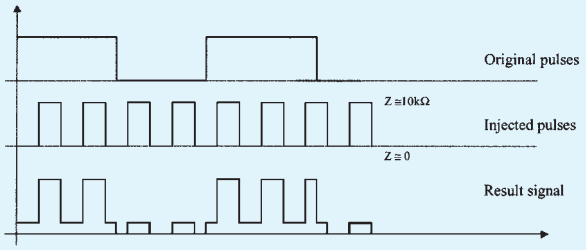
According to the metrology viewpoint, it is difficult to admit that the sensor that measures the distance for the purpose of price calculation can remain unprotected. It is also difficult to admit that the consumer is likely to be confronted with an instrument that has been tampered with.

Only security devices integrated within the instrument are able to effectively fight "invisible" fraud. The technology to accomplish this is available and manufacturers do have appropriate and cost-effective solutions. When implemented, such solutions lead to actual results

Annex: Examples of sensor line disturbances

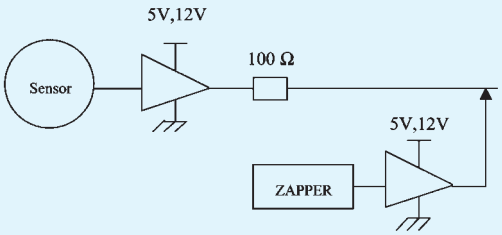
HE/OPC sensor versus zapper type 1

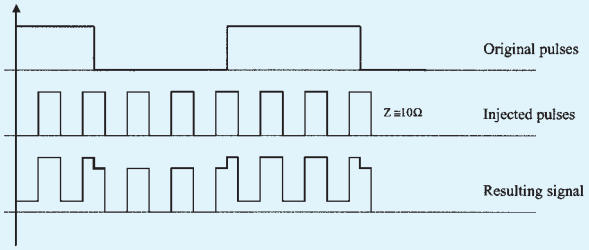




- only the high levels of the sensor signal are affected by the zapper;
- the average amplitude is modified; and
- similar phenomena can be observed with sine pulses.

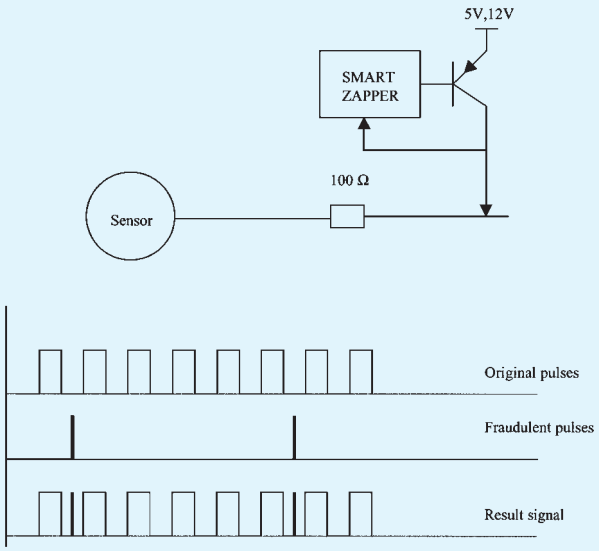
HE/AMP sensor versus zapper type 2 OR 5





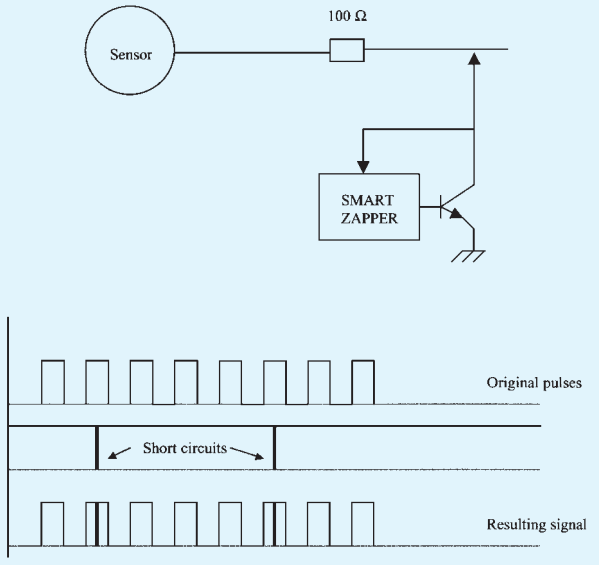
- the fraudulent signal is injected through a low impedance. Then the zapper dominates the sensor;
- injection also generates an amplitude modulation; and
- similar phenomena can be observed with sine pulses.

HE sensor versus smart zapper (high level)



- the smart zapper watches the line (in high impedance), counts *n* pulses and injects an additional pulse, (of very low impedance);
- for instance, if *n* = 5, the distance is up 20 %; and
- similar phenomena can be observed with sine pulses.

HE sensor versus smart zapper (low level)



in the field (ATA has been working on this issue since 1991 and 15 000 anti-zapper systems operate in cabs daily).

But for a manufacturer, this is not a normal concern. The company will tend to satisfy the minimum requirements to pass the type approval tests, but not more. Otherwise the market will reject the product. So the rules must be defined by standards.

Several specialists are working to prevent fraud and at the same time, thousands of drivers are conducting tests to find the flaws in the system. When such flaws are detected, drivers take advantage of them and once they find a way to cheat, many do not hesitate to do so.

Metrology Organizations and States have been dealing with the problem of fraud for a long time. Several Weights and Measurement Boards are working to include security directives in standards and regulations, and especially directives based more on the global result than on imposed solutions. ■

ATA (S.A.) is a private company located near Marseilles in the South of France. The company has been working on taximeters since 1977 and more than 200 000 instruments have been sold around the world. ISO 9002 certified, ATA is recognized for its excellence in fraud fighting: 15 000 anti-zapper systems are working daily. Gleike Inc is an ATA subsidiary in charge of the American market, managed by the ATA founder and located in Chicago.

For further information:

Europe Area Contact:

Michel Le Faou
ATA (Automatismes et Techniques Avancées)
Route de Trets
13710 La Barque
France
Tel.: +33 (0)4 42 58 53 53
Fax: +33 (0)4 42 58 62 82
E-mail: mlf@gleike.com

USA Area Contact:

Claude Ricard
Gleike Inc.
1206, Fairfield Road
Glencoe, IL 60022
Tel.: +1 847 835 7055
Fax.: +1 847 835 7063
E-mail: cr@gleike.com