

(19) **DANMARK**



Patent- og
Varemærkestyrelsen

(12)

Oversættelse af europæisk patentskrift

(10) **DK/EP 2860703 T3**

-
- (51) Int.Cl.: **G 07 B 15/06 (2011.01)**
- (45) Oversættelsen bekendtgjort den: **2016-10-10**
- (80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2016-06-22**
- (86) Europæisk ansøgning nr.: **13187687.2**
- (86) Europæisk indleveringsdag: **2013-10-08**
- (87) Den europæiske ansøgnings publiceringsdag: **2015-04-15**
- (84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**
- (73) Patenthaver: **Kapsch TrafficCom AG, Am Europlatz 2, 1120 Wien, Østrig**
- (72) Opfinder: **Nagy, Oliver, Leopold Steiner Gasse 48, 1190 Wien, Østrig**
Povolny, Robert, Nußdorfer Lände 39, 1190 Wien, Østrig
- (74) Fuldmægtig i Danmark: **Denmeyer & Associates S.A, P.O. Box 700425 , Landaubogen 1-3, DE-81373 Munich, Tyskland**
- (54) Benævnelse: **FREMGANGSMÅDE TIL EFTERPRØVNING AF GEBYRTRANSAKTIONER OG KOMPONENTER HERTIL**
- (56) Fremdragne publikationer:
EP-A1- 2 500 869
EP-A1- 2 530 654
EP-A1- 2 538 363
EP-A1- 2 541 502
EP-A2- 1 708 143

Method for Checking Toll Transactions
and Components therefor

The present invention relates to a method for checking toll transactions and also to a vehicle-based arrangement and a transaction server for same.

In the future European electronic toll system (EETS), vehicle-based on-board units (OBUs) are to be interoperable both with "infrastructure-bound" and "infrastructureless" road toll systems. Infrastructure-bound road toll systems are based on a network of geographically distributed toll beacons, which communicate via short-range radio with OBUs of passing vehicles in order to localise these to the respective beacon location and thus charge for location use. Infrastructureless road toll systems are based on satellite-assisted "self-locating" OBUs, which transmit the position notifications and/or toll transactions via a mobile network to a central station. An EETS-compatible OBU therefore has to have both a short-range transceiver, for example in accordance with the DSRC (dedicated short range communication), CEN-DSRC, UNI-DSRC, IEEE 802.11p or WAVE (wireless access for vehicular environments) or ITS-G5 standards, for communication with the toll beacons of the infrastructure-bound road toll system as well as a satellite navigation receiver and a mobile communications module for communication with the mobile network of the infrastructureless road toll system. Such a multi-functional OBU is therefore constructed in an extremely complex manner and also requires comprehensive testing and certifications so that it meets the accuracy and security requirements of the respective road toll system in order to prevent toll calculation errors and toll fraud.

One object of the invention is to create a multi-functional OBU for interoperable road toll systems, which is of simpler construction and requires lower testing and certification outlay compared with the known systems without undermining the billing and fraud security of the system as a whole. A further object of the invention is to create a method for checking toll transactions of such multi-functional OBUs as well as toll beacons and transaction servers suitable for same.

In a first aspect the invention thus creates a method for checking toll transactions, generated from position notifications of a mobile phone connected via a mobile network to a transaction server, with the aid of a network of distributed toll beacons, which communicate via short-range radio with on-board units of passing vehicles and are connected to the transaction server, comprising:

carrying a mobile phone and an on-board unit on a vehicle;

generating a session identifier, exchanging the session identifier between mobile phone and on-board unit and transmitting the session identifier to the transaction server;

producing position notifications in the mobile phone and sending the position notifications under the session identifier to the transaction server in order to produce toll transactions;

when the on-board unit passes a toll beacon, logging the pass in a beacon log under the session identifier; and

in the transaction server, double-checking the toll transactions produced for the session identifier with the beacon log created for the session identifier.

In accordance with the invention, an interoperable multi-functional OBU is formed from a GNSS (global navigation satellite system) -enabled mobile phone on the one hand and a DSRC (dedicated short range communication) -enabled OBU on the other hand, which exchange data via a common interface. A unique identifier in the road toll system (at least temporarily), that is to say the session identifier, can be exchanged via this interface and forms a link between the infrastructureless billing functions of the multi-functional OBU on the one hand and the infrastructure-bound billing functions of the multi-functional OBU on the other hand. The highly secure and highly accurate position data of toll beacons of an infrastructure-bound road toll system which encounter a multi-functional OBU during the journey thereof, said OBU operating in GNSS or infrastructureless mode, can thus be used with the aid of the checking method of the invention to check the GNSS-based toll transactions, such that billing errors and fraud attempts, to which an infrastructureless road toll system is exposed, can be recognised and pun-

ished. The invention therefore creates an interoperable road toll system with high billing and fraud security on the basis of few, cost-effective components with low certification outlay.

In accordance with a first preferred variant of the invention, when a toll beacon is passed a beacon identifier is transmitted from the toll beacon to the on-board unit and is stored in a first beacon log in the on-board unit, and the first beacon log is transmitted with the session identifier via the mobile phone to the transaction server in order to be double-checked. The beacon log used to double-check the GNSS-based position notifications is thus collected by each multi-functional OBU itself during the journey thereof, which requires only little change to the existing toll beacon network.

In a second variant of the invention, which can be executed alternatively or additionally to the first variant, as a toll beacon is passed the session identifier is transmitted from the on-board unit to the toll beacon and from there is transmitted with a beacon identifier to the transaction server, and all beacon identifiers received under the session identifier are stored in a second beacon log. Here, the toll beacon network collects the passes of a multi-functional OBU past a beacon under a certain session identifier, which relieves the OBU part of the multi-functional OBU, such that OBUs that are more cost-effective and have lower computing power are sufficient.

In a third variant, in which both a first beacon log is collected in a multi-functional OBU and a second beacon log is collected by the toll beacons, the second beacon log may additionally also be double-checked against the first beacon log during the double check. This introduces a further security stage into the system, since not only can either the beacon passes collected by the multi-functional OBUs during the journey thereof in the form of the first beacon logs or the OBU passes collected by the toll beacons in the form of the second beacon logs be used for checking, but both beacon logs, more specifically both for mutual checking and for the checking of the GNSS-based position notifications.

A further advantageous embodiment of the method of the invention comprises the following features:

when passing the toll beacon: recording a vehicle feature using a detector of the toll beacon and storing the vehicle feature under the session identifier in the toll beacon; and
when the double check in the transaction server indicates a mismatch, transmitting the stored vehicle feature from the toll beacon to the transaction server.

The toll beacons passed by a multi-functional OBU in GNSS mode can thus also be used simultaneously for enforcement. In contrast to known DSRC solutions, a vehicle feature is recorded by way of precaution each time a multi-functional OBU passes a beacon; if the subsequent double check in the transaction server reveals that a calculation error, toll offence or fraud attempt has occurred in the GNSS-based toll mode, the vehicle feature recorded at the corresponding toll beacon can be used for enforcement because it proves that this beacon was passed.

The detector is preferably a camera and the vehicle feature is preferably a feature of an external appearance of the vehicle, and therefore an image of the vehicle or of the number plate thereof can be used as enforcement proof, for example.

In order to ensure protection of the personal data of the vehicle user, such as number plate or whereabouts of the vehicle, the recorded vehicle features or images can preferably be encrypted with the aid of the session identifier in order to prevent improper use. If a toll transaction is checked and found to be correct, the session identifier can be deleted in the transaction server and a decryption of stored, encrypted vehicle features or images is thus no longer possible.

Toll transactions are preferably double-checked in the transaction server by means of map matching between geographical positions of toll beacons, which are stored in the beacon log(s) on the basis of the beacon identifiers thereof, and the position notifications. The geographical positions of the toll beacons are known beforehand highly accurately, and therefore they can be used as reference for the geographic checking of the position

data transmitted in the position notifications of a multi-functional OBU in GNSS mode.

A commercially conventional near-range radio communication standard, such as WLAN, WiFi®, Bluetooth®, RFID (radio frequency identification) or, particularly preferably, NFC (near field communication), is preferably used for the interface in the multi-functional OBU between mobile phone and on-board unit. NFC-enabled mobile phones are becoming increasingly widespread. The advantage of NFC is the extremely short range thereof, which requires a direct swipe of the mobile phone relative to the on-board unit in order to establish a temporary NFC connection. By swiping the mobile phone via the on-board unit, the session identifier can thus be generated, and the start of sessions in the mobile phone and the on-board unit is thus initiated; a second swiping terminates these sessions and transmits the first beacon log from the on-board unit via the mobile phone to the transaction server.

The first beacon log is preferably encrypted cryptographically in the on-board unit and is transmitted in this form to the mobile phone. Applications in the mobile phone can thus be prevented from reading or even manipulating the beacon log as said log is transmitted to the transaction server.

With at least one of the aforementioned steps of transmitting the session identifier, an on-board unit identifier may optionally also be transmitted in each case. The transaction server can thus additionally perform an assignment between session identifier and on-board unit identifier, which facilitates enforcement.

In a second aspect the invention creates a multi-functional OBU in the form of a vehicle-based arrangement for the presented method, comprising:

a mobile phone with a satellite receiver for position determination and a mobile communications module for position notification via a mobile network to a transaction server, and
an on-board unit with a short-range transceiver for radio communication with a toll beacon,

wherein the mobile phone and the on-board unit are configured to exchange a session identifier via a common radio interface, which session identifier is used by the mobile phone in a position notification via the mobile network and is used by the on-board unit in a radio communication with a toll beacon.

Lastly, the invention creates, in a third aspect, a transaction server for the specified method, comprising a first interface to a mobile network and a second interface to a network of geographically distributed toll beacons, wherein the transaction server is configured to double-check position notifications of a mobile phone received via the first interface with beacon logs received via the first and/or second interface, wherein toll beacons passed by the mobile phone are specified in said beacon logs.

Further features and advantages of the method, the multi-functional OBU and the transaction server of the invention will now be described in greater detail on the basis of preferred exemplary embodiments with reference to the accompanying drawings, in which:

Fig. 1 shows a schematic overview of a road toll system with components according to the invention;

Fig. 2 shows a block diagram of a vehicle-based arrangement ("multi-functional OBU") of the road toll system of Fig. 1;

Fig. 3a and 3b show the method of the invention in the form of a sequence diagram; and

Fig. 4 to 6 show position data logs and beacon logs occurring in the method of Fig. 3.

Fig. 1 shows, in compressed form, a road toll system 1, which consists of an infrastructure-bound part 2 and an infrastructureless part 3. By way of example, a vehicle 5 is moving on a road 4 in the road toll system 1 and carries an interoperable multi-functional on-board unit (multi-functional or MF OBU 6, that is to say an OBU operable with both parts 2, 3), also referred to here as a "vehicle-based arrangement".

The infrastructure-bound part 2 of the road toll system 1 comprises a multiplicity of toll beacons (roadside entities) 7 or $RSE_1, RSE_2, \dots$, generally RSE_n , which are distributed over the

network of roads 4 and which each have a short-range transceiver 8 for radio communication 9 with an MF OBU 6 passing the beacon 7, a detector 10 for recording a feature of the vehicle 5 carrying the MF OBU 6, for example a camera for recording a vehicle image, and also an interface 11, which components 8, 10, 11 are all controlled by a local processor 12 with memory 13. The beacons 7 are connected via the interfaces 11 to a central transaction server (or a number of central transaction servers) 14 of the road toll system 1.

Due to the limited range of the radio link 9, a vehicle 5, more specifically the MF OBU 6 thereof, can be localised as it passes a beacon 7 or RSE_n to the respective known location P_n of the beacon, and from this a toll transaction TR recording or billing the location use can be produced for the transaction server 14, whether produced directly in the toll beacon 7 and transmitted to the transaction server via the interface 11 or whether only produced in the transaction server 14 on the basis of the data received from the toll beacon 7.

The transceiver 8 and therefore the radio link 9 have a radio range of at most a few metres, a few tens of metres or a few hundred metres, as is implemented for example by the DSRC (dedicated short range communication), CEN-DSRC, UNI-DSRC, IEEE 802.11p or WAVE (wireless access for vehicular environments) or ITS-G5 standards inclusive of WLAN and Wifi®, Bluetooth® or also active and passive RFID (radio frequency identification) technologies. All of these standards are combined here for the sake of simplicity under the term "DSRC", and part 2 of the road toll system 1 is accordingly also referred to as the DSRC part 2.

For cooperation with the DSRC part 2, the MF OBU 6 according to Fig. 2 comprises a DSRC part 15 (also referred to as "DSRC OBU" or "OBU" for short) with a short-range transceiver 16 for establishing the radio link 9 and a processor 17 controlling this and having a memory 18. In the DSRC part 2 of the road toll system 1, each MF OBU 6 is identified by an OBU identifier OID of the OBU 15, and each toll beacon 7 or RSE_n is identified by a beacon identifier BID_n .

The infrastructureless part 3 of the road toll system 1, as indicated by the name, does not have a dedicated road-side infrastructure, but instead uses an existing mobile network 18 (of which just some base stations are shown by way of representation) and also an existing network of navigation satellites 19 (some shown by way of example). The mobile network 18 (public land mobile network, PLMN) can be of any type known in the field, for example a 3G, 4G or 5G mobile network according to the GSM, UMTS or LTE standards, etc. The satellite network 19 may be any known GNSS (global navigation satellite system), for example a GPS, GLONASS or GALILEO network. The part 3 of the road network 1 is also referred to as the GNSS part 3 for the sake of simplicity.

For cooperation with the GNSS part 3 of the road toll system 1, the MF OBU 6 has a GNSS part 20, which comprises a satellite receiver 21 for receiving 22 position signals of the satellite network 19, a mobile communications module 23 for communication 24 in the mobile network 18, and a processor 25, which controls the components 21, 23 and has a memory 26. With the aid of the satellite receiver 21, the geographical position of the vehicle 5 or of the MF OBU 6 is determined continuously, and from this position data ("position fixes") $p_1, p_2, \dots$, generally p_i , are produced and are transmitted as position notifications $pos_1, pos_2, \dots$, generally pos_i , to the transaction server 14 via the mobile communications module 23 and the mobile network 18. The transaction server 14 can thus produce toll transactions TR from the obtained position notifications pos_i , which toll transactions record or bill the location uses of the vehicle 5. Alternatively, "finished" toll transactions TR are already produced in the MF OBU 6 by the processor 25 from the position data p_i and are transmitted in the form of the position notifications pos_i to the transaction server 14, that is to say the position notifications pos_i may contain both "raw" position data p_i and "finished" toll transactions TR that have already been processed.

According to Fig. 2, the MF OBU 6 is not constructed from a single hardware component part for the purposes discussed in the introduction, but instead an arrangement is composed of two sep-

arate components embodying the GNSS part 20 on the one hand and the DSRC part 15 on the other hand, which can communicate with one another temporarily via an interface 27.

The interface 27 for example is a short-range radio interface according to the standards discussed above for the DSRC interface 9, such as WLAN, WiFi®, Bluetooth® or RFID. The interface 27, however, is preferably a near-range radio interface of extremely short radio range, in particular according to the NFC standard (near-field communication). Such an NFC interface 27 is configured exclusively for the near range, that is to say is limited to a few centimetres or a few tens of centimetres, and therefore the components 20 and 15 of the MF OBU 6 have to be brought into the direct vicinity of one another in order to establish a temporary NFC connection 27 during this period of approach. Such an "approaching" is established for example by a "swiping" of the GNSS part 20 over the DSRC part 15 for the short period of the swiping.

For this purpose, the components 20, 15 each comprise a short-range communication module 28, 29, for example an NFC communication module. Here, it is possible for one of the modules 28, 29 to be formed as a reader or requester and for the other module to be formed as a transponder or responder, for example the module 28 is formed as an RFID reader and the module 29 is formed as an RFID transponder ("tag") or vice versa. All of these variants are summarised here under the terms "NFC connection" and "NFC module". The NFC modules 28, 29 are controlled in the components 20, 15 by the respective processor 25 or 17 respectively.

The GNSS part 20 of the MF OBU 6 can be provided for example by an accordingly programmed and NFC-, RFID- or Bluetooth-enabled mobile phone. The term "mobile phone" here includes any type of communication device that can communicate in the mobile network 18 and is additionally equipped with a short-range communication module 28, for example a wireless phone, Smartphone, Notebook PC or tablet PC, personal digital assistant (PDA), etc. Such a mobile phone generally also has a display and input device 29 for the user, for example a screen with keypad or a touchscreen. The

DSRC part 15 of the MF OBU 6 can in turn be formed by a "conventional" OBU for a DSRC road toll system, which is additionally equipped with a short-range communication module 29.

Fig. 3 to 6 show a method for checking toll transactions in the road toll system 1 with use of the components shown in Fig. 1 and 2. The sequence diagram of Fig. 3 has been divided between Fig. 3a and 3b due to its size. Fig. 3b shows the continuation of Fig. 3a.

Portion (a) of Fig. 3a shows a phase of the method in which an MF OBU 6 first cooperates (in the manner of a conventional DSRC OBU) exclusively with the DSRC part 2 of the road toll system 1. By way of example, two DSRC transactions a_1 , a_2 are illustrated with different toll beacons 7 or RSE_1 , RSE_2 over the journey of the vehicle 5. With each DSRC transaction a_1 , a_2 , a toll beacon 7 asks the MF OBU 6, more specifically the DSRC part 15 thereof, to respond via the radio interface 9, for example with the DSRC message "BST" (beacons service table) 31. The MF OBU 6 then responds, in one or more radio communications 9, with the OBU identifier OID thereof (step 32, illustrated in simplified form), whereupon the toll beacon 7 produces a beacon transaction TR and (immediately or later) transmits this under the beacon identifier BID_n thereof to the transaction server 14 (step 33). The toll beacon 7 may optionally return the beacon identifier BID_n thereof and/or the toll transaction TR to the MF OBU 6 (step 34).

Portion (b) of Fig. 3 shows a phase of the method in which the MF OBU 6 acts as a GNSS OBU in the GNSS part 3 of the road toll system 1, wherein it is controlled or double-checked however by the DSRC part 2 of the road toll system 1. To this end, at the GNSS part 20 (also referred to hereinafter as "mobile phone" (HDY)), the user initiates a first temporary NFC connection 35 via the radio interface 27 to the DSRC part 15 of the MF OBU 6, for example by swiping the mobile phone 20 over the OBU 15 (step 36). The swiping 36 prompts the generation of a unique session identifier ("session ID") SID in the road toll system 1, for example a very large random number, of which the occurrence again in the road toll system 1 is extremely unlikely. The session

identifier SID can be generated in the mobile phone 20 and transmitted via the NFC interface 27 to the OBU 15, or can be generated in the OBU 15 and transmitted via the NFC interface 27 to the mobile phone 20; in any case the session identifier SID is exchanged between the mobile phone 20 and OBU 15 (step 37). The OBU 15 may also optionally transmit the OBU identifier OID thereof to the mobile phone 20.

A session 38 and 39 are now started both in the mobile phone 20 and in the OBU 15 respectively under the session identifier SID.

In step 40, the mobile phone 20 transmits the session identifier SID (optionally also the OBU identifier OID if obtained) via the mobile network 18 to the transaction server 14, which then also opens a session 41 under the session identifier SID.

The further exemplary phases b_1 , b_3 and b_5 in Fig. 3 now show billing phases in which the MF OBU 6 functions as a GNSS OBU and deposits position notifications pos_1 , generated with the aid of the satellite receiver 21 thereof, at the transaction server 14 via the mobile network 18. Here, the position data pos_1 are sent in each case together with the session identifier SID to the transaction server 14, and therefore all of these received position data pos_1 can be assigned to the session identifier SID and can be stored in a position data log $posLog(SID)$ 42 (see also Fig. 4). The OBU identifier OID may optionally also be transmitted in the position notifications pos_1 and then assigned identically in the transaction server 14 to the position data log 42. The position data log 42 can then be used to produce "GNSS-based" toll transactions TR in the transaction server 14, or already contains these toll transactions directly (when the position notifications pos_1 were "finished" toll transactions TR).

In the further phases b_2 and b_4 of the method illustrated by way of example, the MF OBU 6, over the journey thereof, now encounters further toll beacons 7 whilst in GNSS toll mode (b), here by way of example the toll beacons RSE_n and RSE_{n+1} , which are used as follows to check the GNSS-based toll transactions TR.

When an MF OBU 6 when passing a toll beacon 7 is requested to respond (step 31), it then answers in the phases b_2 and b_4 not only with its OBU identifier OID, but also with its current ses-

sion identifier SID (step 43). The toll beacon 7 now knows that GNSS billing is running "in the background" via the GNSS part 3 (sessions 38, 39, 41), and now responds differently compared with phases a_1 and a_2 , where it had not obtained a session identifier SID: It now transmits back its own beacon identifier BID_n in the next step 44 to the matching MF OBU 6, which collects the beacon identifiers BID_n thus received of all beacon passes in a first beacon log $BIDLog1(SID)$ 45. Alternatively or additionally, in a step 46, the toll beacon 7 can transmit the OBU identifier
5
10
OID and/or the session identifier SID of the passing MF OBU 6 together with the beacon identifier BID_n thereof to the transaction server 14, which collects this information in a second beacon log $BIDLog2(SID)$ 47.

In addition, the toll beacon 7 records a feature of the vehicle
15
5 using the detector 10, for example an image PIC_n of the vehicle 5, and stores this in the memory 13 of the toll beacon 7 under the session identifier SID, optionally in a form encrypted with the aid of the session identifier SID. The detector 10 of the toll beacon 7 can record any arbitrary characteristic feature of
20
a vehicle 5, for example the outer form or a part thereof, such as vehicle body, axle number, size, width and/or height, the weight of the vehicle, vehicle registration, for example an image of the registration plate of the vehicle 5, on which the vehicle registration can be read by means of optical image recognition methods (optical character recognition or OCR), etc. In
25
this sense, the detector 10 may be, for example, a laser scanner or radar scanner scanning the form of the vehicle, one or more light barriers, a weight sensor and/or a digital camera or video camera.

The beacon identifiers BID_n of all toll beacons 7 passed by the
30
vehicle 5 during the GNSS billing phase (b) are thus collected in the first beacon log $BIDLog1(SID)$ 45 of the MF OBU 6 and/or in the second beacon log $BIDLog2(SID)$ 47 of the transaction server 14; the passed toll beacons 7 simultaneously produce re-
35
cordings PIC_n of features of the passing vehicles 5.

For the termination of the GNSS billing phase (b), the user now establishes a second temporary NFC connection 48 via the NFC in-

terface 27, for example by a renewed swiping of the mobile phone 20 over the OBU 15 (step 49). The OBU 15 now transmits the accumulated first beacon log $BIDLog1(SID)$ 45 to the mobile phone 20 (step 50) and terminates or concludes the session 39. The mobile
5 phone 20 transmits the obtained first beacon log $BIDLog1(SID)$ 45 in step 51 via the mobile network 18 to the transaction server 14 and likewise terminates a session 38. The session 41 running under the session identifier SID can now also be terminated in the transaction server 14; the session identifier SID is also
10 stored where necessary (see process 41'), as will be described later.

The first beacon log $BIDLog1(SID)$ 45 can be encrypted in the OBU 15 cryptographically before it is transmitted in step 50 to the mobile phone 20 in order to prevent the mobile phone 20, an ap-
15 plication therein or the user from reading or manipulating the data in the beacon log 45. By way of example, the first beacon log 45 can also be provided for this purpose with a cryptographic signature and/or a checksum (hash value), which can then be checked in the transaction server 14 for authenticity and/or in-
20 tegrity. The encryption of the first beacon log 45 can be performed for example with the aid of a public/private key method, of which the private key is used in the OBU 15 for encryption and of which the public key is used in the transaction server 14 for decryption.

25 Following termination of the GNSS billing phase (b), the MF OBU 6 and then the beacons 7 passed thereby revert back to the DSRC billing mode (a); see the exemplary beacon pass a_{n+2} with steps 31 to 34.

In a subsequent validation phase (c) of the method, the transac-
30 tion server 14 now has both the toll transactions TR produced or caused by an MF OBU 6 in the GNSS billing phase (b) in the form of the position data log $posLog(SID)$ 42, whether this contains "raw" position data p_1 or "finished" toll transactions TR , and also the first beacon log $BIDLog1(SID)$ 45, which was collected
35 by the MF OBU 6 in this phase on the basis of the beacon passes b_3, b_4 . In a validation or double-checking step 52, the toll transactions TR or $posLog(SID)$ produced for a session identifier

SID can thus be double-checked against or compared with the first beacon log BIDLog1(SID) 45 received under the same session identifier SID in order to detect mismatches. Such a mismatch may be caused for example by the fact that the journey of the vehicle 5 specified by the position data log posLog(SID) 42 or the toll transactions TR based thereon or contained therein does not match with the locations P_n of the toll beacons 7 specified in the first beacon log BIDLog1(SID) or vice versa. For example, this indicates a malfunction of the road toll system 1 or fraudulent manipulation at the MF OBU 6.

Alternatively or additionally, a further double check can be performed with the MF OBU passes signalled by the toll beacons 7, these passes being collected with reference to the respective session identifier SID in the form of the second beacon log BIDLog2(SID) 47. The second beacon log BIDLog2(SID) 47 can be double-checked here against the first beacon log BIDLog1(SID) 45 and/or the position data log posLog(SID) 42 or the toll transactions TR.

The double check step 42 can be, for example a map matching between the journeys of the vehicle 5 in the toll road system 1 indicated by the various logs 42, 45, 47 with the previously known locations P_n of the toll beacons 7 or RSE_n , for example with the aid of digital road maps, which contain possible journeys for vehicles 5 and the locations P_n of the toll beacons 7.

It goes without saying that the beacon logs 45, 47 may also each contain only compressed details of the passed toll beacons 7, for example a hash value of the beacon identifiers BID_n of the passed toll beacons 7. The transaction server 7 can then calculate a comparison hash value from the beacon identifiers BID_n known thereto of those toll beacons 7 that must have been passed by the multi-functional OBU 6 on the journey thereof specified in accordance with the position data posLog(SID) 42 and can then compare this value with the hash value(s) specified in the beacon log(s) 45, 47 in order to detect mismatches. Such compressed (hashed) beacon logs 45, 47, which no longer contain the beacon identifiers BID_n in plain text, but for example only still in the

form of a hash value or a checksum, also fall within the term "beacon log" used here.

In the case of a mismatch, the transaction server 14 may request from the corresponding toll beacon 7 or RSE_n , in a (optional) step 53, the vehicle feature PIC_n recorded in said toll beacon in the memory 13 under the session identifier SID, for example an image of the vehicle 5, and may recover this (step 54). If the vehicle feature PIC_n has been encrypted with the session identifier SID, the session identifier SID is to be stored up until this moment in the transaction server 14 (see process 41') in order to be used for decryption of the vehicle feature PIC_n . Session identifiers SID for toll transactions TR, which were found to be in order in step 52, can be deleted (even as early as step 52) in order to prevent a further decryption of the stored vehicle features PIC_n of "correct" vehicles.

In a step 55, an enforcement dataset REC is produced, which contains the detected mismatch in conjunction with the determined vehicle feature PIC_n and also the session identifier SID and/or the OBU identifier OID (when the latter is also transmitted and has been assigned the session identifier SID). If the OBU identifier OID in the transaction server 14 is not available at this point, the enforcement dataset REC may also contain just the session identifier SID.

It goes without saying that an MF OBU 6, which transmits position notifications pos_i to the transaction server 14 via the mobile network 18 in the GNSS billing phase (b), can also transmit in each case a subscriber identifier TID of the mobile phone 20 in the mobile network 18, for example an IMSI (international mobile subscriber identification), TIMSI (temporary international mobile subscriber identification, IMEI (international mobile equipment identifier) or the like, on the basis of which a GNSS-based toll transaction TR can be attributed to a billing account in the mobile network 18. For exclusively GNSS-based toll transactions TR, the assignment of the session identifier SID and/or the OBU identifier OID to the subscriber identifier TID therefore is not absolutely necessary, but is optional.

The invention is not limited to the presented embodiments, but also comprises all variants and modifications that fall within the scope of the accompanying claims.

FREMANGSMÅDE TIL EFTERPRØVNING AF GEBYRTRANSAKTIONER OG KOMPONENTER HERTIL

Patentkrav

1. Fremgangsmåde til efterprøvning af gebyrtransaktioner, som dannes af
5 positionsmeldinger for en mobiltelefon (20), der via et mobilnet (18) står i forbindelse med en transaktionsserver (14), ved hjælp af et netværk af fordelte gebyrradiofyre (7), som via korttrækkende radio (9) kan kommunikere med onboard-enheder (15) i forbipasserende køretøjer (5) og stå i forbindelse med transaktionsserveren (14), omfattende:
10 medbringning af en mobiltelefon (20) og en onboard-enhed (15) i et køretøj (5);
generering af en sessionsidentifikation (SID), udveksling af sessionsidentifikationen (SID) mellem mobiltelefonen (20) og onboard-enheden (15) og afsendelse af sessionsidentifikationen (SID) til transaktionsserveren (14);
frembringelse af positionsmeldinger (pos_i) i mobiltelefonen (20) og afsendelse af
15 positionsmeldingerne (pos_i) under sessionsidentifikationen (SID) til transaktionsserveren (14) til frembringelse af gebyrtransaktioner (TR);
når onboard-enheden (15) passerer et gebyrradiofyre (7), registrering af passagen i en radiofyrsprotokol (45, 47) under sessionsidentifikationen (SID); og
i transaktionsserveren (14), krydskontrol mellem de til sessionsidentifikationen (SID)
20 frembragte gebyrtransaktioner (TR) og den til sessionsidentifikationen (SID) oprettede radiofyrsprotokol (45, 47)
2. Fremgangsmåde ifølge krav 1, kendetegnet ved, at der ved passage af et gebyrradiofyre (7) sendes en radiofyrsidentifikation (BID_n) fra gebyrradiofyret (7) til onboard-enheden (15) og lagres i en første radiofyrsprotokol (45) i onboard-enheden
25 (15); og at
den første radiofyrsprotokol (45) sendes med sessionsidentifikationen (SID) over mobiltelefonen (20) til transaktionsserveren (14) til krydskontrol.
3. Fremgangsmåde ifølge krav 1 eller 2, kendetegnet ved, at ved passage af et gebyrradiofyre (7) sendes sessionsidentifikationen (SID) fra onboard-enheden (15) til
30 gebyrradiofyret (7) og derfra med en radiofyrsidentifikation (BID_n) til transaktionsserveren (14); og at
i transaktionsserveren (14) lagres alle til sessionsidentifikationen (SID) modtagne radiofyrsidentifikationer (BID_n) i en anden radiofyrsprotokol (47).

4. Fremgangsmåde ifølge krav 2 og 3, kendetegnet ved, at ved krydskontrollen krydskontrolleres også den anden radiofyrspkoll (47) mod den første radiofyrspkoll (45).
5. Fremgangsmåde ifølge ét af kravene 1 til 4, omfattende:
- 5 ved passage af gebyrradiofyret (7): registrering af et køretøjskendetegn (PIC_n) ved anvendelse af en detektor (10) i gebyrradiofyret (7) og lagring af køretøjskendetegnet (PIC_n) under sessionsidentifikationen (SID) i gebyrradiofyret (7); og, når krydskontrollen i transaktionsserveren (14) viser en uoverensstemmelse, afsendelse af det lagrede køretøjskendetegn (PIC_n) fra gebyrradiofyret (7) til transaktionsserveren
- 10 (14).
6. Fremgangsmåde ifølge krav 5, kendetegnet ved, at køretøjskendetegnet (PIC_n) lagres krypteret ved hjælp af sessionsidentifikationen (SID).
7. Fremgangsmåde ifølge ét af kravene 1 til 6, kendetegnet ved, at krydskontrollen sker ved en kortsammenligning mellem geografiske positioner (P_n) af gebyrradiofyrene
- 15 (7), der er lagret i den eller de radiofyrspkoller (45, 47) baseret på deres radiofyrsidefikatorer (BID_n) og positionsmeldingerne (pos_i).
8. Fremgangsmåde ifølge ét af kravene 1 til 7, kendetegnet ved, at genereringen af sessionsidentifikationen (SID) og afsendelsen af den første radiofyrspkoll (45) i hvert tilfælde sker over en midlertidig nærområdeforbindelse (27), fortrinsvis en NFC-
- 20 forbindelse, mellem mobiltelefon (20) og onboard-enhed (15).
9. Fremgangsmåde ifølge ét af kravene 2 til 8, kendetegnet ved, at den første radiofyrspkoll (45) krypteres i onboard-enheden (15) og sendes i denne form til mobiltelefonen (20).
10. Fremgangsmåde ifølge ét af kravene 1 til 9, kendetegnet ved, at der ved mindst ét
- 25 af de nævnte trin med afsendelse af sessionsidentifikationen (SID) hver gang også medsendes en onboard-enhedsidentifikation (OID) af onboard-enheden (15).
11. Køretøjsbaseret indretning til en fremgangsmåde ifølge ét af kravene 1 til 10, omfattende:
- en mobiltelefon (20) med en satellitmodtager (21) til positionsbestemmelse og et
- 30 mobilradiomodul (23) til positionsmelding via et mobilnet (18) til en transaktionsserver (14), og
- en onboard-enhed (15) med en kortrækkende transceiver (16) til radiokommunikation med et gebyrradiofyr (7),
- hvor mobiltelefonen (20) og onboard-enheden (15) er indrettet til, via en fælles
- 35 radiogrænseflade (27), at udveksle en sessionsidentifikation (SID), som mobiltelefonen

(20) anvender i en positionsmelding (24) over mobilnettet (18), og onboard-enheden anvender i en radiokommunikation (9) med et radiofyr (7).

12. Køretøjsbaseret indretning ifølge krav 11, kendetegnet ved, at radiogrænsefladen (27) er en NFC-grænseflade til midlertidige NFC-forbindelser.

5 13. Køretøjsbaseret indretning ifølge krav 11 eller 12, kendetegnet ved, at onboard-enheden (15) er indrettet til modtagelse af en radiofyrsideidentifikation (BID_n) fra et gebyrradiofyr (7) og lagring i en første radiofyrsprotokol (45).

10 14. Køretøjsbaseret indretning ifølge krav 13, kendetegnet ved, at onboard-enheden (15) er indrettet til at sende den første radiofyrsprotokol (45) via den fælles radiogrænseflade (27) til mobiltelefonen (20), og at mobiltelefonen (20) er indrettet til at sende en modtaget første radiofyrsprotokol (45) via mobilnettet (18) til transaktionsserveren (14).

15 15. Transaktionsserver til en fremgangsmåde ifølge ét af kravene 1 til 10, med en første grænseflade til et mobilnet (18) og en anden grænseflade til et net af geografisk fordelte gebyrradiofyr (7), hvor transaktionsserveren (14) er indrettet til at krydskontrollere via den første grænseflade modtagne positionsmeldinger (pos_i) vedrørende en mobiltelefon (20) med via den første og/eller anden grænseflade modtagne radiofyrsprotokoller (45, 47), hvori der er angivet gebyrradiofyr (7), som er passeret af mobiltelefonen (20).

20 16. Transaktionsserver ifølge krav 15, kendetegnet ved, at transaktionsserveren (14) er indrettet til ved forekomst af en ved krydskontrollen optrædende uoverensstemmelse at anmode om ét i et gebyrradiofyr (7) lagret køretøjskendetegn (PIC_n) via den anden grænseflade.

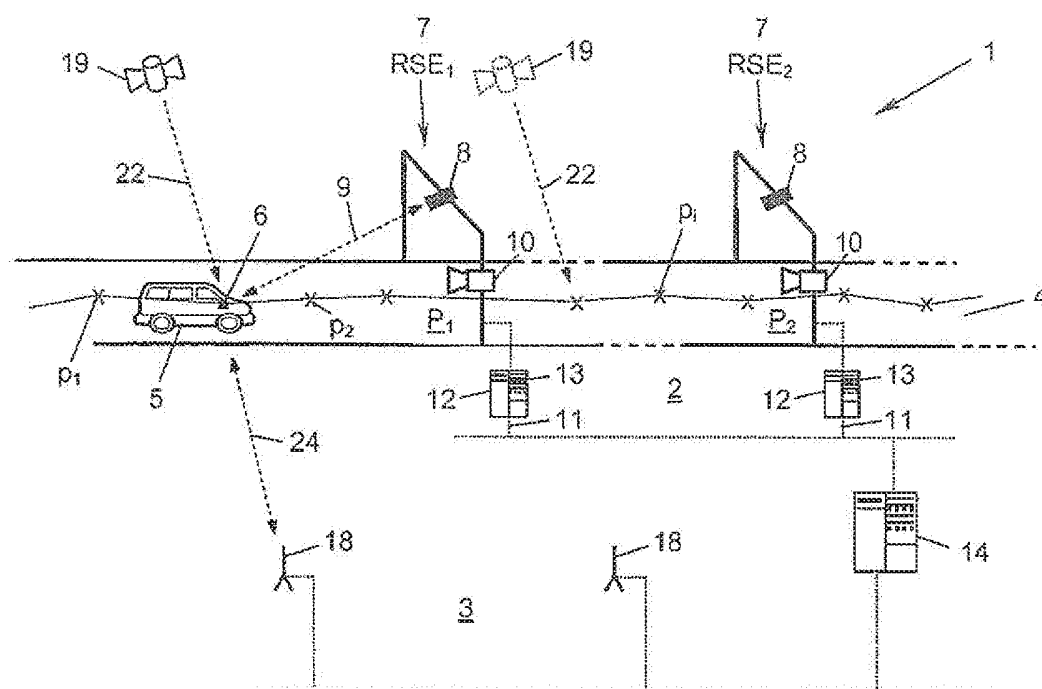


Fig. 1

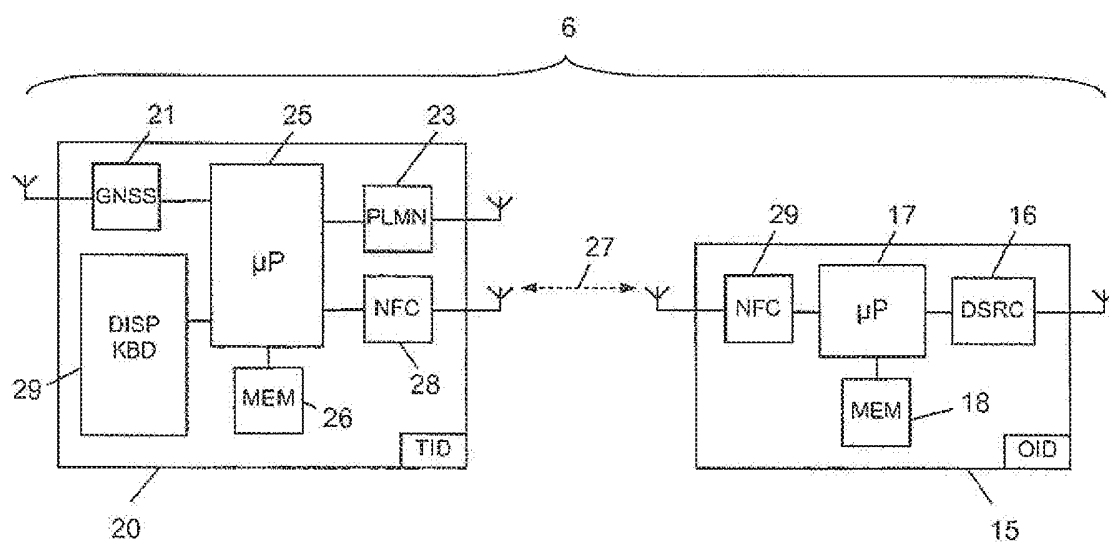


Fig. 2

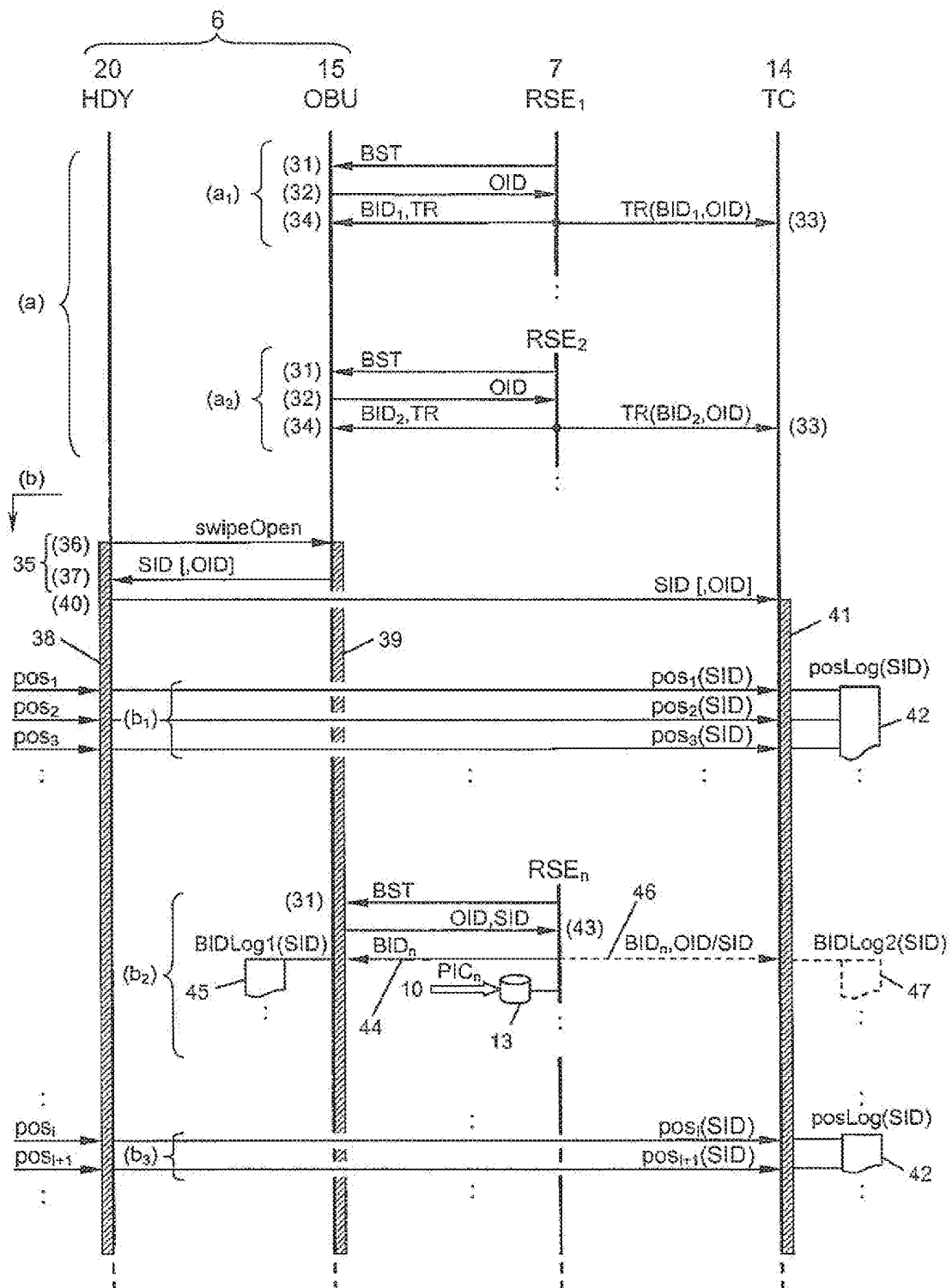


Fig. 3a

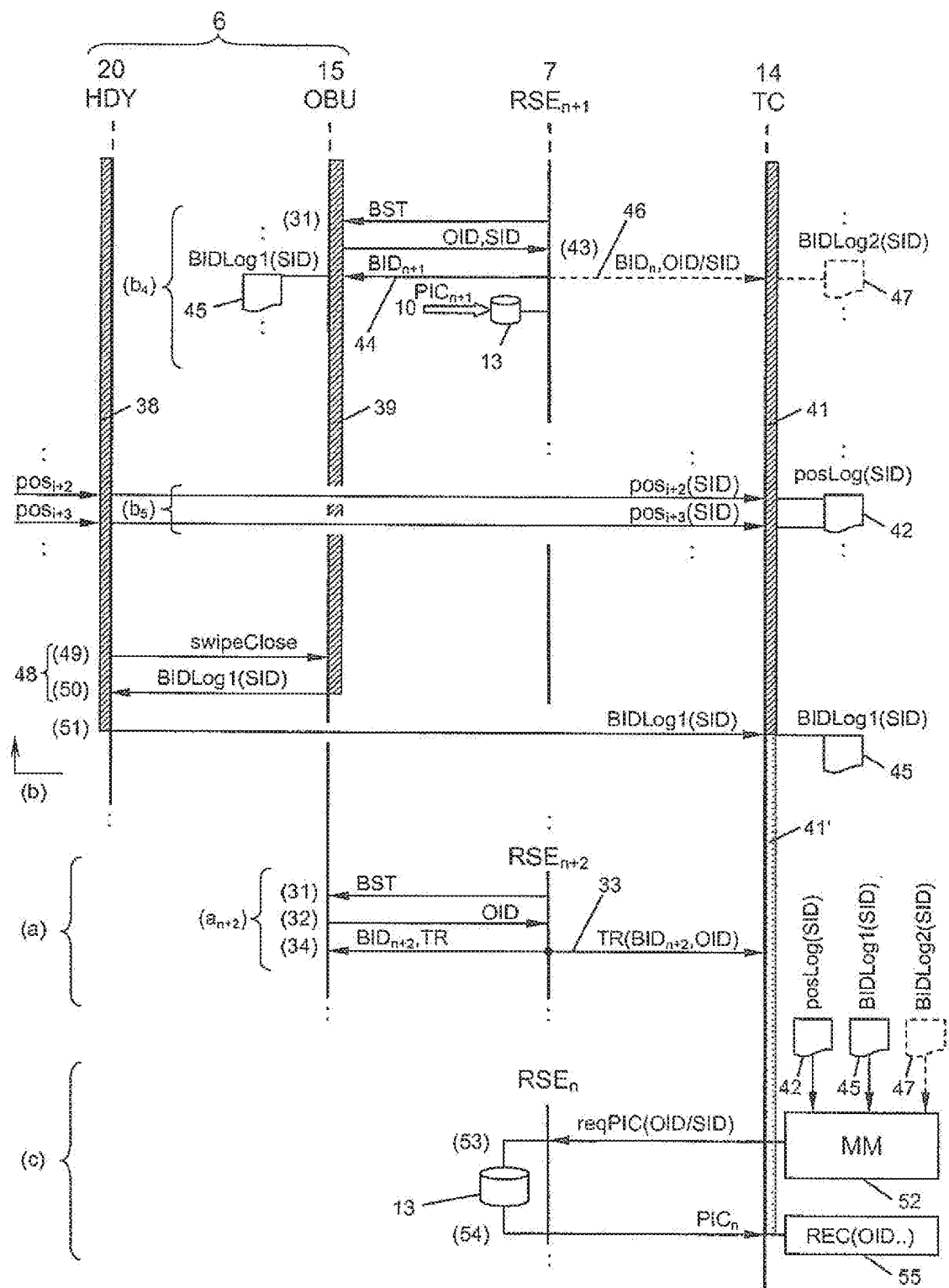


Fig. 3b

posLog(SID)	
SID	pos ₁
	pos ₂
	⋮
	pos _i
	⋮

42

Fig. 4

BIDlog1(SID)	
SID	BID ₁
	BID ₂
	⋮
	BID _n
	⋮

45

Fig. 5

BIDLog2(SID)	
BID _n	OID ₁ /SID ₁
	OID ₂ /SID ₂
	⋮
	OID _i /SID _i
	⋮

47

Fig. 6