(51) International Patent Classification:
G07B 15/06 (2011.01)  G07C 5/00 (2006.01)

(21) International Application Number:
PCT/EP2012/055772

(22) International Filing Date:
30 March 2012 (30.03.2012)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
1105385.7 30 March 2011 (30.03.2011) GB

(71) Applicant (for all designated States except US): ACT WIRELESS LTD [GB/GB]; 39 Holywood Road, Belfast Antrim BT4 3BA (GB).

(72) Inventors and
Inventors/Applicants (for US only): SCANLON, William [GB/GB]; 33 Kilton Lane, Islandmagee, Larne Antrim BT40 3TA (GB). McQUISTON, Johnathan [GB/GB]; 53 Farm Lodge Park, Greenland Antrim BT38 8YB (GB).

COTTON, Simon [GB/GB]; 1 Farm Lodge Park, Greenland Antrim BT38 8YB (GB).

(74) Agent: WALLACE, Alan; FRKelly, 4 Mount Charles, Belfast Antrim BT7 1NZ (GB).


Published:
— with international search report (Art. 21(3))

(54) Title: VEHICLE USAGE VERIFICATION SYSTEM

FIG. 2

10

14A

34

14B

map

40

(57) Abstract: A computer-implemented system for verifying vehicle usage comprising a server capable of communication with a plurality of clients across a communications network. Each client is provided in a respective vehicle and with a respective global positioning system (GPS) by which the client can determine the location of the respective vehicle. A first of the clients sends a token to a second of the clients when the respective vehicles are within a valid range of one another. One or both of the first and second clients modifies the token to include information dependent on the location of one or both of the vehicles when the token is exchanged. The modified token is returned to the server which extracts the location dependent information from the modified token. This allows validation of the returned token. Validated tokens can be used in the assessment of vehicle usage and toll calculation. The system can offer a high level of privacy to users as well as being robust against fraudulent use.
Vehicle Usage Verification System

Field of the Invention

The present invention relates to systems for verifying vehicle usage. The invention relates particularly, but not exclusively, to toll systems for roads.

Background to the Invention

Governments in developed countries are keen to tackle road congestion, raise revenue for infrastructure development and offer fairness in taxation by using "per-mile" road tolling (so called, "pay as you drive"). High resolution tracking technology is already ubiquitous with GPS-enabled smartphones, personal and in-car satellite navigation systems. Commercial fleet operators are routinely managing both employees and their services through live vehicle tracking. One barrier to full end-user (the everyday motorist) implementation of per-mile road tolling is privacy. Another problem is the potential for fraudulent behaviour.

It would be desirable to provide a secure toll system that provides end-user privacy. It would also be desirable to provide a system supporting usage validation that allows the operator to identify potential fraud and to thus intelligently target their enforcement resources. Advantageously, such systems should require relatively little infrastructure to implement.

Summary of the Invention

A first aspect of the invention provides a computer-implemented system for verifying vehicle usage comprising a server capable of communication with a plurality of clients across a communications network, each client being provided in a respective vehicle and being co-operable with a respective global positioning system by which the client can determine the location of the respective vehicle,

wherein a first of said clients is arranged to communicate to a second of said clients at least one computer usable token when the respective vehicles are within a valid range of one another,

one or both of said first and second clients being arranged to modify said at least one token to include information dependent on the location of one or both of said vehicles substantially when said at least one token is communicated between the clients,
and wherein one or both of said first and second clients is arranged to communicate said at least one token to said server, said server being arranged to extract said location dependent information from said at least one token.

In a preferred embodiment, the system comprises a toll system for verifying vehicle usage for the purpose of calculating tolls. The extracted location dependent information may be used, conveniently by the server, to calculate a toll payable by the user of the second client’s vehicle.

The location dependent information optionally comprises information indicating a road type, wherein the road type may be one of a plurality of road types supported by the system. Each road type may be associated with a respective toll. The road type included in said at least one token is determined by the location of one or both of the respective vehicles, preferably at least by the location of said second vehicle, when said at least one token is communicated between the clients. It is noted that this may not be precisely at the time of token transfer but is approximately at the same time. To determine road types, each client may have access to a computer usable map that links global positions to road types.

The location dependent information preferably comprises information from which the relative distance between the first and second vehicles at the time of token exchange can be assessed, for example to determine whether or not the vehicles are deemed to have been sufficiently close to one another (e.g. at substantially the same location or within a threshold distance) at the time of token exchange. This may be achieved by including information determined by the respective location of each vehicle involved in the token exchange. For example, respective location information for each vehicle may be determined from the global position of the vehicle. Preferably, an approximation of the precise global position is used for this purpose. The location information may comprise an indication of, or reference to, a location on a map, especially a computer usable map.

Preferably, data identifying a grid location (e.g. a grid reference), and especially a coarse grid location, may be used for this purpose.

Preferably, the location information is encoded (or otherwise transformed, preferably irreversibly, using a mathematical function or other function, e.g. a hash function or other one-way function, typically a mathematical function) to conceal the true location of each vehicle, e.g. by performing a hash function on the respective location data and incorporating the results into the modified token. Conveniently, the server may validate
location dependent information by performing a comparison between the respective hash values (or result of any other function/transformation that may alternatively be performed) of the modified token, in particular in respect of the location of each vehicle when the token was transferred. Hence, the token may be used to cross validate the location dependent information but without disclosing the location itself to the server (e.g. billing system).

The first client may be arranged to determine a road type associated with the location of its respective vehicle, and to determine if its determined road type matches the determined road type associated with the vehicle of the second client, and to incorporate into said at least one token information indicating whether or not the road types match.

In preferred embodiments, at least some and preferably all of said clients are arranged to act as said first client or said second client.

Conveniently, said server is arranged to distribute tokens to at least some of said clients, and preferably also to generate said tokens. In the preferred embodiment, said server distributes at least one original token, said at least one original token being modified by one or both of said first and second clients as part of an exchange of said at least one token from said first client to said second client. Preferably, modified tokens include the respective unmodified token combined with said location dependent information and, optionally, said road type match information.

Advantageously, at least said location dependent information is encoded in said modified token, e.g. by performing a hash function on said location dependent information, conveniently with the respective original token, and including the result of the hash, or other encoding, into the modified token.

A second aspect of the invention provides a client for use in the system of the first aspect of the invention, said client being arranged to act as either or both of said first and second clients.

A third aspect of the invention provides a computer-implemented method of determining road usage, or vehicle usage, in a computer-implemented system comprising a server capable of communication with a plurality of clients across a communications network, each client being provided in a respective vehicle and being co-operative with a
respective global positioning system by which the client can determine the location of the respective vehicle, the method comprising:

communicating from a first of said clients to a second of said clients at least one computer usable token when the respective vehicles are within a valid range of one another,

modifying said at least one token to include information dependent on the location of one or both of said vehicles when said at least one token is communicated between the clients,

communicating said at least one token to said server, and

extracting said location dependent information from said at least one token.

Said location dependent information may be said to comprise validation information. Advantageously, the token may be used to cross validate the location dependent information but without disclosing the location itself to the server (billing system).

Preferred embodiments of the invention provide a GPS-based infrastructure-less road tolling system, or other vehicle usage verification system, offering relatively high levels of consumer privacy while simultaneously providing relatively low risk of fraudulent use to the system operator. The preferred system allows finely detailed “per-mile” billing or taxation for vehicles based on updatable maps while giving the consumer the reassurance that exact routes or details of journeys are never stored or transmitted to the system operator or any other party.

Typically, systems embodying the invention combine telematics technology such as GPS, cellular connectivity and embedded systems with the concept of vehicle to vehicle communications (V2V), together with secure electronic transaction technology.

In preferred embodiments, time-limited, digitally-secured tokens are distributed by the system to vehicles during interactions with at a base, e.g. home, location (so that privacy is not breached). The tokens are then passed to other vehicles as they encounter each other and used to validate the position of the vehicles so that fraud can be readily detected.

The system may distribute a fixed number of tokens per day (or other period) in a certain (geographical) area. The tokens are preferably processed a one-way function with a location indicator in a way that does not give away the location of the vehicles, or at least the token-receiving vehicle, when the token exchange took place. Accordingly, the
transaction of the system passing a token to a first vehicle (which may be referred to as the ‘carrier’ or ‘distributor’ of the token) is known and verifiable (as is, preferably also, the carrier’s use of the token). However, when the carrier vehicle encounters a second vehicle (which may be referred to as the ‘recipient’ of the token, or as the ‘anonymous’ vehicle) during any of its journeys, the token, along with a cross-verification of both vehicles’ GPS positions may be used to produce a hash (typically comprising a one way function), which may be appended to the recipient’s billing data. The network operator expects a certain minimum number of verified hash data (since it knows how many tokens were given out then used in a certain region) for each recipient.

Advantages of the preferred system include: it can be implemented without building any new roadside structures; end-user privacy is provided, with no individually identifiable journeys being recorded or transmitted; not susceptible to denial of service attacks such as blocking of GPS or cellular connectivity; immunity to highly sophisticated (and expensive) fraud such as GPS spoofing (tricking the GPS receiver into recording a different route); updatable route-pricing maps, for example to change the category of an individual road for certain times of the day; technology independent – the system is not dependent on particular aspects of the cellular network or the GPS system and could be implemented on a range of telematics platforms or in any country provided that there is sufficient cellular connectivity and access to satellite navigation. Furthermore, the charging organisation could, without loss of consumer privacy, distribute tokens from fixed infrastructure points (typically close to higher value roads) to mitigate against extensive GPS unavailability or in sparse deployments where the number of client vehicles is insufficient to ensure sufficient validation points.

Advantages of the preferred system include that it is secure and cannot easily be defrauded, it offers privacy to users and, with the vehicle-to-vehicle token distribution, it can be wholly or substantially infrastructure less.

The invention is not limited to use with toll systems and may be applied to other tasks, e.g. verifying or monitoring vehicle usage for the purposes of insurance.

Other preferred features are recited in the dependent claims, and further advantageous features of the invention will be apparent to those ordinarily skilled in the art upon review of the following description of a specific embodiment and with reference to the accompanying drawings.
Brief Description of the Drawings

An embodiment of the invention is now described by way of example and with reference to the accompanying drawings in which:

Figure 1 is a schematic view of a toll system embodying the invention, the system being shown implementing a token distribution phase of operation;

Figure 2 is a schematic view of the system of Figure 1, the system being shown implementing a location validation phase of operation;

Figure 3 is a schematic view of the system of Figure 1, the system being shown implementing a cost calculation phase of operation;

Figure 4 is a schematic representation of a token passing method suitable for use in systems embodying the invention;

Figure 5 is a schematic representation of token structures suitable for use with systems embodying the invention;

Figure 6 is a schematic representation of alternative token structures suitable for use with systems embodying the invention; and

Figure 7 is a schematic representation of further alternative token structures suitable for use with systems embodying the invention.

Detailed Description of the Drawings

Referring now to Figure 1 of the drawings there is shown, generally indicated as 10, a system embodying the invention. For the purposes of example, the system 10 comprises a toll system for determining vehicle usage. The toll system 10 is particularly intended for charging vehicle owners for use of roads according to a toll schedule. Respective tolls, or toll rates, may be applied for different road types, e.g. A roads, B roads or motorways, and/or for specific roads or road features (e.g. bridges or tunnels), for specific users or types of users and/or for different times of day or year. The toll schedule provides for a cost per unit distance. Alternatively, a flat toll may be applied for use of a specific road, road feature, or part thereof. The preferred system 10 employs telematics for
communication between its component parts and so may be referred to as a telematic toll system 10.

The system 10 comprises a server 12 configured for communication with a plurality of vehicles 14 (only one shown in Figure 1) via a communications network 16. The vehicles 14 are configured for communication with a global positioning system (GPS) in order that each vehicle 14 may determine its global position. To this end, each vehicle 14 includes a GPS receiver 20, or other GPS locating unit (not shown), for communication with the GPS system (represented by a single GPS satellite 18, although in practice multiple satellites are used).

The server 12 comprises a suitably programmed computer system that may take any suitable form, i.e. may comprise one or more computers running one or more computer programs, and any other hardware and/or software that may be required, the components of which may be co-located or distributed. In the drawings, the server 12 is represented for convenience as comprising two systems, namely a billing system 12A and a token management system 12B.

The network 16 may comprise any suitable communications network, e.g. a data network (e.g. comprising home broadband and/or WiFi) and/or a telephone network (e.g. PSTN and/or cellular), as is convenient.

Each vehicle 14 is equipped not only with a GPS locating unit, but also with a client device 22, preferably in the form of a telematics device, configured to communicate with the server 12 across the network 16. The client 22 is also in communication with the respective GPS receiver 20 so that it may obtain global position data for the respective vehicle 14 during use. The client 22 may take any suitable form, typically comprising a suitably programmed computing device, and including, or being co-operable with, a transceiver unit 24 for sending and receiving data via the network 16, and for communication with other vehicles.

The transceiver 24 typically comprises at least a cellular telephone network transceiver, e.g. a GSM transceiver. Alternatively, or in addition, the transceiver may comprise one or more other wireless transceivers, such as a WiFi transceiver and/or a Bluetooth transceiver, for communication with a base station (not shown) and/or with other vehicles 14 that are part of the system 10. For example, the base station may comprise a wireless hub at the vehicle owner’s home (not shown), with which the transceiver 24 may
communicate wirelessly via a WiFi or other suitable transceiver, e.g. as part of a wireless LAN. The wireless hub may be connected to the network 16, e.g. via the PSTN or other domestic telephone/data network. The client 22 may therefore communicate with the server 12 via the base station. For communication with other vehicles 14, and more particularly with the respective client device 22 of other vehicles, the transceiver 24 supports any suitable wireless communication technology that allows the respective client 22 to broadcast signals to correspondingly equipped clients 22, and to detect and respond to broadcast signals. WiFi Dedicated Short Range Communication (DSRC), Bluetooth or proprietary ISM-band communication are examples of suitable wireless technologies.

The system 10 is configured to distribute computer usable tokens 30 to the vehicles 14, and to collect modified versions of the tokens. A distributed token (D-token) is received from the server 12 (in this case the token management server 12B) by a first vehicle 14 and communicated to a second vehicle 14 when the two vehicles are within a suitable range of one another. The communicated token is modified by the client device 22 of the first and/or second vehicle 14 depending on the GPS position of at least one of the first and second vehicles 14 at the time the token is exchanged. Preferably, the token is modified to include information from which the relative distance between the first and second vehicles at the time of token exchange can be assessed or derived, for example to determine whether or not the vehicles are deemed to have been sufficiently close to one another (e.g. at substantially the same location or within a threshold distance) at the time of token exchange. This may be achieved by including information determined by the respective location of each vehicle involved in the exchange. Preferably, the location information is encoded, or otherwise transformed using a suitable (preferably non-reversible) transformation function, to conceal the true location, e.g. by performing a hash function on the respective location data and incorporating the results into the modified token. Advantageously, the location data is determined from a relatively coarse grid map and may take the form of a grid reference, or other map reference. For example, the location may be determined by the GPS position of the, or each, of the first and second vehicles 14 in conjunction with a computer usable road map 40 that correlates GPS positions with map locations, preferably coarse map locations. The road map may be stored locally to the client device 22, or may be otherwise available to the client device 22, e.g. from a remote computer or data storage device (not shown) via the network 16 or other network, for example the internet.
The distributed token is preferably also modified by the client device 22 of the first and/or second vehicle 14 to include information indicative of a road type determined in use by one or both of the respective client devices 22. The road type may be determined by the GPS position of the, or each, of the first and second vehicles 14 in conjunction with a computer usable road map that correlates GPS positions with road types. The road map 40 conveniently is configured for this purpose. For a given accounting period, each vehicle 14 communicates to the server 12 the modified tokens that it has collected during the accounting period, together with data representing the journey(s) undertaken by the vehicle during the accounting period. The server 12 uses the journey data to calculate a bill for the vehicle 14, and uses the respective modified token(s) to verify the journey data.

The tokens 30 may take any convenient form. In preferred embodiments, each token comprises a respective computer readable code, each code preferably being unique. More generally, a token may comprise any wirelessly transmittable digital data, e.g. a digital certificate, code, ID or other digital data. The tokens 30 are conveniently generated by the server 12, in particular the token management server 12B, typically using a pseudo-random code generator (not shown). Advantageously, each code is encrypted such that only the server 12 is capable of decrypting tokens that are collected from the vehicles. For example, a public key cryptography system may be used in which the token management server 12B uses a private, or secret, encryption key to encrypt the tokens 30 before they are distributed to the vehicles. The vehicle clients 22 may use a public encryption key to process the tokens 30, including where necessary further encrypting the tokens. The token management server 12B uses the private key to decrypt tokens collected from the vehicles.

Preferably, for the prevention of fraud, the tokens 30 are configured to expire, e.g. after a given date and/or time, or a period of time after they are created by the server or distributed to a vehicle. This may be achieved by any suitable means, typically involving generating a code for the token that has a time dependent aspect. For example, the token may comprise a code that includes an expiry component from which at least the token management server 12B and optionally also the clients 22 can determine whether or not the token has expired. For example, the expiry component that is indicative of time and/or date. Alternatively, or in addition, the code may be generated using a key, for example comprising a generation code or a mathematical function, that changes periodically. Subsequent processing of the token can be performed by the clients 22 and/or the server 12 to determine which key was used to generated the code, or at least
whether or not the code was generated by a current key, thus allowing the clients 22 
and/or the server 12 to determine if the token has expired.

Figure 1 illustrates a token distribution phase of the preferred system’s operation. The 
token management server 12B communicates via network 16 at least one, but preferably 
a plurality of tokens 30 to the client 22 at least some vehicles 14, and optionally each 
vehicle 14, of the system 10. Alternatively, or in addition, the tokens 30 may be 
generated and/or distributed to vehicles 14 by one or more other system components (not 
shown), e.g. road side stations. Advantageously, each vehicle 14 is provided with a 
respective set of one or more tokens that are different from the token(s) provided to other 
vehicles 14. It is preferred that the server 12B distributes a finite number of tokens to 
each vehicle client 22. This allows the server 12B to monitor token usage as is described 
in more detail hereinafter. Each vehicle client 22 stores the received tokens in local 
memory for distribution to other vehicle clients 22, as is described in more detail with 
reference to Figure 2. In a simpler embodiment, vehicle clients 22 may be provided with 
a single token for passing to other vehicles, although this is considered to be less secure 
than the preferred embodiment.

In preferred embodiments, the distribution of tokens 30 to vehicles 14 is performed at a 
respective base location for each vehicle. Conveniently, the system 10 determines if the 
vehicle 14 is in its base location by the current GPS position of the vehicle 14. For 
example, the vehicle client 22, upon determining that the vehicle 14 is at its base location 
using the GPS receiver 20, initiates communication with the server 12 via network 16. 
The server 12B may transmit tokens to the vehicle client 22 depending on any suitable 
criteria, e.g. depending on how many valid tokens are already in circulation in the system 
10 and/or how many valid tokens the vehicle 14 already has. Alternatively, the server 12 
may automatically send one or more tokens to the vehicle 14 upon request. 
Conveniently, communication between the server 12 and the client 22 is established 
automatically, i.e. without user initiation, when the vehicle 14 is at its base location.

Optionally, communication between the server 12 and the client 22 is established only at 
specific times, e.g. at the end of an accounting period. Most conveniently, the base 
location is the home location for the vehicle 14.

While communication is established between the server 12 and the client 22 (before 
during or after the distribution of tokens 30), the vehicle client 22 conveniently transmits to 
the server 12, and in particular the billing system server 12A, via network 16 data relating 
to one or more journeys undertaken by the vehicle 14, and/or data relating to tokens that
it has distributed to other vehicles, as is described in more detail hereinafter with reference to Figure 3.

In alternative embodiments, communication between the server 12 and the client 22 may be established at any time and at any location, and/or may be user initiated or automatic. For example, the communication may be established automatically at the end of an accounting period irrespective of the vehicle’s location. It is preferred, however, for vehicles 14 to communicate with the server 12 only when at the respective base location in order to increase the privacy offered by the system 10.

Figure 2 illustrates a positional validation phase of the preferred system’s operation, in which tokens are exchanged between vehicles 14. During a journey, a first vehicle 14A having one or more tokens 30 received from the server 12 advertises to other vehicles (represented by a second vehicle 14B) that it has tokens for distribution. This may be achieved by any suitable means. For example the client 22 of the first vehicle 14A may broadcast a signal using its transceiver 24, which signal indicates the availability of one or more tokens. The client 22 of the, or each, second vehicle 14B is configured to detect the broadcast signal via its own transceiver 24. Should the client 22 of the second vehicle 14B determine that it requires a token, then it sends a token request signal to the first vehicle 14A.

To this end, the respective transceivers 24 may be configured to support a vehicle-to-vehicle communications channel, including a broadcast facility for the first vehicle 14A. Since the vehicle to vehicle exchange of tokens is intended to allow positional validation of the second vehicle 14B, the transceivers 24 are preferably configured to support only short range communication between vehicles 14, for example using WiFi, DSRC, Bluetooth or other short range wireless communication technology. A typical range of vehicle to vehicle communication may be up to approximately 50 metres, preferably up to approximately 20 metres and most preferably up to approximately 10 metres. This ensures that only vehicles that are physically close to one another (and which may therefore be assumed to be on the same road) can exchange tokens.

In preferred embodiments, the server 12, in particular the billing system 12B, is arranged to set a maximum valid token transfer range for vehicles, where any tokens transferred between vehicles that are determined by the server (e.g. by comparing the location data from the tokens) to have been further apart that the maximum range when the token was transferred are deemed to be invalid. Advantageously, the server 12 may adjust the
maximum range depending on conditions, e.g. to compensate for the density of the network (for example in sparse deployments range should be higher, in dense networks, range should be restricted). Alternatively, or in addition, the vehicle client 22 of one or other or both of the vehicles involved in a token exchange may check that distance between the vehicles is within the maximum range before exchanging a token, requesting a token or accepting/validating a received token, as applicable. This may be achieved by any convenient means, e.g. transmission of GPS data from one vehicle to another for comparison with the GPS data of the other vehicle. The maximum range may be set and, if necessary adjusted, by the server and communicated to the vehicles as is convenient.

It is not necessary for the vehicle 14A to be identified and so, preferably, neither the communications between the vehicles 14A, 14B nor the exchanged token identify the vehicle 14A.

Optionally, a first vehicle 14A is configured only to advertise and/or distribute tokens to other vehicles 14 when it is within a predetermined range of its base location (or other central location), as may be determining by comparing its current GPS position with the GPS position of its base/central location.

The first vehicle 14A may be arranged to transmit a token to a second vehicle 14B upon receipt of a valid request from the second vehicle 14B. Preferably, in order to validate a token request, the first vehicle client 22 checks whether or not the second vehicle 14B is sufficiently close to the first vehicle 14A so that the respective locations of the vehicles 14A, 14B may be deemed to match. In a simple embodiment, a location match may be assumed by receipt of a request from the second vehicle 14B, since the vehicle transceivers 24 are only capable of support inter-vehicle communication over short range. Preferably, however, the second vehicle 14B transmits its GPS position to the first vehicle 14A, conveniently as part of the token request signal. The client 22 of the first vehicle 14A is arranged to compare its own GPS position with the received GPS position from the second vehicle 14B and to determine that the request is valid if the respective GPS positions are sufficiently close together, i.e. within a pre-determined range.

In cases where more than one second vehicle 14B requests a token from the first vehicle 14A at approximately the same time, the first vehicle 14A may attempt to send a token to each vehicle 14B, or to just one of the vehicles 14B. Either way, the first vehicle 14A needs to determine which of the second vehicles 14B to communicate with first. One option is for the first vehicle 14A to transmit a token to the second vehicle 14B associated
with the first valid token request received by the first vehicle. Alternatively, the first vehicle 14A may be arranged to determine, using the respective GPS positions received from the respective second vehicles 14B, which vehicle 14B is closest to itself, and to transmit a token 34 to the closest vehicle 14B from which it receives a valid token request. As such, vehicles 14B may be said to bid for tokens from the first vehicle 14A. Once the first vehicle 14 has transmitted a token 34 to a selected vehicle 14B, it may attempt to process the received token request(s) from vehicle(s) that were unsuccessful in the previous bidding. In many cases, such vehicles 14B may be out of range and so, preferably, unsuccessful token requests are ignored. Preferably, therefore, once the vehicle 14A has successfully transmitted a token 34 to a second vehicle 14B, it returns to its token advertising state to await new token requests.

Tokens that are transmitted from vehicle to vehicle as described above are modified by one or both of the vehicles 14A, 14B depending on one or more aspects of the location of the or each vehicle 14A, 14B at the time the token was exchanged. Depending on whether or not the first vehicle 14A is responsible for some or all of the modification, therefore, the token 34 transmitted from the first vehicle 14A to the second vehicle 14B may or may not be the same as the corresponding token 30 that the first vehicle 14A received from the server 12B.

Preferably, the originally distributed token 30 is modified using the respective location of one or both of the first and second vehicles 14A, 14B, as may be derived from the respective GPS positions of the vehicles (preferably in conjunction with a computer usable map, as is described in more detail hereinafter), at the time of the token exchange. It is particularly preferred that the token 30 is modified using both of the respective GPS positions, and more preferably a derivative thereof. For example, the respective GPS positions may be processed to produce a data value that is indicative of the respective vehicle locations, or of the difference between the two positions, the resulting data value(s) being incorporated into the token. For example, the respective GPS positions, or preferably respective vehicle location data derived therefrom (e.g. from a computer usable map), together with the distributed token 30 may be transformed using one or more one-way hash functions (or other mathematical transformation function(s), preferably one-way transformation function(s)) to produce a modified token 34. In any event, the modification is such that the server 12B, in due course, is able to determine that the first and second vehicles 14A, 14B had substantially matching locations at the time the token 34 was exchanged, which in turn may be used to validate the journey data transmitted to the server 12B by the second vehicle 14B, as is described in more detail.
hereinafter. Modification of the token based on the respective vehicle locations may be performed by the client 22 of either the first vehicle 14A or the second vehicle 14B. If performed by the second vehicle 14B, then the first vehicle 14A must transmit not only the token 34, but also its own GPS position (or derivative) to the second vehicle 14B.

5 Advantageously, the respective vehicle location data is incorporated into the token 34 in such a way that the respective GPS position data, or location, cannot be retrieved from the modified token 34. As is described in more detail hereinafter, in the preferred embodiment, this is achieved by using a combination of hash functions and public key encryption (e.g. encrypting the location hash using the public key. The token receiving vehicle then cannot "fake" the same hash as it cannot decrypt the token. All it can do is calculate its own hash. The server then (having the private key that will decrypt the token) makes the comparison.)

15 Alternatively, or in addition, the GPS position of the first vehicle 14A may be used to validate a road or road type to be recorded by the second vehicle 14B. For example, as is described in more detail below, the second vehicle 14B compiles journey data that includes identification of road types, or optionally specific roads (e.g. toll roads), on which it has travelled. This may be achieved by comparing the second vehicle’s GPS position with an electronic map 40. Upon exchange of the token 34, the GPS position of the first vehicle 14A may be compared against the map to determine a road type or specific road/feature corresponding to the GPS position of the first vehicle 14B. This information may be incorporated into the modified token 34 in any convenient manner, for example by modifying the token to indicate whether or not the respective road types/road features match one another, or by modifying the token to include information identifying the road type/road feature associated with the GPS position of the first vehicle 14B, which information can subsequently be used by the server 12B to validate the corresponding road/road feature recorded by the second vehicle 14B. The modified token may be created by performing a one-way hash function (or other transformation, preferably a one-way transformation) on the original token 30 together with data indicating the road type/road feature associated with the GPS position of the first vehicle 14B, or data indicating whether or not the respective road types/road features match one another. Such modification of the token 30 is conveniently performed the client 22 of the second vehicle 14B, in which case the GPS position, or derivative thereof, of the first vehicle is provided thereto.
In the preferred embodiment, the modified token includes information indicative of the road type declared by the second vehicle 14B in respect of the token exchange.

Optionally, the modification of the token 30 may include incorporation of information into the modified token that is indicative of the time and/or date at which the token was passed from the first vehicle to the second vehicle.

The second vehicle 14B stores the modified tokens in local memory for subsequent communication to the server 12.

The client 22 of the second vehicle 14B has access to (either in local memory or via the network 16) the electronic map 40 that correlates road information with GPS position. In the preferred embodiment, the road information comprises a road type, each type being associated with a respective toll (which may be zero). For example, the road type may relate to whether the road type is an A road, B road, motorway, bridge, tunnel, or toll-free road. More generally, each road type relates to a toll category, the map assigning roads, parts of roads or features of roads to a respective road type depending on the desired toll category. Toll categories may be associated with a respective price-per-mile or a flat toll. Using the map 40 and its GPS position, the client 22 is able to record journey data from which toll payments can be calculated. For example, the journey data may comprise identification of one or more road types in association with the distance travelled on the respective road types, and/or the number of times one or more road types are used. The journey data may also include an indication of the time and/or date on which the respective road types are used. Journey data is typically compiled in respect of an accounting period.

The modified tokens stored by the second vehicle 14B are associated with the respective journey data compiled over a common period. Accordingly, the, or each, token that is associated with respective journey data is used by the server 12 to validate the journey data, as is described in more detail hereinafter. The modified tokens are preferably encrypted by the client 22 that creates them, for example using a public encryption key.

It will be understood that each vehicle 14 in the system 10 may behave as both the first and second vehicles 14A, 14B described above, depending on whether they are distributing tokens to other vehicles, or receiving tokens from other vehicles.
Figure 3 illustrates a journey validation and toll calculation phase of the preferred system's operation. The client 22 of the vehicle establishes communication with the server 12 via network 16 and transmits to the server 12 its journey data (i.e. journey related data gathered in respect of the vehicle's journeys, but not including details of the routes taken), together with the, or each, modified token that has been collected in respect of the journey data (details of actual routes taken are not transmitted to the server 12). This is typically performed periodically, e.g. at the end of an accounting period, which may for example be one week or one month. Hence, the journey data relates to journey(s) undertaken during the respective period, and the corresponding modified tokens are those collected during the same period. Preferably, the transmission of journey data and tokens to the server 12 is performed when the vehicle 14 is located at its base location. For example, this may be achieved automatically by the client 22 upon determining that the vehicle 14 is at its base location (and that it is timely to do so, e.g. at the end of an accounting period). Alternatively, the transmission may be initiated manually by the user, and/or in response to a request from the server 12. As described with reference to Figure 1, the vehicle 14 may receive new tokens 30 from the server at approximately the same time.

The server 12, and more particularly the token management server 12B in this example, verifies the journey data using the associated modified tokens. To this end, the server 12B extracts validation data from the, or each, modified token. For example, the server may process the modified tokens to check that they were generated from a valid original token 30. To this end the modified token preferably includes the respective original token, or a derivative thereof, the derivative being such that validity can be verified. The server 12B may also extract data indicating the road type recorded in the token. Also by way of validation of the modified token, the server 12B may extract information from the modified token that indicates the relative distance between the vehicles when the token was exchanged. Alternatively, or in addition, the server may cross-validate the vehicles' locations at the time of token exchange by comparing respective location data (advantageously a hashed representation of location, preferably coarse grid location). As is described in more detail hereinafter, this may be achieved by incorporating into the token information that represents the respective locations of the vehicles at the time the token was exchanged.

In preferred embodiments, the server 12B may be configured to expect that at least a threshold number of tokens should be collected per unit distance. Hence, for a given distance travelled by the vehicle 14, a minimum expected number of tokens can be
calculated by the server 12. The threshold number may be different for some or all of the road types, and may also depend on the time of travel (in embodiments where time is recorded). So if, for example, the journey data indicates that X miles were travelled on type T1 roads, then the server 12B knows how many corresponding tokens should statistically have been collected in respect of type T1 roads. If the actual number of valid tokens collected in respect of the respective road type substantially matches (i.e. is within a respective range) the expected number of tokens, then the server 12 may verify that the journey data is correct. For road types that are not associated with a price-per-distance toll, e.g. a tunnel, bridge or flat fee toll road, collection of a single respective token may be sufficient for the server 12 to validate the journey data in respect of the road type. For road types that may be so short or so remote or low in traffic for other reasons that a vehicle may be expected not to encounter any other vehicles from which to receive a token, one or more road side token dispensing stations may be provided, which stations may behave in a manner substantially the same as described above for the first vehicle 14A.

Once the journey data has been verified, the server 12, or more particularly the billing system server 12A in this example, calculates the fees due in respect of the accounting period.

In the preferred embodiment, each the client 22 of each vehicle 14 records its journey data for a given accounting period based on the GPS locations of the vehicle during that period, and using a current version of the billing map. Then, during the billing information upload to the server 12, this information is summarised as X miles on type T1 roads, Y miles on type T2 roads, and so on. The respective road types are determined by the map 40 in conjunction with the GPS location of the vehicle. The billing server 12A calculates the toll due in accordance with whatever toll schedule may be in place. Also, the validation tokens should match up on the basis of the ratios of the usage claimed, e.g. so many for category A roads, so many for category B.

The preferred system 10 requires no end-user interaction. The system 10 may provide billing information to users by any suitable means, e.g. by SMS, e-mail and/or a website. The preferred system 10 operates without requiring any dedicated infrastructure, or at least a minimal amount of infrastructure. This provides a major cost saving over existing tolling technologies, whether they are based on number plate recognition, RFID “pass” or fee collection at booths.
In the preferred embodiment, the server 12 analyses token statistics as an anti-fraud measure. In particular the server 12B records which vehicles 14 received which tokens 30 from the server 12, and which tokens 34 were subsequently distributed to other vehicles 14. The server 12B also knows which modified tokens were returned to it. Advantageously, the modification of a token is such that the server 12B is able to identify that a collected modified token is a valid unmodified token 30 that was originally distributed by the server 12, and optionally that is has not expired. Although one option is for the server to perform a one to one match of distributed tokens to received (modified) tokens, this may be viewed as a loss of privacy and so, in preferred embodiments, the server verifies that the token was valid and, optionally, that it had not expired, without matching distributed tokens to received tokens.

For example, in respect of one or more of the vehicles 14, the server 12B may calculate the rate of tokens delivered by one vehicle 14 to other vehicles 14, i.e. the number of tokens delivered in a given time period (e.g., x per week). The delivery rate of one or more vehicles 14 can be used to determine the expected rate of receipt of modified tokens by the server 12. This can be used to calculate an average number of tokens expected per unit distance over the entire road network managed by the system 10 (since the average mileage of the vehicles over the same time period is known). Therefore, vehicles whose rate of reporting validation tokens does not substantially match (i.e. not within a given range, or at least is substantially less than) the estimated average number per unit distance could be flagged for further investigation for possible fraud.

In the preferred system 10, the server 12 distributes tokens on a periodic basis, e.g. daily, to a selected set (preferably a randomly or pseudo-randomly selected set) of vehicles 14 and, advantageously, incorporates a time limitation on the validity of the tokens (as described above). Since, in the preferred embodiment, tokens 30 are distributed by the server 12 only when a vehicle 14 is in its base location, this distribution of tokens 30 by the server 12 is advantageously weighted to compensate for differences in time spent at the respective base location by respective vehicles 14, i.e. the number of tokens sent to a vehicle by the server during a distribution phase, is dependent on the number of tokens previously sent to said vehicle during one or more earlier distributions. This could be achieved by calculating a distribution rate (which is indicative of the rate at which tokens have historically been distributed to the respective vehicle by the server) in respect of each vehicle and distributing tokens depending on the respective distribution rates of the vehicles (e.g. vehicles with relatively high distribution rates receive fewer tokens during a distribution phase than vehicles with a relatively low distribution rates). The system 10
preferably tracks the number of tokens received by each vehicle 14 from the server 12 over a significant period of time (say, a few months) to obtain data for use in the inverse weighting such that a vehicle having a relatively low rate of receiving tokens is more likely to receive a token in the next distribution than a vehicle that has a high rate. These measures help to mitigate against possible attempts by a would-be fraudulent party to reverse engineer and modify the in-vehicle client devices 22 so that they could use fake GPS co-ordinates and use their own tokens for distribution for validation of false routes.

In terms of the vehicle to vehicle communications, there is a trade off between coverage and token validation accuracy. For example, if the supported range of the vehicle to vehicle communication link is too short, then token transfer will occur less frequently (as the chance of hearing a vehicle advertising tokens is reduced). Against this, a relatively short range improves the accuracy of the “validation” of tokens as both vehicles are more likely to be on the same road. However, in the case of relatively large ranges for vehicle to vehicle communications, this leads to higher hit rates in terms of token distribution, but the validation accuracy is reduced. To optimise this trade off and as described in relation to Figure 2, the preferred system 10 gives priority to vehicles that are closest to the vehicle distributing the token. In this way, the validation accuracy is always as high as possible.

One example of token distribution between vehicles is illustrated in Figure 4. The distributor vehicle, which is indicated by the label D-vehicle in Figure 4 and corresponds to the first vehicle 14A of Figure 2, received one or more tokens (identified as D-token in Figure 4) from the server 12. After clear channel assessment, the D-vehicle sends a broadcast message advertising the availability of tokens. Nearby anonymous vehicles then respond by transmitting a signal comprising their GPS co-ordinates, preferably the current road type at their GPS location, and preferably also a hash, or other identification, of their current map version preferably including a digital signature. Each bidding vehicle may remain anonymous, e.g. by identifying themselves using a temporary random session node address. Multiple responses are possible by using, for example, a random slotted backoff wireless transmission algorithm, or other suitable multiple access method.

The D-vehicle then calculates the distance, preferably the Euclidian distance, between its GPS co-ordinates and the respective GPS co-ordinates of each “bid” signal received from the nearby anonymous vehicles. The D-vehicle then decides on a winner (closest vehicle, identified as the “A-vehicle” in Figure 4). It is preferred that a vehicle can only be selected
for receipt of the token if the distance between the D-vehicle and A-vehicle is below a maximum inter-vehicle spacing, \( r_{\text{max}} \).

The D-vehicle compares the map hash received from the A-vehicle with a corresponding hash, or other corresponding identifier, of its own map. If these match each other, then the D-vehicle is able validate the road-type declared by A-vehicle by comparison with its own determined road type (which should be the same as the one declared by the A-vehicle). Otherwise, the declared road type may still used, but the “quality” of the claimed road type may recorded as unverified. Information indicating whether the road type is a match or not can be incorporated into the modified token by the client of one or other of the vehicles, conveniently the D-vehicle.

The D-vehicle responds to the A-vehicle by transmitting to it an “A-token” that comprises a modified D-token. The A-token may comprise the respective D-token modified to incorporate information indicating the D-vehicle’s location (preferably a coarse location, e.g. a map grid location preferably with a grid resolution greater than twice \( r_{\text{max}} \)). The location may be determined by comparing the D-vehicle’s GPS position against the map. In an alternative embodiment, the D-vehicle’s GPS data itself, or a derivative thereof, could be used as the location data in place of the map/grid location.

Preferably, the A-token comprises the respective D-token combined with a hash (or other transformation) of the D-token and the D-vehicle’s location (see Figure 5). The A-token preferably also includes information identifying the declared road type.

Advantageously, at least the D-vehicle’s location hash and the road type information are encrypted (e.g. using the system’s public encryption key). The D-token component of the A-token is preferably sent unencrypted, e.g. in plaintext.

The A-vehicle then creates a final validation token (V-token) by adding to the A-token information identifying its own location (preferably a coarse location, e.g. a map grid location preferably with a grid resolution greater than twice \( r_{\text{max}} \)). Preferably, this is achieved by calculating its own location hash from the respective D-token and its location (preferably the coarse grid location) at the time of its “bid”, and combining the result with the A-token (see Figure 5). Optionally, the A-vehicle encrypts the V-token, e.g. using the system public key. The location may be determined by comparing the A-vehicle’s GPS position against the map. In an alternative embodiment, the A-vehicle’s GPS data itself, or a derivative thereof, could be used as the location data in place of the map/grid location.
location. Also, to the extent that the two vehicles involved in the token exchange are at substantially the same location, the GPS data and/or map location of either vehicle instead of both could be incorporated into the modified token as described above.

Using a map grid location as the location data for incorporation into tokens is preferred since it simplifies the location validation aspect of tokens, i.e. two vehicles that are close enough to exchange a token will usually have the same map grid location and this simplifies the comparison of respective location data hashes (or other transformed values) e.g. the respective location data hashes (or other transformed values) should match. For example, where a one way hash function, or similar transformation function is used, the respective location data hash value will be the same for two vehicles at the same grid location (and so a simple comparison as to whether they are the same or not can be performed). Where a more precise indication of location is used, e.g. GPS data, location comparison can still be performed, although may be more complicated depending on what transformation is used when incorporating the more precise data into the tokens.

In the preferred embodiment, the V-token can only be verified using the system's private encryption key, in this case by the server 12.

In low vehicle density road networks (e.g. during the start up phase of the deployment of the system 10), D-tokens may be created and distributed by fixed stations such as traffic lights or signposts. Low cost devices (similar to the client devices described herein) may receive the encryption keys and token generator functions, as required, over a secure communications link. By generating their own nonce, the system would still not know which vehicles had received the D-tokens, maintaining user privacy.

Referring now in particular to Figure 5, examples of the tokens are described. The D-token comprises a code, e.g. a number, which may for example be 128 or 256 bits long, created by using a random nonce that is wholly divisible by a mathematical function, in this case a generator polynomial G(x), which is preferably changed periodically, e.g. changed every day / week / year. The D-token is preferably encrypted, e.g. using a private, or secret, key matched to G(x). Hence D-tokens cannot be generated by third parties. The D-tokens are time limited in this example since they can only be decrypted by a secret key that changes with time since it is dependant on G(x). Preferably, the D-tokens are not stored by the server 12.
The A-token (anonymous token) comprises the respective D-token combined with a location hash (a hash of the D-token with an indication of the D-vehicle’s location e.g. coarse grid location) a road type, and preferably also road type validation information. Preferably, the location hash and road type related information are encrypted, in this case using the system’s public key.

The V-token comprises the respective A-token combined with a hash of the A-vehicle’s location, optionally encrypted using, in this case, the public key.

The server 12 is arranged to, in this example by decrypting using its private key twice, extract the location hash for both the D-vehicle and the A-vehicle, the road category for the A-vehicle (and the D-vehicle validation of same if available) and the D-token. Validation of journey data by the server 12 occurs if the two location hashes are equal (or deemed to match one another), which does not reveal the actual GPS location of the respective vehicles. Preferably, validation only occurs if the D-token is valid (which in this example may be tested by trying one or more recent secret keys to extract the (128-bit) nonce and checking if it is wholly divisible by the respective G(x) corresponding to that secret key).

To further improve the privacy offered by the system 10, and in particular to prevent vehicle locations from being determined from the location hashes (e.g. from the D-token and the relevant coarse grid, all possible hashes could be computed), each of the first and second vehicles 14A, 14B may be caused to create their respective location hash (or other transformation of the location data) including a unique identifier generated, preferably randomly, for the respective token transfer. The unique identifier may comprise a (pseudo) random nonce or number, and may for example comprise data indicating the time (e.g. UTC) of the token transfer. This is illustrated in Figure 6, where the unique identifier is assumed to comprise a session ID created in respect of the token transfer (and which may subsequently be discarded). A similar description applies as per Figure 5, except that the D-vehicle and A-vehicle location hashes are each formed from the D-token or A-token, respectively, a unique session ID and the respective coarse grid locations. The same session ID, or other unique ID, is preferably used by each vehicle – it may be generated by one vehicle and communicated to the other.

A further option for preventing fraud, in particular to prevent a single vehicle from forging the V-token from the D-token without any interaction with another vehicle, involves creating the D-token from two parts, D1 and D2, each vehicle 14A, 14B involved in a
token transfer carrying a respective part D1, D2. This is illustrated in Figure 6 where the D-vehicle 14A has D1, receives D2 from the A-vehicle as part of the token transfer process, and combines D1 and D2 to make the D-token. The token parts (D1 or D2) distributed to each vehicle by the server are linked, e.g. belonging to a mathematical series, such that D-tokens and/or V-tokens formed from parts D1, D2 that originated from the same vehicle can be detected, e.g. by comparison of the respective D1 and D2 parts.

The foregoing description of system 10 assumes that user privacy, in particular the locations visited by the user, is important to protect. In other embodiments user privacy is considered to be less important. Such systems may be substantially as illustrated in Figures 1 to 4 and so the same description may be applied, as would be apparent to a skilled person, unless otherwise indicated hereafter. In the token distribution phase (Figure 1) and cost calculating/token uploading phase (Figure 3), there is no need for the transfer of tokens or other data between the server 12 and the vehicle 14 to be performed while the vehicle 14 is in a particular location, e.g. at home or other base location (although it may be convenient to do so). Transfer of tokens and/or other data may be performed at any convenient time or location by any available means, e.g. WiFi or cellular network.

During token exchange (Figures 2 and 4), the D-vehicle (14A) may advertise tokens as described above and the, or each, A-vehicle (14B) in the vicinity may request a token. This may be performed in the manner described above. Alternatively, where multiple A-vehicles are bidding for a token, the A-vehicles may send a request signal to the D-vehicle and the D-vehicle may select an A-vehicle based on the strength of the signal request (a stronger signal indicating a closer vehicle), or by applying any other convenient selection criteria (e.g. first-received request), or by making a random selection. The request signal from the A-vehicle may for example comprise a session ID or other unique identifier.

In this example it is assumed that the D-vehicle modifies D-tokens before sending them to A-vehicles, although it will be understood that this is optional and that modification could be performed by the A-vehicle only. The D-vehicle responds to the A-vehicle by transmitting to it an “A-token” that comprises a modified D-token, an example of which is illustrated in Figure 7. The A-token may comprise the respective D-token modified to incorporate information indicating the D-vehicle’s location, e.g. its GPS location and optionally the time (e.g. UTC) of transfer (see Figure 7). In this case, the actual GPS location may be used for convenience (i.e. a fine, or precise, indication of location rather
than the coarse one provided by grid locations). The D-vehicle's location could be taken as the location, e.g. its GPS location and optionally the time (e.g. UTC) of transfer, at the time the request was received from the A-vehicle, or the location at the time the A-token is created. The D-vehicle's GPS data itself, or a derivative thereof, could be used as the location data. Optionally, a vehicle ID for the D-vehicle may be included in the A-token. The location data, and preferably also the vehicle ID when used, are encrypted, e.g. using the system's public key. The D-token itself (unmodified and preferably unencrypted) is preferably also included in the A-token. In this example, the creation and encryption of the A-token is performed by the client running on the D-vehicle.

The A-vehicle then creates a validation token (V-token), an example of which is shown in Figure 7) by adding to (i.e. modifying) the A-token information identifying its own location (e.g. at the time of its request to the D-vehicle), and preferably combining the result with the A-token. In this case, the actual GPS location of the A-vehicle may be used for convenience (i.e. a fine, or precise, indication of location rather than the coarse one provided by grid locations). Optionally the time (e.g. UTC) of transfer may be incorporated into the V-token. The A-vehicle's GPS data itself, or a derivative thereof, may be used as the location data. Optionally, a vehicle ID for the A-vehicle may be included in the V-token. The location data, and preferably also the vehicle ID when used, are encrypted, e.g. using the system's public key. The A-token itself (unmodified and preferably unencrypted) is preferably also included in the V-token. In this example, the creation and encryption of the V-token is performed by the client running on the A-vehicle. Also, to the extent that the two vehicles involved in the token exchange are at substantially the same location, the GPS data either vehicle instead of both could be incorporated into the modified token as described above. V-tokens may be transmitted to the server 12 at any convenient time or location.

In this embodiment, during the cost calculating phase (Figure 3), the server 12, typically the billing server 12A, may check each validation token (V-token) by decrypting it using the system private key to extract the location and vehicle ID of each vehicle involved in the token exchange. The server 12 may assess the respective vehicle locations extracted from the V-token, e.g. by comparing them to determine how close they are to each other, i.e. to determine if they are within a threshold distance of each other. If so, then the returned token may be deemed to be valid. In preferred embodiments, the unmodified D-token is retrievable from the V-token and may be used by the server for validation and/or anti-fraud purposes as described above.
It will be apparent from the foregoing that systems having less emphasis on user privacy may be simpler that those having higher emphasis on privacy. For example, creating coarse location hashes, incorporating road type data into one or more of the tokens, and communication with the server 12 at a specific base location may all be omitted (although any one or more of these could be used in any embodiment as desired).

In further alternative embodiments, a token sent from the first vehicle 14A (e.g. the D-vehicle) to the second vehicle 14B (e.g. the A-vehicle) may be returned (in a modified state) to the first vehicle 14A by the second vehicle 14B, in which case the modified token may be transmitted to the server 12 by the first vehicle 14A. Such tokens could be used to validate the journey of the first vehicle 14A and/or the second vehicle 14B depending on the configuration of the system. Also depending on the configuration of the system, the D-vehicle may perform its modification of the token before it is sent to the A-vehicle or after it is returned from the A-vehicle (duly modified by the A-vehicle). Token modification may take any convenient form, including those described above. In such embodiments, the token sent in the first instance from the first vehicle 14A to the second vehicle 14B could also be processed and returned to the server 12 by the second vehicle 14B as described above with reference to Figures 1 to 7 to validate the journey of the second vehicle.

It will be understood that other transformation functions, preferably one way transformation functions, may be used instead of the hash function described herein.

The invention is not limited to use with toll systems and may be applied to other tasks, e.g. verifying or monitoring vehicle usage for the purposes of insurance. In such cases, the system need not necessarily compute tolls.

The invention is not limited to the embodiments described herein, which may be modified or varied without departing from the scope of the invention.
CLAIMS:

1. A computer-implemented system for verifying vehicle usage comprising a server capable of communication with a plurality of clients across a communications network, each client being provided in a respective vehicle and being co-operable with a respective global positioning system (GPS) by which the client can determine the location of the respective vehicle,
   wherein a first of said clients is arranged to communicate to a second of said clients at least one computer usable token when the respective vehicles are within a valid range of one another,
   one or both of said first and second clients being arranged to modify said at least one token to include information dependent on the location of one or both of said vehicles substantially when said at least one token is communicated between the clients,
   and wherein one or both of said first and second clients is arranged to communicate said at least one modified token to said server, said server being arranged to extract said location dependent information from said at least one modified token.

2. A system as claimed in claim 1, wherein said server is arranged to assess the extracted location dependent information and to validate said at least one modified token based on said assessment of said location dependent information.

3. A system as claimed in claim 1 or 2, wherein said location dependent information comprises information from which the relative distance between the first and second vehicles substantially at the time said at least one token was communicated between the clients can be assessed, said server being arranged to assess said location dependent information by determining if said relative distance is within a threshold limit.

4. A system as claimed in any preceding claim, wherein said location dependent information is indicative of the respective location of both of said first and second vehicles, said server being configured to assess said location dependent information by determining if the distance between said respective locations is within a threshold limit.

5. A system as claimed in claim 4, wherein said location dependent information comprises the respective GPS location of each vehicle.

6. A system as claimed in any preceding claim, wherein said location dependent information includes respective information dependent on the respective locations of said
first and second vehicles, said server being configured to assess said location dependent information by determining if the respective location dependent information for said first and second vehicles match.

7. A system as claimed in claim 6, wherein said respective location dependent information for said first and second vehicles comprises an approximation of the respective vehicle’s GPS location.

8. A system as claimed in claim 7, wherein said respective location dependent information for said first and second vehicles comprises an indication of a location on a map.

9. A system as claimed in claim 8, wherein said map location comprises a grid reference for the map.

10. A system as claimed in any one of claims 1 or 2 or 6 to 9, wherein one or both of said first and second clients are arranged to modify said at least one token to include said location dependent information such that the respective location of one or both of said vehicles is not extractable from said at least one modified token.

11. A system as claimed in claim 10, wherein said location dependent information is transformed using a mathematical function, preferably a one-way mathematical transformation, for example a hash function, the result of said transformation being incorporated into said at least one modified token.

12. A system as claimed in claim 11 when dependent on any one of claims 6 to 9, wherein said server is configured to assess said location dependent information by determining if the respective transformation result for each vehicle match each other.

13. A system as claimed in any preceding claim, wherein said location dependent information comprises information indicating a road type determined by the location of one or both of the respective vehicles, preferably at least by the location of said second vehicle, when said at least one token is communicated between the respective first and second clients.
14. A system as claimed in claim 13, further including at least one computer usable map that links GPS locations to road types, and wherein said map is accessible by one or both of said first and second clients.

15. A system as claimed in claim 14, wherein one or both of said first and second clients are configured to determine a road type associated with the location of the respective vehicle, and to determine if its determined road type matches the determined road type associated with the vehicle of the other of said clients, and to incorporate into said at least one token information indicating whether or not the road types match.

16. A system as claimed in any preceding claim, wherein said server is arranged to distribute tokens to at least said first client.

17. A system as claimed in any preceding claim, wherein said at least one token comprises at least one original token, one or both of said first and second clients being configured to modify said at least one original token as part of an exchange of said at least one token between said first client and said second clients.

18. A system as claimed in claim 17, wherein said first client is configured to modify said at least one original token to include information dependent on the location of said first vehicle, and to send at least one correspondingly modified token to said second client.

19. A system as claimed in claim 18, wherein said second client is configured to modify said at least one correspondingly modified token to include information dependent on the location of said second vehicle to create at least one correspondingly further modified token.

20. A system as claimed in claim 17, wherein said first client is configured to send said at least one original token to said second client, said second client being arranged to modify said at least one original token to include information dependent on the location of said second vehicle, and optionally also on the location of said first vehicle.

21. A system as claimed in any one of claims 17 to 20, wherein said second client is configured to send said at least one modified token to said first client.
22. A system as claimed in claim 21, wherein said first client is configured to modify said at least one modified token to include information dependent on the location of said first vehicle.

23. A system as claimed in any one of claims 17 to 22, wherein said second client is configured to send said at least one modified token to said server.

24. A system as claimed in any one of claims 17 to 23, wherein said first client is configured to send said at least one modified token to said server.

25. A system as claimed in any preceding claim, wherein said at least one modified token includes the respective unmodified token combined with said location dependent information.

26. A system as claimed in any preceding claim, wherein one or both of said first and second clients are configured to modify tokens to include data identifying the respective vehicle.

27. A system as claimed in any preceding claim, wherein one or both of said first and second clients are configured to modify tokens to include data identifying a respective token exchange session.

28. A system as claimed in any preceding claim, wherein said at least one original token is distributed to said first client, conveniently by said server.

29. A system as claimed in any one of claims 1 to 27, wherein a first part of said at least one original token is distributed to said first client and a second part of said at least one original token to said second client, and wherein at least one of said first and second clients communicates its part to the other of said first and second clients.

30. A system as claimed in any preceding claim, wherein one or both of said first and second clients is configured to encrypt at least part of said at least one modified token prior to sending said at least one modified token to the other of said first and second clients or to said server.

31. A system as claimed in claim 30, wherein one or both of said first and second clients is configured to encrypt said location dependent information.
32. A system as claimed in claim 30 or 31 when dependent on claim 25, wherein one or both of said first and second clients is configured to leave said unmodified token unencrypted.

33. A system as claimed in antecedent claim, wherein said server is arranged to use said at least one validated modified token in calculating a toll payable by the user of the first and/or second client's vehicle.

34. A computer-implemented method of determining road usage, or vehicle usage, in a computer-implemented system comprising a server capable of communication with a plurality of clients across a communications network, each client being provided in a respective vehicle and being co-operable with a respective global positioning system by which the client can determine the location of the respective vehicle, the method comprising:

   communicating from a first of said clients to a second of said clients at least one computer usable token when the respective vehicles are within a valid range of one another,

   modifying said at least one token to include information dependent on the location of one or both of said vehicles when said at least one token is communicated between the clients,

   communicating said at least one token to said server, and

   extracting said location dependent information from said at least one token.
FIG. 6

- Random 128-bit nonce with $G(x)$ as a factor
- Encrypted with secret key $S(x)$

D1

D2

D-token

D-vehicle coarse grid location

Session ID

Encrypted with system's public key $(n, e)$

A-token

A-vehicle coarse grid location

A-vehicle location hash

A-token hash

V-token

D-token = D1 + D2

Road category info
A-token

D-token

Random 128-bit nonce with G(x), as a factor

Encrypted with secret key S(x)

D-vehicle location

Encrypted with system's public key (n,e)

A-vehicle ID

A-vehicle location

Encrypted with system's public key (n,e)
**INTERNATIONAL SEARCH REPORT**

**International application No**

PCT/EP2012/055772

### A. CLASSIFICATION OF SUBJECT MATTER

**INV.** G07B15/06 G07C5/00

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07B G08G G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 2009/015989 A1 (BOSCH GMBH ROBERT [DE]; REBSCH JOHANNES-CHRISTOF [DE]; FRIESE MICHAEL) 5 February 2009 (2009-02-05) abstract page 4, line 26 - page 8, line 12 figure 2 -----</td>
<td>1-34</td>
</tr>
</tbody>
</table>

* Further documents are listed in the continuation of Box C.

X **See patent family annex.**

- **A** document defining the general state of the art which is not considered to be of particular relevance
- **E** earlier application or patent but published on or after the international filing date
- **L** document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- **O** document referring to an oral disclosure, use, exhibition or other means
- **P** document published prior to the international filing date but later than the priority date claimed
- **T** later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- **X** document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- **Y** document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- **&** document member of the same patent family

**Date of the actual completion of the international search**

31 May 2012

**Date of mailing of the international search report**

14/06/2012

**Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk, Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016**

Stenger, Michael
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EP 2176836 A1</td>
<td>21-04-2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2009015989 A1</td>
<td>05-02-2009</td>
</tr>
<tr>
<td>DE 102007035738 A1</td>
<td>05-02-2009</td>
<td>DE 102007035738 A1</td>
<td>05-02-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2176837 A2</td>
<td>21-04-2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2009015987 A2</td>
<td>05-02-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2168110 A2</td>
<td>31-03-2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2306431 A2</td>
<td>06-04-2011</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2009011838 A2</td>
<td>22-01-2009</td>
</tr>
</tbody>
</table>