Abstract:
The present disclosure relates to a method performed in a communication network 1 comprising a Radio Access Network (RAN) 2 for facilitating resource management in the communication network of signalling relating to vehicles 4 which are connected to the network via the RAN. The method comprises detecting that a connected vehicle is stationary. The method also comprises obtaining location information about which location the vehicle is stationary. The method also comprises correlating the location information with security information. The method also comprises determining number and type of sensors 5 in the vehicle which connect to the communication network when the vehicle is stationary in the location. The method also comprises allocating network resources to the vehicle based on the determining and on the correlated security information.
RESOURCE MANAGEMENT IN A RADIO COMMUNICATION NETWORK

TECHNICAL FIELD
The present disclosure relates to a method and devices for resource management in a communication network of signalling relating to vehicles which are connected to the network.

BACKGROUND
The European Telecommunications Standards Institute (ETSI) machine-to-machine (M2M) standard contains an overall end-to-end M2M functional architecture as shown in figure 1. The ETSI M2M standard ETSI Technical Specification (TS) 102 690 Version 2.1.1 specification document describes a resources-based architecture that can be used for the exchange of data and events between machines.

As a part of the Internet of Things (IoT), for example cars and other vehicles may be wirelessly connected and use M2M communication. Also, autonomous driving is likely to emerge progressively as driver assistance systems become more sophisticated. Services associated with autonomous driving may be provided, such as mapping, car-sharing and car recharging services.

A connected smart vehicle comprises of group of sensors including security sensors. Some sensors can work on battery while others run when the engine is running. Security sensors of vehicles can be active even when the vehicle is parked (or is in a stationary state) and engine is switched off.

Security sensors can alarm the users about inception of security events relating the vehicle. Security sensors traditionally involves short range communication technologies and alerts user via sounds, but in connected vehicle ecosystem, operators can play a role to help the user initiate contact
with the parked (stationary, engine off) vehicle or vice versa using Third Generation Partnership Project (3GPP) network technologies.

The number of active sensors can change in various states of the vehicle, for instance a security sensor might be more active during a vehicle's stationary and switched off state, while the speed sensors are found active when the vehicle has a particular speed i.e. while running on a road and the engine is on. Security sensors are part of a vehicle as they help the owner or parking manager to rest assured that the vehicle is safe. It is quite possible in connected vehicle ecosystem, that telecommunications operators are connected to and can access security sensors, thereby enabling security related services in the vehicles remotely by activating one or more sensors or enable using 3GPP network intelligence to activate one or more sensors in a vehicle relating to security at a locations or street using 3GPP network technologies. It is quite possible that an operator might want to trigger one or more security sensors in one or more connected vehicles (even in stationary, engine-off but battery-on state, like during parking of a car near the roadside, e.g. if the driver (user) went buying things in a nearby shop) to help the user get data or information from those sensors.

SUMMARY

Designated car-parking locations, such as a car part or garage, including multi-level parking, parking lots at malls, offices, cinema, etc., are the officially marked parking locations.

Vehicles come and get parked at designated parking locations. During parked state, one or more security sensors (inside the vehicle and/or outside in parking location) are active and may be triggered based on some local security hazard events, alert the users (owner, parking manager) via some network communication platform, e.g. smart-phone, interactive voice
response (IVR), Short Messaging Service (SMS), Unstructured Supplementary Service Data (USSD), Interactive Messaging (IM) etc.

Sensor activation can be programmed inside the vehicle based on the state of the vehicle (e.g. stationary, locked and engine off) or can be triggered by a 3GPP operator using network technologies when it detects some criteria e.g. a security issue.

Non-designated car parking locations includes parking near roadsides or at any place not officially marked as an official parking location.

For a vehicle parked at an available location (which is not a designated parking location, like parking on roadside while doing some shopping), security related location based information, such as accident related location information available in the Intelligent Transportation System (ITS) databases, e-Call databases, or at network operator domain using Global Positioning System (GPS) maps or the like, vehicle cloud, that would help operators are used to activate/trigger one or more security sensors (in one or more parked vehicles at unofficial locations, e.g. streets) so as to enable alerting the user/driver on some network communication platform, e.g. smart-phone, interactive voice response (IVR), Short Messaging Service (SMS), Unstructured Supplementary Service Data (USSD), Interactive Messaging (IM) etc., when some incident is detected by these sensors which are activated / auto triggered by an operator in the vehicle.

Sensor activation maybe pre-programmed in the vehicle based on state of the vehicle (vehicle stationary, locked and engine off) or may be triggered by the 3GPP operator externally using network technologies based on some criteria like subscriptions type, street analysis, vehicle type (motorcycle, bicycle, car, luxury vehicle, Sport Utility Vehicle (SUV), traveller, truck etc.) in the stationary (stopped or parked) vehicle.
Each day in smart cities, comprising smart vehicles, smart parking lots and smart road infrastructures, millions of vehicles may be parked near road sides during nights due to space scarcity, since most of the city sleeps while during the day most of the vehicles are parked in office parking lots. Security sensors (automatically triggered or externally triggered) may be active in the stationary vehicles, at parking locations and/or in the surrounding infrastructure near roads or parking lots/garages in smart cities, such that even during no risk situations one or more sensors may capture and send security metrics data periodically over to user or servers, further allowing a stationary vehicle-to-user and vice versa communication.

Large volumes of security-based heterogeneous sensor traffic are present in various communication scenarios in smart cities, comprising of traffic from stationary smart vehicles, smart parking lots/garages and smart road infrastructures. This presents a difficulty at operator's end to allocate proper network resources for signalling (e.g. in a Policy Control and Charging (PCC) Node) relating one or more security sensors (automatically activated in stationary vehicles, or activated externally by an operator based on criteria such as location-based security analytics, or surrounding locations and road infrastructures) in/around stationary vehicles so as to help provide proper Quality of Experience (QoE) in safety and security use cases in designated as well as non-designated parking locations around the city.

Existing state-of-the-art does not handle the security-based communication optimization in the mentioned smart cities IoT use cases involving smart vehicle and smart infrastructure, which therefore creates a need for improved network resource management which grows greater in step with increasing numbers of connected vehicles.
It is an objective of the present disclosure to provide a method and device for facilitating network resource management in an IoT scenario, especially relating to signalling from sensors of stationary network connected vehicles.

According to an aspect of the present disclosure, there is provided a method performed in a communication network comprising a Radio Access Network (RAN) for facilitating resource management in the communication network of signalling relating to vehicles which are connected to the network via the RAN. The method comprises detecting that a connected vehicle is stationary. The method also comprises obtaining location information about in which location the vehicle is stationary. The method also comprises correlating the location information with security information. The method also comprises determining number and type(s) of sensors in the vehicle which connect to the communication network when the vehicle is stationary in the location. The method also comprises allocating network resources to the vehicle based on the determining and on the correlated security information.

According to another aspect of the present disclosure, there is provided a computer program product comprising computer-executable components for causing a network arrangement of (e.g. forming a part of) the communication network to perform an embodiment of the method of the present disclosure when the computer-executable components are run on processor circuitry comprised in the network arrangement.

According to another aspect of the present disclosure, there is provided a network arrangement for (e.g. for being comprised in) a communication network comprising a RAN, and for facilitating resource management in the communication network of signalling relating to vehicles which are connected to the network via the RAN. The network arrangement comprises processor circuitry, and storage storing instructions executable by said processor circuitry whereby said network arrangement is operative to detect
that a connected vehicle is stationary. The network arrangement is also
operative to obtain location information about in which location the vehicle is
stationary. The network arrangement is also operative to correlate the
location information with security information. The network arrangement is
also operative to determine number and type(s) of sensors in the vehicle
which connect to the communication network when the vehicle is stationary
in the location. The network arrangement is also operative to allocate
network resources to the vehicle based on the determining and on the
correlated security information.

According to another aspect of the present disclosure, there is provided a
computer program for facilitating resource management in a communication
network of signalling relating to vehicles which are connected to the network
via a RAN. The computer program comprises computer program code which
is able to, when run on processor circuitry of a network arrangement of the
communication network, cause the network arrangement to detect that a
connected vehicle is stationary. The code is also able to cause the network
arrangement to obtain location information about in which location the
vehicle is stationary. The code is also able to cause the network arrangement
to correlate the location information with security information. The code is
also able to cause the network arrangement to determine number and type(s)
of sensors in the vehicle which connect to the communication network when
the vehicle is stationary in the location. The code is also able to cause the
network arrangement to allocate network resources to the vehicle based on
the determining and on the correlated security information.

According to another aspect of the present disclosure, there is provided a
computer program product comprising an embodiment of the computer
program of the present disclosure and a computer readable means on which
the computer program is stored.
By means of embodiments of the present disclosure, the network resources may be allocated to sensors of a connected vehicle based on security information relating to the location where the vehicle is stationary and on how many sensors are active (i.e. connected to the network) in the vehicle as well as the type or types of said active sensors. Thus, additional resources may be allocated e.g. to a vehicle which is determined to be stationary in an unsafe environment while less resources may be allocated (and fewer sensors may be activated) in a vehicle which is stationary in e.g. a designated and monitored parking lot or garage.

It is to be noted that any feature of any of the aspects may be applied to any other aspect, wherever appropriate. Likewise, any advantage of any of the aspects may apply to any of the other aspects. Other objectives, features and advantages of the enclosed embodiments will be apparent from the following detailed disclosure, from the attached dependent claims as well as from the drawings.

Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated. The use of "first", "second" etc. for different features/components of the present disclosure are only intended to distinguish the features/ components from other similar features/ components and not to impart any order or hierarchy to the features/components.
**BRIEF DESCRIPTION OF THE DRAWINGS**

Embodiments will be described, by way of example, with reference to the accompanying drawings, in which:

Fig 1 is a schematic block diagram of a standard M2M network architecture.

Fig 2 is a schematic diagram of an embodiment of a communication network in accordance with the present disclosure.

Fig 3a is a schematic block diagram of an embodiment of a network arrangement in accordance with the present disclosure.

Fig 3b is a schematic functional block diagram of an embodiment of a network arrangement in accordance with the present disclosure.

Fig 4 is a schematic illustration of an embodiment of a computer program product in accordance with the present disclosure.

Fig 5 is a schematic flow chart of an embodiment of the method of the present disclosure.

Fig 6 is a schematic diagram of system feedback to policy nodes in accordance with an example embodiment of the present disclosure.

Fig 7a is a schematic diagram illustrating movements and stops of a vehicle in accordance with an example embodiment of the present disclosure.

Fig 7b is an example origin-destination (OD) matrix in accordance with an example embodiment of the present disclosure.

Fig 7c is an example security matrix in accordance with an example embodiment of the present disclosure.

Fig 8 is a schematic block diagram of the policy control network of an operator.
DETAILED DESCRIPTION

Embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments are shown. However, other embodiments in many different forms are possible within the scope of the present disclosure. Rather, the following embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the disclosure to those skilled in the art. Like numbers refer to like elements throughout the description.

Figure 2 is a schematic block diagram of one or a plurality of sensor(s) (could alternatively be called detector) 5 in a vehicle 4 (e.g. a car as illustrated in the figure) connected to a communication network 1 run/controlled by a telecommunications network operator. The communication network 1 comprises a RAN 2, typically a cellular RAN in accordance with a 3GPP standard, comprising one or a plurality of RAN nodes 3, e.g. evolved Node B (eNB) or Node B in combination with Radio Network Controller (RNC). The communication network 1 also comprises a Core Network (CN) 12 comprising an serving gateway (SGW) 7 and a packet data network (PDN) gateway (PGW) 8 as well as a mobility management entity (MME) 6 and a policy and charging rules function (PCRF) 11, and any other standard CN nodes needed. The communication network 1 comprises a network arrangement 13 which may be comprised in the RAN 2 or the CN 12 or comprise parts of both the RAN and the CN, and may additionally comprise other parts of the communication network 1 such as cloud resources. For instance the network arrangement 13 may comprise one or more nodes or elements of communication network 13 such as one or more nodes or elements of the RAN and/or of the CN and/or of other parts of the communication network e.g. a service network of the operator or cloud resources. Via the PGW, the communication network is connected to the PDN 9, e.g. the Internet, in which a service provider (SP) 10 resides with one or a plurality of servers e.g.
Content Delivery Network (CDN) servers, for providing a service to a service client e.g. in the vehicle 4 or in a smartphone or other computer hardware of a user/driver of the vehicle 4 or of personnel monitoring the stationary vehicle 4 e.g. in a parking lot/garage, or in a network operator server.

The sensor 5 may be any radio device or user equipment (UE), mobile or stationary, enabled to communicate over a radio channel in a communication network 1, for instance but not limited to e.g. mobile phone, smart phone, detectors, meters configured for being positioned in/on a vehicle 4 for detecting any event/action taking place in relation to the vehicle.

Figure 3a schematically illustrates a network arrangement (e.g. one or more network nodes in the communication network 1) 13 of the present disclosure. The network arrangement 13 comprises processor circuitry 31 e.g. a central processing unit (CPU). The processor circuitry 31 may comprise one or a plurality of processing units in the form of microprocessor(s). However, other suitable devices with computing capabilities could be comprised in the processor circuitry 31, e.g. an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or a complex programmable logic device (CPLD). The processor circuitry 31 is configured to run one or several computer program(s) or software (SW) 41 (see also figure 4) stored in a storage 32 of one or several storage unit(s) e.g. a memory. The storage unit is regarded as a computer readable means 42 (see figure 4) as discussed herein and may e.g. be in the form of a Random Access Memory (RAM), a Flash memory or other solid state memory, or a hard disk, or be a combination thereof. The processor circuitry 31 may also be configured to store data in the storage 32, as needed. The network arrangement 13 also comprises a communication interface 33 for communication with other parts (e.g. nodes or elements) in the communication network 1 as well as with the sensor 5 over a radio interface.
Thus, according to an embodiment of the present disclosure, there is provided a network arrangement 13 for a communication network 1 comprising a RAN 2 and for facilitating resource management in the communication network of signalling relating to vehicles 4 which are connected to the network via the RAN. The arrangement 13 comprises processor circuitry 31, and storage 32 storing instructions 41 executable by said processor circuitry whereby said arrangement is operative to detect that a connected vehicle 4 is stationary. The arrangement 13 is also operative to obtain location information about in which location the vehicle 4 is stationary. The arrangement 13 is also operative to correlate the location information with security information. The arrangement 13 is also operative to determine number and type of sensors 5 in the vehicle 4 which connect to the communication network 1 when the vehicle is stationary in the location. The arrangement 13 is also operative to allocate network resources to the vehicle 4 based on the determining and on the correlated security information.

Figure 3b is a schematic block diagram functionally illustrating an embodiment of the network arrangement 13 in figure 3a. As previously mentioned, the processor circuitry 31 may run software 41 for enabling the network arrangement 13 to perform an embodiment of the method of the present disclosure, whereby functional modules may be formed in the network arrangement 13 e.g. in the processor circuitry 31 for performing the different steps of the method. These modules are in the figure schematically illustrated as blocks within the network arrangement 13.

Thus, according to an embodiment of the present disclosure, there is provided a network arrangement 13 for a communication network 1 comprising a RAN 2 and for facilitating resource management in the communication network of signalling relating to vehicles 4 which are connected to the network via the RAN. The arrangement 13 comprises means
(e.g. the detection module 34) for detecting that a connected vehicle 4 is stationary. The arrangement 13 also comprises means (e.g. the obtaining module 35) for obtaining location information about in which location the vehicle 4 is stationary. The arrangement 13 also comprises means (e.g. the correlation module 36) for correlating the location information with security information. The arrangement 13 also comprises means (e.g. the determining module 37) for determining number and type of sensors 5 in the vehicle 4 which connect to the communication network 1 when the vehicle is stationary in the location. The arrangement 13 also comprises means (e.g. the allocation module 38) for allocating network resources to the vehicle 4 based on the determining and on the correlated security information.

Figure 4 illustrates a computer program product 40. The computer program product 40 comprises a computer readable (e.g. non-volatile and/or non-transitory) medium 42 comprising a computer program 41 in the form of computer-executable components 41. The computer program/computer-executable components 41 may be configured to cause a network arrangement 13, e.g. as discussed herein, to perform an embodiment of the method of the present disclosure. The computer program/computer-executable components may be run on the processor circuitry 31 of the network arrangement 13 for causing it to perform the method. The computer program product 40 may e.g. be comprised in a storage unit or memory 32 comprised in the network arrangement 13 and associated with the processor circuitry 31. Alternatively, the computer program product 40 may be, or be part of, a separate, e.g. mobile, storage means/medium, such as a computer readable disc, e.g. CD or DVD or hard disc/drive, or a solid state storage medium, e.g. a RAM or Flash memory. Further examples of the storage medium 42 can include, but are not limited to, any type of disk including floppy disks, optical discs, DVD, CD-ROMs, microdrive, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, DRAMs, VRAMs, flash memory devices, magnetic or optical cards, nanosystems (including molecular
memory ICs), or any type of media or device suitable for storing instructions and/or data. Embodiments of the present disclosure may be conveniently implemented using one or more conventional general purpose or specialized digital computer, computing device, machine, or microprocessor, including one or more processors, memory and/or computer readable storage media programmed according to the teachings of the present disclosure. Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.

According to an aspect of the present disclosure, there is provided a computer program product 40 comprising computer-executable components 41 for causing a network arrangement 13 of the communication network 1 to perform an embodiment of the method of the present disclosure when the computer-executable components are run on processor circuitry 31 comprised in the arrangement 13.

According to another aspect of the present disclosure, there is provided a computer program 41 for facilitating resource management in a communication network 1 of signalling relating to vehicles 4 which are connected to the network via a RAN 2. The computer program comprises computer program code which is able to, when run on processor circuitry 31 of a network arrangement 13 of the communication network, cause the network arrangement to detect that a connected vehicle 4 is stationary. The code is also able to cause the network arrangement 13 to obtain location information about in which location the vehicle 4 is stationary. The code is also able to cause the network arrangement 13 to correlate the location information with security information. The code is also able to cause the network arrangement 13 to determine number and type of sensors 5 in the vehicle 4 which connect to the communication network 1 when the vehicle is stationary in the location. The code is also able to cause the network
arrangement 13 to allocate network resources to the vehicle 4 based on the determining and on the correlated security information.

According to another aspect of the present disclosure, there is provided a computer program product 40 comprising an embodiment of the computer program 41 of the present disclosure and a computer readable means 42 on which the computer program is stored.

Figure 5 is a schematic flow chart of an embodiment of the method of the present disclosure. The method is performed in a communication network 1 comprising a RAN 2 and the method is for facilitating resource management in the communication network of signalling relating to vehicles 4 which are connected to the network via the RAN. As discussed herein vehicles 4 may be connected to/via the network 1 by means of one or a plurality of sensors 4 which may or may not be active and signalling at any certain time (e.g. when the vehicle is stationary). The method may be performed by a network arrangement 13 comprised in the communication network 1.

That a connected vehicle 4 is stationary is detected Si. In some embodiments, the detecting Si comprises receiving signalling from a sensor 5 in the vehicle 4, the signalling indicating that the vehicle is stationary, which sensor is only activated when the vehicle is stationary or which sensor provides mobility and/or location information. The sensor(s) 5 may e.g. be activated automatically when the vehicle is stationary, thus indicating to the network arrangement 13 that the vehicle is stationary, and/or the sensor(s) may be activated by the network operator in response to observing that the vehicle is stationary within the communication network 1. and/or the sensor(s) may be activated manually by the user/driver of the vehicle when parking. In some embodiments, the detecting Si comprises determining that the vehicle 4 is stationary based on its mobility within the RAN 2, e.g. by means of any known network mobility process.
Then, location information about in which (geographical) location the vehicle 4 is stationary is obtained S2, e.g. GPS or longitude and latitude coordinates. In some embodiments, the obtaining S2 location information comprises receiving signalling from a location sensor 5 in the vehicle 4, e.g. a satellite navigation sensor such as a Global Positioning System (GPS), Global Navigation Satellite System (GLONASS) and/or Galileo satellite navigation sensor, or comprises obtaining S2 the location information by means of a positioning process in the RAN 2 e.g. triangulation. In some embodiments, the obtaining S2 location information comprises obtaining information about whether the location corresponds to a designated parking location e.g. a garage or parking lot or an undesignated parking location e.g. at a roadside. This information may indicate whether the location in which the vehicle is stationary is potentially unsafe or relatively safe (e.g. in a security monitored designated parking).

After the obtaining S2 of the location information, the location information is correlated S3 with security information. This security information may e.g. be provided for different positions (e.g. designated and/or undesignated parking locations) in a grid over a smart city, town, village or part thereof, or the like. The security information may be provided before or concurrently with the obtaining S2 of the location information but may also be continuously updated. For instance, new information may be added indicating that many resent thefts or break-ins of vehicles have occurred in an area, or that there is currently a fire or other emergency situation in an area making it unsuitable or risky for a stationary vehicle. In some embodiments, the correlating S3 comprises correlating the location information with information about historical and/or projected future movements of the vehicle 4. The network arrangement 13 may thus have information about e.g. where the vehicle 4 is regularly parked and at which times and for how long, as well as the route the vehicle may take between the parking locations, and may from this
information project future sensor signalling resources that will likely need to be allocated for the vehicle.

Before, concurrently with or after the correlating S3, the number and type/types of sensor(s) 5 in the vehicle 4 which connect (will be connecting, are in the process of connecting or have connected) to the communication network 1 when the vehicle is stationary in the location is determined S4. The network arrangement 13 may e.g. in real time detect how many and which sensors 5 of the vehicle 4 are connecting to the network 1, or the network arrangement 13 may project future sensor connections e.g. based on the correlating S3 of security information and/or historical and/or projected future movements or parking locations of the vehicle 4.

Network resources are allocated S5 to the vehicle 4 (e.g. to the signalling to/from sensors 5 of the vehicle) based on the determining S4 and on the correlated S3 security information. In some embodiments, the allocating S5 comprises setting a priority for at least some of the network resources based on the security information. For instance, if the security information indicates that the location the vehicle is stationary in is unsafe, a higher priority may be awarded to sensors (e.g. security sensors such as movement alarm, break-in alarm, sensor detecting that a wheel or hub cap is being removed, etc.) of that vehicle. With a higher priority, sensor signals may be allowed also in case of congestion in the communication network. In some embodiments, the allocating S5 comprises sending a notification to a driver/user or other personnel of the vehicle 4, e.g. to a smartphone of the driver or to a display of the vehicle, warning the driver that the location is unsafe and/or suggesting another location for parking the vehicle. The driver may thus activate additional security sensors 5 or move to another parking location. In some embodiments, the allocating S5 comprises allocating S5 the network resources, e.g. for modifying traffic flows, based on net uplink (UL) and downlink (DL) traffic, respectively, generated by the determined S4.
number and type of sensors. The number of sensors (e.g. heterogeneous security sensors) activating, deactivating, connecting, disconnecting leads to modification in net UL or DL traffic (per vehicle, or group of vehicles) flows as per different security applications, services, traffic classes etc. This is referred to as modification in traffic (uplink or downlink) flows.

In some embodiments of the present disclosure, the network resources being allocated comprise RAN resources, operator network resources and/or cloud communication resources.

In some embodiments of the present disclosure, the vehicle is a truck, car, motorcycle or bicycle. Alternatively, the vehicle may be any other type of vehicle.

In some embodiments of the present disclosure, the method is performed in a telecommunications operator network or in a cloud communication network comprised in the communication network 1.

EXAMPLE 1

Below follow a description of different modules in the network arrangement in accordance with an example embodiment.

The detection module 34

The detection module 34 may be configured for detecting whether one or more connected vehicles are stationary in one or more locations. Connected vehicles may include any network connected smart vehicle, like connected cycles, connected bikes, connected cars, connected SUV, connected trucks, connected buses, connected travellers, connected wagons etc.

The obtaining module 35
The obtaining module 35 may locate the connected vehicle using standard telecom localization procedures used for locating a User equipment (UE) inside the communication network 1. Telecom operators may easily determine if a connected vehicle 4/sensor 5 is changing its location in the network from one cell to another cell. The connected vehicle may be connected to a vehicle cloud, application and services through the 3GPP communication network 1.

**The correlation module 36**

The two following supporting matrixes are obtained and correlated with the location of the vehicle 4.

- Origin-Destination (OD) connected vehicle matrix. The OD matrix helps in understanding the commuting pattern of the connected vehicle 4 (or mobile M2M vehicle based sensors 5 whose locations also changes with vehicles).

- Location based safety and security incidents latitude-longitude matrix (security matrix). The security matrix may be a bit-matrix with binary 0 or 1 which helps with understanding the location based security hazards reported in the past.

The matrices help understand if the vehicle is stationary at a designated parking location likes at offices, multi-level parking garages, or at a non-designated parking like near a roadside. Matrix values would tell about vehicle mobility at a location (like multi level parking) and location based security assessment based on reported data in the security matrix. Vehicle commuting patterns in the OD matrix will help with understanding whether the vehicle 4 will be parked for at least a few hours (like during night at home, visiting office during day etc.).
Security incidents may be indirectly captured by analyzing the number of users or callers to police telephone number, fire brigade telephone number, Interactive voice response (IVR) etc. from one or more locations or a street asking for help. This would help in estimating the number of security/fire safety calls received on helpline numbers per street or location in a city.

Sample matrices for two locations A and B, such that the OD matrix tells that a vehicle 4 travels from A to B, while security matrix information for the B to A path has faced security issues in the past.

\[
\begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 \\
1 & 0
\end{bmatrix}
\]

Matrix values helps in understanding the frequent commuting patterns of stationary vehicles through secure and un-secure location paths, which further helps to understand the security sensor 5 based communication scenario possibilities currently active or which will occur in near time as per commuting patterns.

The determining module 37

Quantifying the metrics such as number and type of sensors in a vehicle, as per mobility patterns of the OD matrix involving a origin and destination, for understanding the number of connected vehicle based sensors 5 (or vehicle security sensor devices) connected, disconnected or reconnected per locations. Connection, disconnection and reconnection of sensor devices from the network 1, can be based on user driven, operator driven or service client driven actions which may be activated per location by operators, clients or by the user. Quantifying the number of devices would help in understanding sensor devices 5 connected, disconnected or reconnected from
the network to understand the traffic (uplink, downlink) modification induced by those sensor devices.

Quantification criteria may further include

- security client type,
- security service type,
- service provider type,
- security sensor device type,
- subscriptions type etc.

To understand the percentage of sensors connecting, disconnecting or reconnecting as per the criteria, the following formulas may be used.

\[
\%\text{Connect} = \frac{\text{Number of devices connected as per profile or criteria for the stopped connected vehicle}}{\text{Total number of devices per profile or criteria for the connected vehicle}} \times 100
\]

\[
\%\text{Disconnect} = \frac{\text{Number of devices disconnected as per profile or criteria for the stopped connected vehicle}}{\text{Total number of devices per profile or criteria for the connected vehicle}} \times 100
\]

\[
\%\text{Re-connect} = \frac{\text{Number of devices re-connected as per profile or criteria for the stopped connected vehicle}}{\text{Total number of devices per profile or criteria for the connected vehicle}} \times 100
\]

The allocation module 38

The allocation module may first activate resource consumption rules (security sensor related policy rules). A resource consumption rule may be
attached with the sensors 5 of a vehicle. Resource consumption rules may relate to e.g.:

- allocation,
- de-allocation,
- prioritization,
- de-prioritization

of network and cloud resources of the communication network 1 that can be used toward providing services to the user or system administrator. Resource consumption may use feedback from the determining module 37 to policy control and charging (PCC) nodes as well as to any device connection platform (if used by an operator). Feedback may comprise of %connect, %disconnect, %reconnect sensor devices in accordance with a criteria or profile as illustrated in figure 6.

Network resource consumption may involve Quality of Service (QoS), bandwidth and charging policy in accordance with the operator priorities (like subscription type, vehicle type, location type, street type, service provider 10 type, application type, service type, security priorities types). Cloud resources may include storage, processing power, memory, and databases which maybe redistributed depending on operator priorities.

The network impact type and magnitude of the connected sensors 5 may relate to connection, disconnection of sensor devices and traffic (uplink and downlink) modification involving one or more vehicle based sensor devices activated on its own when vehicle stops or activated by operator upon identifying a stopped (or parked) vehicle 4 in a connected vehicle ecosystem. To know how many sensors are coming on-line or going off-line at a time
would help an operator to provide optimum resources to the involved security sensors devices in various communication scenarios.

Attaching a resource consumption rule helps in optimizing the network resources as well prioritizing vehicle security based communication involving one or more sensor devices 5 throughout the 3GPP network 1. Thus, enabling better Quality of Experience (QoE) in security based communication involving one or more sensors devices 5.

Sensor communication scenarios may include:

- sensor 5 to sensor 5 communication,
- sensor 5 to network 1 communication,
- sensor 5 to infrastructure (e.g. roadside units, traffic lights, sensors in buildings e.g. in a parking garage) communication,
- infrastructure to sensor 5 communication,
- sensor 5 to user/driver communication,
- user/driver to sensor 5 communication,
- sensor 5 to infrastructure to user/driver communication (e.g. a sensor alerts a parking garage device about an issue, whereby the parking garage device contacts the driver of the vehicle which comprises the sensor),
- user/driver to infrastructure to sensor 5 communication, etc.

The consumption rules may then be enforced. Attaching the consumption rules may enforce some decision as per rule policy. These decision may help in enforcing the optimization, security, and legality policies in the network 1.

EXAMPLE 2
A connected vehicle (e.g. a car) going from a location to another location, such that it is parked near a roadside (non-designated parking location) a few times during the journey, besides being also parked in multi-level parking garages (designated parking location) a few times for varying time durations. A smart city with connected vehicles 4 would be such that parking locations, parking infrastructure, road infrastructure (street lights, traffic lights, roadside units), cars and other vehicles, road sensors, parking sensors etc. may be smart enough to provide valuable information to a driver on the road. For instance, road, location, vehicles, road and parking infrastructure may be smart enough to provide value based security services to vehicle owners or parking managers so as to provide a safe and secure parking environment.

It is possible that location based security driven analytics induces the activation of one or more heterogeneous sensors in a vehicle 5 or in the infrastructure surrounding the vehicle by the 3GPP operators or by the vehicle processing components itself. 3GPP operators may be connectivity providers or perform the connection management via a device connectivity platform.

In such smart cities, lots of security based communication scenarios may occur, involving one or more sensors 5 (present in the vehicle 4, infrastructure or other surroundings) as listed above.

Addressing the security- based heterogeneous sensor communication traffic optimization for stationary or parked vehicles in these scenarios for the parked vehicles at various locations (designated parking or roadside) would presents an opportunity for operators to understand scenarios and optimize the security sensor based communication traffic. Besides optimization, resource management and Service Level Agreement (SLA) enforcement are other opportunities presented herein which would help an operator to better
manage security based communication traffic e.g. per vehicle type like luxury vehicles, logistic industries etc.

In an example of matrices for a vehicle 4, the vehicle may be moving between eight locations as illustrated in figure 7a, such that it is stationary at these locations (including both designated and non-designated parking locations) for parking. The network arrangement would fetch the OD matrix and security matrix. The OD matrix of figure 7b includes a "1" for every location visited by the vehicle.

A security based latitude-longitude bit-matrix in figure 7c includes a "0" for any location without security concerns and a "1" for any locations with a recorded security concern or accidents in the past. In the example security matrix of the figure, paths (Location 3 to Location 4), (Location 7 to Location 8), (Location 8 to Location 1) are un-secure paths.

It is possible that a number of security sensors 5 are activated in parked vehicles 4, infrastructure, parking locations etc., such that activated sensors connects, disconnects or reconnects to the communication network 1 on inception or detection of an event or the sensors are activated by 3GPP operator at a location. Sensor activation may be event detection driven logic present in vehicles using short range communication technologies or by 3GPP operator using 3GPP network technologies towards connected vehicles subscriptions based on security analytics performed in connected vehicle cloud or for locations or for streets by operators using network data, e.g. GPS data.

Security sensors 5 may be triggered in the surrounding of the parked vehicle or in the vehicle itself for the location coordinates like multi-level parking locations, any roadside locations or they may be active for the complete journey of the unsafe paths (3-4), (7-8) and (8-1) of figure 7a.
Studying frequent commuting patterns of parked vehicles through secure and insecure locations would help in understanding the scope of security sensor based communication possibilities for a connected vehicle in the smart city network.

These sensors may communicate in various cases, even when no security issue is present so as to timely inform a user or parking attendant about parked vehicles' status by collecting data from security sensors of the vehicles and doing some analytics on the same in the parking locations.

The large number of sensor devices, in vehicles, infrastructure, parking and near roadside infrastructure etc., may be activated (connected, disconnected, reconnected) in accordance with internal logic or by external triggering, and tries to communicate among each other, with users or parking attendants in varying mentioned ways.

Large volumes of security based heterogeneous sensor devices activating, deactivating or reactivating as illustrated in figure 8 for the parked vehicles or in the infrastructure surrounding the vehicles, be it in a road or parking lot, during the night or during the day time, at various locations around the city, and communicating in various communication scenarios can be studied by means of embodiments of the present disclosure.

Sensors may be connected/ disconnected:

Remotely, via a communication channel, e.g. a 3GPP operator triggers one or more sensors in the vehicle or in surrounding infrastructure, see remote_disconnect, remote_reconnect in figure 8;

Manually, using e.g. a push button as for hazard lights sensors activated explicitly by the driver while parking near a roadside, which may in smart cities also indirectly activate one or more sensors in the surrounding
infrastructure and vehicles, see manual_disconnect, manual_reconnect in figure 8; or

Locally (automatically by the sensor or vehicle itself), by a function or internal logic, e.g. event detection by internal security sensor of a vehicle, see local_disconnect, local_reconnect in figure 8.

%connected, %disconnected and %reconnected sensor devices 5 for parked vehicles 4 may be understood by operators using above formulas to help understand the type or number of security sensor devices activated in the network 1.

Quantification of the magnitude in term of e.g. number, type, percentage, proportion, fraction etc. of security-based sensor devices in vehicles 4, infrastructure and/or surroundings which are connecting, disconnecting or reconnecting to the network 1 for the parked vehicles, would help understanding the number of heterogeneous devices pushing or downloading data (as per different traffic class) from the network in accordance with for instance:

- security service client (herein alternatively called application) type,
- security service type,
- service provider type,
- sensor type,
- subscription type etc.

Quantification of impact on/magnitude of required network resources may be studied in accordance with e.g. the following view points:
(a) Uplink and downlink communication traffic modification (increase or decreases) due to these heterogeneous sensors based communication in the network in various use cases. Since the sensors are activated, they start pushing or downloading data from the network as per application, services, service provider, device type, subscriptions types etc. It is possible they start setting up one or more communication scenarios mentioned above to request or respond to changes.

(b) Connect, disconnect request related communication traffic load on Device Connectivity Platform (DCP) due to the heterogeneous sensors devices activating and deactivating in the network.

(c) Traffic prioritization or de-prioritization relating to the security in various mentioned communication scenarios application, services, service provider, device type, subscriptions types, traffic classes etc.

(d) Peak load due to the sensors at times when large number of vehicles are parked near roadside during night time or during day at office parking locations for different time durations.

(e) Resource management relating to managing of network and cloud resources. Network resources includes QoS, bandwidth and charging and Cloud resources includes memory, processing power, storages etc. Allocation or de-allocation of various resources in relation to security application and services.

(f) SLA enforcement relating to the security related communication involving heterogeneous sensors in various communication scenarios. Enforcing a particular SLA in relation to a security based application and services at a point in time.

(g) Legal Management: Legal policies may be answered by PCRF policy control mechanisms by enforcing one or more security-based sensor
communication formats like modifying the time period or frequency when pinging to a server (relating to a security function, logging) if a vehicle has just detected that it is party to an accident on road. Insurance companies can request enforcing legal policies on the communication format of the security-based sensors to the server in both self triggering or external triggering relating of one or more sensors in one or more environmental conditions. Further, on inception of an event at one place in a parking location, a parking attendant can enforce changing of communication format of one or more types of security-based sensors (in vehicle, in parking location, in infrastructure) so to be legally complaint with the insurance agencies requirement if a security hazard takes place inside the official parking locations.

The feedback comprising of impact type, magnitude and criteria may be shared with PCC and DCP nodes to help prioritize, allocate or de-allocate resources using the feedback, as shown in figure 6.

PCC may use the feedback to develop policy profiles relating QoS, bandwidth and charging as per the impact feedback, which activates in accordance with the conditions which are found true and decision of resource management are enforced upon the security communications relating the parked vehicle.

For example:

PCC Policy profile 1: Prioritization of security-based sensor communication traffic (Uplink and Downlink) as per traffic classes relating gold category subscription based luxury vehicles at a location or per mobility pattern between origin and destination, over silver categories subscriptions based connected vehicles.
PCC Policy Profile 2: QoS and charging differentiations of different security-based sensor communication scenarios involving smart vehicle, parking, infra-structures, user and the network in a smart city use cases.

Location or journey route based security traffic prioritizations / de-prioritization may be targeted for the parked vehicles at one or more locations.

An example of PCC node flow is presented in figure 9.

**EXAMPLE 3**

Implementation of embodiments of the present disclosure based on Value Added Service (VAS) recommendation for a secure location use case.

**Value Added Service:** For people driving to an unsecure parking location, a recommendation for a more secure location may be provided.

**Use case:** Consider a user taking a drive from A to B. When the user reaches the location \((x_1, y_1)\) he parks, whereby the system pops up a notification on his smart-phone, indicating it as an unsecure location and proposes him to go to another location \((x_2, y_2)\) for parking, which is secure and has vacant parking spots.

**Step 1:** The user drives in and tries to park his vehicle 4. When stationary, the vehicle is detected by the operator using standard procedures like network data, location based data, M2M data etc., relating 3GPP subscriber identity module (SIM).

**Step 2:** The network arrangement obtains the matrices - OD and security matrices for the location. These matrices are maintained at the operator as per locations with crime rate per location etc., to mark a location as secure or unsecured.
Matrix cell values shows secure and unsecured locations.

Matrix below shows user moving from A to B:

$$\text{OD Matrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

The security matrix below shows that location B (Cell [1,2]) is an unsecure location, and location C (Cell [1,3]) (column 3) is a secure parking location available near to the vehicle.

$$\text{Latitude Longitude Security Bit Matrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Step 3: As per cell value from the security matrices, the operator sends the recommendation to the user to go back to his vehicle, recommending him to use another parking C a few meters away since this location B is an unsecure location. Further, the operator may also recommend him that a designated parking location has a few vacant parking slots at this time.

It's up to the user to accept the new parking recommendations, but if the user still decides to park his vehicle in the unsecure location, in accordance with the vehicle's current location (secure or unsecure), operators may actuate one or more internal sensors of the vehicle to provide a kind of security cover, enable security based network services using security matrices inputs as shown above. One such network service could be allowing the vehicle to update its state (capturing vital vehicle parameters) to its user periodically using any communication mechanism (call, SMS, twitter update etc.). If the vehicle is parked in the basement of an unsecured location, where radio network signals are weak, the vehicle could try Wi-Fi calling to the user device as a communication mechanism.
Similarly, an operator may quantify a set of vehicles parked at different places as per OD and security matrices, and quantifying using filled lists of vehicle/devices as per the service type (like SMS), application type (like twitter updates), UL/DL communication traffic modification per vehicles gateways, when vehicle is triggered (sensor actuated) as per location to communicate to the user its current state or vital parameters using different communication methods possible at its end.

Step 4: Attach a resource consumption rule e.g. in accordance with security traffic class, vehicle type, application type, service type or as per a criteria set by the operator to differentiate different categories so to sub divide different list of devices 5. Filled lists show the quantified data. It may be represented/sub-divided as per the % change discussed herein.

In a current example, if a vehicle 4 initiates a Wi-Fi call from an unsecured basement parking which is actuated by internal vehicle sensors triggered by operator intelligence using OD and security matrices, then this step may allocate resources to all such vehicles 4 parked in unsecured locations taking suitable network action (i.e. making a Wi-Fi call, or SMS, twitter updates) to talk/update its user regarding the network service action taken.

Step 5: Activate resource consumption rule as per operator criteria and enforce the decisions so as to enable optimized security communication.

By means of embodiments of the present disclosure, sensor communication for stationary vehicles may be optimized for different use cases (including security and legal) and different stakeholders (business partners, subscribers, operators) in designated or non-designed parking locations in smart cities.

The present disclosure has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally
possible within the scope of the present disclosure, as defined by the appended claims.
CLAMS

1. A method performed in a communication network (1) comprising a Radio Access Network, RAN, (2) for facilitating resource management in the communication network of signalling relating to vehicles (4) which are connected to the network via the RAN, the method comprising:

- detecting (Si) that a connected vehicle (4) is stationary;
- obtaining (S2) location information about in which location the vehicle (4) is stationary;
- correlating (S3) the location information with security information;
- determining (S4) number and type of sensors (5) in the vehicle (4) which connect to the communication network (1) when the vehicle is stationary in the location; and
- allocating (S5) network resources to the vehicle (4) based on the determining (S4) and on the correlated (S3) security information.

2. The method of claim 1, wherein the detecting (Si) comprises receiving signalling from a sensor (5) in the vehicle (4), the signalling indicating that the vehicle is stationary, which sensor is only activated when the vehicle is stationary or which sensor provides mobility and/or location information.

3. The method of claim 1, wherein the detecting (Si) comprises determining that the vehicle (4) is stationary based on its mobility within the RAN (2).

4. The method of any preceding claim, wherein the obtaining (S2) location information comprises receiving signalling from a location sensor (5) in the vehicle (4), e.g. a satellite navigation sensor such as a Global Positioning System, GPS; Global Navigation Satellite System, GLONASS; and/or Galileo
satellite navigation sensor; or comprises obtaining (S2) the location information by means of a positioning process in the RAN e.g. triangulation.

5. The method of any preceding claim, wherein the obtaining (S2) location information comprises obtaining information about whether the location corresponds to a designated parking location e.g. a garage or parking lot or an undesignated parking location e.g. at a roadside.

6. The method of any preceding claim, wherein the correlating (S3) also comprises correlating the location information with information about historical and/or projected future movements of the vehicle (4).

7. The method of any preceding claim, wherein the determining (S4) comprises determining which services should be provided to the vehicle.

8. The method of any preceding claim, wherein the allocating (S5) comprises setting a priority for at least some of the network resources based on the security information.

9. The method of any preceding claim, wherein the allocating (S5) comprises sending a notification to a driver of the vehicle (4), e.g. to a smartphone of the driver or to a display of the vehicle, warning the driver that the location is unsafe and/or suggesting another location for parking the vehicle.

10. The method of any preceding claim, wherein the allocating (S5) comprises allocating (S5) the network resources for modifying traffic flows based on net uplink and downlink traffic, respectively, generated by the determined (S4) number and type of sensors (5).

11. The method of any preceding claim, wherein the network resources comprise RAN resources, operator network resources and/or cloud communication resources.
12. The method of any preceding claim, wherein the vehicle is a truck, car, motorcycle or bicycle.

13. The method of any preceding claim, wherein the method is performed in a telecommunications operator network or in a cloud communication network comprised in the communication network (1).

14. A computer program product (40) comprising computer-executable components (41) for causing a network arrangement (13) of the communication network (1) to perform the method of any one of claims 1-13 when the computer-executable components are run on processor circuitry (31) comprised in the arrangement.

15. A network arrangement (13) for a communication network (1) comprising a Radio Access Network, RAN, (2), and for facilitating resource management in the communication network of signalling relating to vehicles (4) which are connected to the network via the RAN, the arrangement comprising:

processor circuitry (31); and

storage (32) storing instructions (41) executable by said processor circuitry whereby said arrangement is operative to:

detect that a connected vehicle (4) is stationary;

obtain location information about in which location the vehicle (4) is stationary;

correlate the location information with security information;

determine number and type of sensors (5) in the vehicle (4) which connect to the communication network (1) when the vehicle is stationary in the location; and
allocate network resources to the vehicle (4) based on the determining and on the correlated security information.

16. A computer program (41) for facilitating resource management in a communication network (1) of signalling relating to vehicles (4) which are connected to the network via a Radio Access Network, RAN, (2), the computer program comprising computer program code which is able to, when run on processor circuitry (31) of a network arrangement (13) of the communication network, cause the network arrangement to:

detect (S1) that a connected vehicle (4) is stationary;

obtain (S2) location information about in which location the vehicle (4) is stationary;

correlate (S3) the location information with security information;

determine (S4) number and type of sensors (5) in the vehicle (4) which connect to the communication network (1) when the vehicle is stationary in the location; and

allocate (S5) network resources to the vehicle (4) based on the determining (S4) and on the correlated (S3) security information.

17. A computer program product (40) comprising a computer program (41) according to claim 16 and a computer readable means (42) on which the computer program is stored.
**Fig. 4**

1. **S1** Detecting stationary vehicle
2. **S2** Obtaining location
3. **S3** Correlating security info
4. **S4** Determining sensors
5. **S5** Allocating resources

**Fig. 5**
Fig. 6

Fig. 7a
O-M Matrix =
\[
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

Fig. 7b

Security based Latitude-Longitude Bit-Matrix =
\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

Fig. 7c

Policy Designer Interface
Policy Profiles
Policy Controller
Policy Decision
Enforce Policy Decision

Network Application Data
Subscription Data
Charging Data

Feedback
Policy profiles (QoS, bandwidth, charging) relating feedback as per Magnitude of devices and criteria

Fig. 8
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
G08G1/123, H04W2/8/00, G06F17/00, G08B23/00 Version=2.015.01

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)
G08G, H04W, G06F, G08B

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)

DATABASES: PATSEER, IPO INTERNAL
SEARCH TERMS: WIRELESS, SENSOR, VEHICLE, PARKING, CORRELATION

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>A</td>
<td>US2013073143 A1 (TOYOTA MOTOR CO LTD), 21 MARCH 2013 (21-03-2013); Paragraph :=[102], Lines := [1]-[3]</td>
<td>1-13, 15</td>
</tr>
<tr>
<td>A</td>
<td>US8686864 B2 (MARWAN, Hannon), 01 APRIL 2014 (01-04-2014); Paragraph := [4], Lines := [1]-[9])</td>
<td>1-13, 15</td>
</tr>
</tbody>
</table>

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
  "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

"Y" 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

"X" 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
20-11-2015

Date of mailing of the international search report
20-11-2015

Name and mailing address of the ISA/Indian Patent Office
Plot No. 32, Sector 14, Dwarka, New Delhi-110075

Facsimile No.

Authorized officer
Hitendra Sharma

Telephone No. +91-1125300200

Form PCT/ISA/210 (second sheet) (January 2015)
This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 14, 16–17 because they relate to subject matter not required to be searched by this Authority, namely: 

   The claims relate to computer program product.

2. ☐ Claims Nos.: because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☒ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☒ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.
<table>
<thead>
<tr>
<th>Citation</th>
<th>Pub. Date</th>
<th>Family</th>
<th>Pub. Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>JP 4435845 B2</td>
<td>24-03-2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2007122926 A1</td>
<td>01-11-2007</td>
</tr>
<tr>
<td>us 2013073143 A1</td>
<td>21-03-2013</td>
<td>WO 2013035129 A1</td>
<td>14-03-2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 8676495 B2</td>
<td>18-03-2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2014180500 A1</td>
<td>26-06-2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2015057342 A</td>
<td>26-03-2015</td>
</tr>
</tbody>
</table>