

DEVICES AND METHODS FOR PROVIDING ACCESS TO A NETWORK

TECHNICAL FIELD

[0001] Methods and devices for providing access to a network are described. The
5 devices and methods can be used in particular in the context of providing network access
to a user device through a shared connection with a cellular phone through an intermediate
device acting as a wireless access point. More specifically, the context can be the
anonymous peer-to-peer sharing of a cellular data plan.

10 BACKGROUND

[0002] In the digital age, mobile data usage has become an integral part of
everyday life. However, traditional data plans and contracts often impose limitations,
leading to inefficiencies and suboptimal resource utilization. Users frequently encounter
situations where their purchased data plans go underutilized, resulting in wasted resources
15 and unnecessary cost. Simultaneously, many users require additional data but lack
flexible and cost-effective options to meet their specific needs.

[0003] In the latter case, users have the option to de-activate their data access
based on the data plan of their cellular phone and restrict connectivity to the sole
20 connection provided by a wireless access point connected to the internet, such as a public
hotspot in a shop or in dedicated urban areas. Such hotspots are not available everywhere
and require the user to be within a limited range of the wireless access point creating the
hotspot.

[0004] Users can also borrow connectivity from a phone owner using their
25 cellular phone to set up a hotspot for connection sharing. Access to such a hotspot requires
approval of the owner of the cellular phone acting as hotspot. In such a situation, the user
must know the password of the personal hotspot, and – in most cases – physically identify
the person sharing their personal hotspot. This may lead to a forced and unnecessary
social link, leaving little room for the owner of a smartphone to decline sharing identity.

30

[0005] These methods may compromise security, expose personal information,

or involve rigid contractual agreements. In practice, it is today difficult to legally connect to the personal hotspot of a phone owner without knowing this owner and interacting with them to get the password of their shared connection. It is also impossible to measure the quantity of data a user has used from the shared connection of a smartphone without
5 asking the phone owner to check on their smartphone in real time.

[0006] There is thus a need for a technical solution that would provide a user-friendly, secure, and anonymous mobile data sharing system, in order to leverage the global presence of cellular phones in the surrounding that can serve as internet access
10 points, and yet preserve anonymity of the transaction, and thus the safety of the parties sharing these data.

SUMMARY

15 [0007] A first aspect concerns a method for data transfer over a communication network, in a system comprising:

- a first communication device comprising a communication interface configured to provide:

- a wireless connection to a second communication device;
- 20 ○ a wireless access point for providing a wireless network;

the second device comprising a communication interface configured to provide a shared connection to a communication network to the first device, wherein the shared connection is adapted to enable data transfer over the communication network;

25 - a third communication device comprising a communication interface to connect to the wireless network of the access point of the first device;

the method comprising, at the third device:

- obtaining, by the third device, information representative of at least one offer for transferring data over the shared connection of the second device;
- 30 - in response to the transmission of a message indicative of acceptance of a received offer, receiving access, by the third device, to the shared connection

corresponding to the accepted offer for transferring data according to one or more conditions of the accepted offer, wherein communication between the second device and the third device, of said data, is performed solely through the first device.

5

[0008] It is in practice the first device that effectively connects to the shared connection and allows the third device to obtain and send data. Credentials necessary for allowing access to the shared connection, e.g. a password, a name of the second device providing the shared connection... need not be communicated to the third device, which
10 can connect to the first device for the purpose of benefiting from the shared connection. The anonymity of the person controlling the first device capable of the shared connection is preserved.

[0009] A user of the third device can thus benefit from a data plan, without having their own subscription to such a plan. Also, only the desired or needed quantity of data
15 can be acquired, i.e. there is less waste.

[0010] According to an embodiment, the method further comprises, before enabling access, validating a transaction authorizing payment of a price associated with the accepted offer.

20 [0011] According to an embodiment, the wireless network has a network identifier indicating to the third device that the first device is adapted to provide access to the shared connection.

[0012] The third device can thus easily detect wireless networks provided by first devices that are connected to a shared connection from which the third device may
25 possibly benefit.

[0013] According to an embodiment, the system comprises a plurality of first devices connected to respective second devices, each first device providing a given wireless network, all given wireless networks using a same network identifier, the
30 network identifier being known to the third device.

[0014] According to an embodiment, the obtaining, by the third communication

device, of information representative of at least one offer for data transfer over the shared connection of the second communication device comprises, at the third device:

- detecting the wireless network of the first device using the network identifier of the first device;
- 5 - obtaining the information representative of at least one offer for data transfer over the shared connection of the second communication device through the first device.

[0015] According to an embodiment, the information representative of an offer
10 comprises an amount of data to be transferred and the price for enabling transfer of the amount of data.

[0016] According to an embodiment, the information representative of an offer further comprises an estimated time of presence of the second device at a current geographical location.

15 [0017] According to an embodiment, the information representative of an offer comprises no information concerning the identity of said user of the first device.

[0018] According to an embodiment, the communication network is a cellular network and the second device is a cellular phone.

20 [0019] According to an embodiment, validating a transaction authorizing payment of a price associated with the accepted offer is performed by a software application executed by the third device, the method further comprising

- transmission of an information indicative of the validation of the transaction by the third device to the first device;
- 25 - transmission of the information indicative of the validation of the transaction by the first device to the second device;
- enabling access to the shared connection by the second device responsive to the information indicative of the validation of the transaction.

[0020] According to an embodiment, the method further comprises, at the third
30 device,

- detection of the wireless network of the first device using the predefined network identifier;
- obtaining the information representative of the at least one offer for data transfer through the first device.

5 [0021] According to an embodiment, the system further comprising a cloud server, the method further comprises:

- obtaining, by the third device, from the cloud server, information representative of at least one offer for data transfer of the second device as a function of a geographic location of the second device and a geographic location of the third device.
- 10

[0022] According to an embodiment, the method further comprises, at the third device:

- sending, to the cloud server, an information indicative of the accepted offer;
- 15 - receiving, from the cloud server, information enabling the connection of the third device to the wireless network of the first device connected to the second device for the purpose of transferring data over the shared connection;
- connecting to the wireless network using the information enabling the connection.

20 [0023] According to an embodiment, the method further comprises registration of the third device with the cloud server, comprising setting up a purse for transaction payment at the cloud server.

[0024] A second aspect concerns a third communication device, comprising a processor and, memory comprising software code, the third communication device being
25 configured to carry out one of the methods as disclosed herein.

[0025] A third aspect concerns a method for data transfer over a communication network, in a system comprising:

- 30 - a first communication device comprising a communication interface configured to provide:

- a wireless connection to a second communication device;
 - a wireless access point for providing a wireless network;
- the second device comprising a communication interface configured to provide a shared connection to a communication network to the first device, wherein the
- 5 shared connection is adapted to enable data transfer over the communication network;
- a third communication device comprising a communication interface to connect to the wireless network of the access point of the first device;
- the method comprising, at the second device:
- 10
- enabling the shared connection;
 - configuring the first device to allow the first device to connect to the shared connection;
 - providing information representative of at least one offer for transferring data over the shared connection, for obtention by the third device, wherein
- 15 communication between the second device and the third device of said data upon acceptance of an offer is performed solely through the first device.

- [0026] According to an embodiment, the system further comprising a cloud server, providing information representative of at least one offer comprises
- 20
- transmitting said information, by the second device to the cloud server, wherein information of an offer comprises an amount of data to be transferred and a price for enabling transfer of the amount of data.

- [0027] According to an embodiment, said information comprises a current geographical location of the second device.

- 25 [0028] According to an embodiment, said information comprises an estimated time of presence of the second device at the current geographical location.

- [0029] A fourth aspect concerns a second communication device, comprising a processor and, memory comprising software code, the third communication device being
- 30 configured to carry out one of the methods disclosed herein.

[0030] A fifth aspect concerns a method for data transfer over a communication network, in a system comprising:

- a first communication device comprising a communication interface configured to provide:

- 5 ○ a wireless connection to a second communication device;
 - a wireless access point for providing a wireless network;
- the second device comprising a communication interface configured to provide a shared connection to a communication network to the first device, wherein the shared connection is adapted to enable data transfer over the communication
- 10 network;

- a third communication device comprising a communication interface to connect to the wireless network of the access point of the first device;

the method comprising, at the first device:

- connecting to the shared connection of the second device;
- 15 - providing said wireless network for connection by the third device;
- responsive to information indicative of acceptance by the third device of an offer for transferring data over the shared connection of the second device, transferring said data between the second device and the third device.

20 [0031] A sixth aspect concerns communication device, comprising a processor and, memory comprising software code, the third communication device being configured to carry out one of the methods disclosed herein.

[0032] Non-transitory computer-readable storage medium comprising instructions that when executed cause a processor of a computing device to carry out the

25 steps according to one of the methods disclosed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] Example embodiments will be more fully understood from the detailed description provided herein and the accompanying drawings, which are given by way of

30 illustration only.

Fig. 1 is a schematic diagram of a system according to a non-limiting embodiment.

Fig. 2 is a schematic diagram of one of the devices of the system of Fig. 1.

Fig. 3 is a screen copy of an application run by one of the devices of Fig. 1 for offering an amount of data for use according to a non-limiting embodiment.

Fig. 4 is a screen copy of an application run by another one of the devices of Fig. 1 for
5 requesting an amount of data for use according to a non-limiting embodiment.

Fig. 5 is a flowchart of a method implemented in the application according to a non-limiting embodiment.

Fig. 6 is a diagram schematically illustrating the use of a cloud server within the system described above according to one embodiment.

10 Fig. 7 is a diagram schematically illustrating the use of a cloud server within the system described above according to another embodiment.

Fig. 8 is a diagram schematically illustrating the use of a cloud server within the system described above according to yet another embodiment, involving the use of electronic purses at the user devices.

15 Fig. 9 is a diagram schematically illustrating the use of a cloud server within the system described above according to yet another embodiment, involving the use of electronic purses at the server.

DETAILED DESCRIPTION

20 [0034] Various exemplary embodiments will now be described more fully with reference to the accompanying drawings. However, specific structural and functional details disclosed herein are merely representative for purposes of describing example embodiments. The exemplary embodiments may be embodied in many alternate forms and should not be construed as limited to only the embodiments set forth herein. It should
25 be understood that there is no intent to limit example embodiments to the particular forms disclosed.

[0035] It should be appreciated by those skilled in the art that any functions, engines, block diagrams, flow diagrams, state transition diagrams, message sequence
30 charts and / or flowcharts herein represent conceptual views of illustrative circuitry embodying the principles of the exemplary embodiments. Functions, actions or steps

described herein can be implemented in hardware or software or any combination thereof, and ordering of these functions, actions or steps may be different from that presented. If implemented in software, the functions, blocks of the block diagrams and/or flowchart illustrations can be implemented e.g. using software code executed by a processor or a
5 processing device.

[0036] In the present description, functional blocks denoted as “means configured to perform ...” a certain function are to be understood as functional blocks comprising circuitry that is adapted for performing or configured to perform a certain function.
10 Moreover, any entity described herein as “means”, may be implemented as one or more distinct entities or within an entity providing additional functions. When provided by a processor, the functions may be provided by a single processor or several processors. Moreover, the term “processor” includes one or more of a digital signal processor, remote processor, graphical processing units (‘GPUs’), dedicated or generic circuitry, read only
15 memory for storing software, random access memory, and non-volatile storage.

[0037] The present invention addresses the technical challenges mentioned above by introducing a novel peer-to-peer mobile data sharing and transaction system that leverages a small electronic device (named a “#dot”) distinct from the device (e.g. cellular
20 phone) providing a network access through a shared connection and from the user device seeking to obtain connectivity. The intermediate device (i.e. the “#dot” device) connects to the device capable of providing the shared connection via a wireless connection such as WiFi (IEEE 802.11) or Bluetooth. The intermediate device acts as a mobile access point and creates an independent wireless network that a user device seeking connectivity
25 can access.

[0038] It is in practice the intermediate device that effectively uses the shared connection. For this purpose, the intermediate device and the device capable of providing the shared connection over the cellular network are configured (‘paired’) under the control of the person controlling the device capable of providing the shared connection
30 to allow use of this shared connection by the intermediate device. Credentials necessary for allowing access to the shared connection, e.g. a password, a name of the device

providing the shared connection..., are used only during the pairing phase between the intermediate device and the device capable of providing the shared connection and are not communicated to any user device seeking connectivity. The person ('seller') controlling the device capable of providing the shared connection determines one or more

5 conditions for use of the shared connection, through the intermediate device, for data transfer by a user device (e.g. one or more among a limit to the quantity of data, a price for a quantity of data, a time of presence at or close to the current geographical location...). The intermediate device creates a wireless network and allows connection by a user device in a simple way. E.g. a user device can easily spot a wireless network of an

10 intermediate device based on characteristics an identifier of the network. For example, this identifier is known in advance to a user device. The user ('buyer') of the user device views the conditions of use and can accept the conditions (e.g. the buyer may accept to pay a certain price for a certain amount of data), in which case the intermediate device can be used for data transfer under the accepted conditions.

15 [0039] In this way, the credentials of the device capable of the shared connection are not communicated to the user device and the anonymity of the person controlling the device capable of the shared connection is preserved.

[0040] Figure 1 is a block diagram of a system showing a wireless hotspot device 101 (also referred to as seller user device), an intermediate device 102 and a buyer user device 103 according to a one or more embodiments. The wireless hotspot device 101 provides internet connectivity. The wireless hotspot device 101 and the intermediate device 102 can communicate using a wireless connection, e.g. a wireless station interface of the intermediate device 102 may connect to an access point of the hotspot device 101. The intermediate device 102 and the buyer user device 103 communicate over a specific

20 wireless network created by the intermediate device 102 as disclosed herein. The user device 103 may be any device configured to make use of internet connectivity, including but not limited to a smartphone, a personal computer, a tablet, a wearable device.

[0041] The intermediate device 102 has knowledge or is provided with the information necessary to connect to the hotspot device 101. The connection of the two

30 devices 101 and 102 is also referred to as the two devices being 'paired'.

[0042] According to one non-limiting embodiment, an intermediate device

connects to only one hotspot device at a time.

[0043] A typical use case comprises the hotspot device (a cellular phone in the embodiments described herein) and the intermediate device being controlled by a same person. The person uses the intermediate device to create an easily accessible specific
5 wireless network that provides a certain anonymity to that person, as compared to offering direct access to a shared connection provided by the hotspot device.

[0044] According to one non-limiting embodiment, an unpaired intermediate device carries out the following:

- it creates a wireless network visible and identifiable by any compatible devices capable
10 of providing a shared connection and seeking to pair with it;
 - it provides a pairing password upon reception of a request over the wireless network from a hotspot device running a software application allowing pairing to be performed.
- Any compatible hotspot-capable device may then pair with the intermediate device. Once this is done, the seller user device activates connection sharing and allows the
15 intermediate device to connect to it as a hotspot. The seller user device may need to deactivate its WiFi in order to allow the seller user device to function as hotspot. According to a variant embodiment, the pairing password is well known and identical for all intermediate devices, i.e. it is known in advance by a device wishing to pair with an intermediate device.

20

[0045] According to one or more embodiments, a wireless network created by intermediate device 102 for access by user device 103 bears a predetermined identifier that allows this wireless network to be identified by a user device as providing connectivity as described. For example, the wireless network bears a predetermined
25 SSID, e.g. “#dot:dot”. The predetermined name is known to the user device, allowing it to detect the wireless network provided by the intermediate device.

[0046] According to an embodiment, several pairs of intermediate devices and hotspot device may be in the wireless range of the buyer user device. In such a case, distinct wireless networks created by distinct intermediate devices bear a same SSID,
30 meaning that two such networks created by intermediate devices paired to distinct hotspot devices won't be differentiated through their SSIDs. They will however be distinguished

within a software application running on the buyer user device, through which the buyer user device will be able to see surrounding intermediate devices and select the one they want to connect to.

5 [0047] Fig. 2 is a schematic block diagram of an intermediate device 102 according to one or more non-limiting embodiments. The intermediate device comprises a processor 201. The intermediate device also comprises a wireless radio 203, which provides a wireless network access point functionality. For example, radio 203 is an IEEE 802.11 compatible radio. The intermediate device 102 also comprises a wireless station
10 interface 204 for connecting to wireless hotspot 101. Processor 201 and radio 203 are shown separately, but in practice may be integrated into one component or shared among more than two components. The processor may be a microcontroller. For example, the processor can be an ESP32 or ESP8266 from Espressif, a nRF7002 from Nordic, or a CC32x0 or CC3235 from Texas Instruments. These processors integrate part of the
15 wireless radio functionality. In one embodiment, the radio 203 is compatible with the wireless radio frequencies of smartphones, i.e. at present 2.4 GHz or 5 GHz. The intermediate device also comprises a memory 202 holding software code. The processor 201, when executing the code, causes device 102 to carry out the methods described herein.

20 [0048] According to one or more embodiments, an intermediate device 102 is configured to repeat any compatible wireless hotspot, e.g. such as a hotspot stemming from a shared connection of a cellular phone. As indicated above, the wireless hotspot device 101 has internet connectivity. A wireless station, STA, of the intermediate device 102 is capable of connecting to the hotspot device 101 access point, and an access point,
25 AP, 203 of the intermediate device creates a wireless network with the predetermined SSID, e.g. “#dot:dot”, visible to other devices.

[0049] Devices 101 and 103 each comprise communication interfaces for carrying out the disclosed types of communication (e.g. cellular and wireless LAN), as well as a processor and memory, containing software code.

30 [0050] Any buyer user device seeking connectivity, e.g., a cellular phone, can connect to the wireless network or networks created by the intermediate device or devices,

either with no password, or with a password that is publicly known. The buyer user device however does not know the password to the shared connection.

[0051] In the example embodiment that follows, the hotspot device and the
5 intermediate device are described as being controlled by same person. This is however simply an illustrative use case, and the teachings derived from the embodiment also extend to use cases where the hotspot device and the intermediate device are controlled by distinct people.

[0052] The person controlling a hotspot device paired with an intermediate device
10 will have created an account in a software application, e.g. an application running on the controlling person's hotspot device or another device adapted to running a software application. This person is also referred to as the 'seller'.

[0053] According to one or more embodiments, account information of the seller
15 includes information allowing a payment to be made by a third party (e.g. the buyer using buyer user device 103) to the person's bank account, a Paypal or Stripe account or another type of monetary account. This information may for example be a tag. The tag identifies the account but does not allow direct identification of the seller by a buyer.

[0054] According to one or more embodiments, when pairing an intermediate
20 device with a hotspot device, the application of the hotspot device shares a quantity of data (e.g. the number of gigabytes) offered by the seller, and the financial tag mentioned above.

[0055] According to an optional feature, the hotspot device may also share a price for the quantity of data. The price may be zero (in case the seller wishes to provide a data allowance for free) or different from zero.

25 [0056] Optionally, the application of the hotspot device also shares an estimate of the time of presence of the seller at the geographic location where they are sharing their connection.

[0057] The information described in the two preceding paragraphs, as well as an identifier (e.g. the MAC ID number) of the intermediate device, can then be obtained
30 from the intermediate device by a third-party device (such as a buyer user device seeking connectivity).

[0058] Fig. 3 shows an exemplary screen displayed by the application to a given seller seeking to offer a certain amount of data, according to one non-limiting embodiment. E.g. the amount of data may correspond to a sum of upload and download data quantities. In Fig. 3, the hotspot device 101 is a cellular phone. The application requests input of the amount of data and of the price the given seller asks for.

5 [0059] Optionally, the application displays offers from other sellers. This provides a basis for comparing the prices asked by other sellers, which helps the given seller determining his/her own price when this option is implemented.

10 [0060] According to one non-limiting embodiment, a buyer user willing to purchase a data allowance creates an account. Account creation may be performed using the same application as the one used by the seller (i.e. the application provides an interface both for a seller to offer a data allowance and for a buyer seeking connectivity through the intermediate device to obtain a data allowance). The buyer connects to the wireless network created by the intermediate device with their own device, e.g. their own cellular phone.

[0061] Optionally, the buyer can identify on a map, within the application, the presence of several intermediate devices proposing quantities of data of mobile internet access, and can verify the quantity of data available on each of them. Optionally, the buyer also obtains and checks the estimated time of presence of the seller, e.g. to ensure it sufficiently overlaps with the buyer's own presence in the vicinity to allow the buyer to use the quantity of data he/she purchases. This information may also impact the quantity of data the buyer decides to acquire from a given seller user. Upon selecting an offer, the buyer user accesses a transaction platform in which the said buyer user enters payment information, e.g. the credentials of their credit card or online payment account, and gives authorization for future payment. Optionally, the application contains a "wallet" i.e. the buyer user has prepaid a quantity of data, e.g. a number of gigabytes of data, the number being stored in the wallet, and which can be used as currency-tokens to pay for the desired quantity of data at the time of connection. Use of a wallet has certain

20
25
30

advantages which include: (i) the wallet enables a single payment for multiple connections, thus reducing the amount of transaction fees; (ii) the wallet can be filled either with a direct money transfer using a credit card and an appropriate digital monetary transfer protocol, or as mentioned above, via the sale of quantities of data.

5 [0062] After this transaction is validated, the intermediate device receives an encrypted confirmation code from the application of the device of the buyer user, with the payment details of the buyer user and the confirmation that the payment is authorized. The intermediate device then transfers this validation to the application running on the cellular phone 101, and the application enables the internet access to the shared
10 connection of the cellular phone 101. Upon validation of the transaction, a unique password or code is generated for the buyer user, granting the buyer user device 103 access to the wireless network of the intermediate device. The intermediate device 102 acts as a root node, accessing the internet through the seller cellular phone 101 acting as a router.

15 [0063] According to one or more embodiments, the password is specific to the buyer user and valid only for the duration of the transaction. This differentiates from a direct access of a buyer user device to a shared connection, which does not allow transaction based dynamic allocation of a password to individual users.

[0064] At this moment, the buyer user device 103 can access the internet through
20 the shared connection of the cellular phone 101.

[0065] According to a variant embodiment, the payment is carried out locally using respective electronic purses of the buyers and sellers .

[0066] This internet link can be interrupted in a variety of ways:

25 - The quantity of data purchased by the buyer user is equal to the quantity of data consumed, as measured by the #dot: in this case, the #dot sends a termination message to the #dot:dot server which sends a notification to the buyer user's application that is displayed on the buyer user device's screen. The #dot terminates the connection, the server performs a financial transaction for the
30 amount corresponding the quantity of data initially booked by the buyer user, and disables the financial tag that was used initially to open the connection.

- The seller or the buyer leaves the geographic location where they were, along with their respective devices, so that the distance with the intermediate device is larger than the wireless network range of an intermediate device. This range is typically of the order of 30 to 50 meters, depending on the environment, the presence of obstacles... In this case, the connection is interrupted by the intermediate device, and a financial transaction is performed by the server for an amount proportional to the quantity of data actually used vs the quantity of data initially booked by the buyer. The financial tag that was used to initially open the connection is disabled permanently.

10

[0067] According to one or more embodiments, intermediate devices of several people offering data allowances are available within the range of a user device. The software application running on the user device can be configured to gather relevant information and facilitate selection by the buyer user of one among the multiple offers.

15 Each intermediate device creates a wireless network with the same SSID, making them indistinguishable based on network name alone. However, each intermediate device collects the quantity of data to share from the seller user device it is paired with, the anticipated time of stay, in addition to their own identifier (such as their MAC ID), for sharing with the buyer user device.

20 [0068] By sharing this information with the buyer user's device within the application running on the device, the intermediate devices allow the application to display on the buyer user device's screen the respective offers from all sellers in a given neighborhood, enabling the buyer user to choose the most suitable option. The application presents a comprehensive list of sellers along with their specific offers, allowing the buyer

25 user to make an informed decision based on their requirements. Once the buyer selects a specific seller and completes the financial transaction, the buyer effectively chooses a particular MAC ID number associated with the appropriate intermediate device, and the bank authorization and activation proceed as described previously.

30 [0069] Fig. 4 shows an exemplary screen displayed, by the application running on a buyer user device 103, to a buyer seeking to reserve a certain amount of data. The

screen shows a field for the buyer to enter the desired amount of data. The screen shown furthermore lists aliases of the sellers, a price per quantity of data and the amount of data made available for each seller. In the example shown, the list results from a filtering of all offers based on the desired quantity of data.

5

[0070] Fig. 5 is a flowchart illustrating an overall method 500 carried out by an application according to one or more embodiments. The illustrated method supposes that a single application is used by an seller and a buyer. Of course, functionalities concerning a buyer and functionalities concerning an seller can be implemented in distinct applications as well.

10

[0071] The flowchart of Fig. 5 has been grossly split into four sections, respectively section 501 for account creation, section 502 for intermediate device pairing, and sections 503 and 504 for buying and selling data. Interconnections exist between the different sections, although not all will be detailed here. The application displays three choices in succession, i.e. whether the user connects for the first time, intermediate device acquisition or pairing, or whether the user wants to buy or sell a quantity of data, each choice then leading to one of the above sections.

15

[0072] In section 501, the application asks at 501.1 whether a user connects for the first time or whether the user wishes to pair a new intermediate device with their hotspot. If yes, the user may watch a video at 501.2, explaining the principles of the use of the intermediate device. Creating an account is proposed at 501.3, which can be performed at 501.4 if the user decides so, with the user entering their credentials, including bank account information.

20

[0073] In section 502, the application offers at 502.1 to pair and/or acquire an intermediate device. If a user does not have an intermediate device and/or wishes to acquire a new intermediate device, they are led to a corresponding website (502.2, 502.3). If a user wants to pair an intermediate device, the pairing with and connection to the cellphone's shared connection is performed at 502.4, with various user input required. The application asks the user to confirm that the connection was successful, i.e. to confirm that an appropriate signal is displayed (e.g. a white LED is lit) by the intermediate device at 502.5. Pairing can be carried out over a wireless connection, e.g. a WiFi connection

25

30

between the hotspot-capable device and the intermediate device. Once the devices are paired, the hotspot mode of the hotspot-capable device is activated, and the intermediate device gains access to the shared connection over the cellular network.

[0074] In section 503, the application offers the choice of buying or selling an amount of data at 503.1. Note that in the case of buying data, there is no need for prior pairing.

[0075] If the user wishes to buy an amount of data, they are asked whether they are connected to a wireless network of an intermediate device at 503.2. If this is not the case, the user is asked to connect to at least one such a wireless network at 503.3. If the user is already connected to a wireless network of an intermediate device, they are asked to select a quantity of data they wish to buy at 503.4. A list of prices is then displayed for one or more corresponding offers from one or more sellers/owners. The user is asked to select an offer with a given price at 503.5 or accept no offer and indicate that no price is acceptable at 503.6, in which case the user gets asked to see whether they can connect at another location to other intermediate devices to get other offers. If an offer is selected, the application checks whether the user has an account at 503.7. If not, the user is asked whether they want to create an account (at 501.3). If however this is the case, the application requests validation of the price of the selected offer at 503.8. Transaction validation is then carried out as described earlier and the application initiates a message to the intermediate device so that it will allow data to be received by or sent from the user device through the shared connection through the intermediate device. If the data allowance was fully used (test at 503.10), the session is terminated at 503.12 and the full payment is initiated to the owner account. Else, if the session is simply interrupted, a pro rata price is calculated at 503.11 and payment of the partial price is initiated at 503.13. The session can be continued at another time (e.g. using the code shown in Fig. 3). A transaction dashboard (report) may then be displayed if the user asks for it at 503.14, else the method goes back to proposing the choice between buying and selling at 503.1. Similarly, a dashboard of all past transactions can be displayed upon request at 504.9, or a global dashboard of transactions at 504.10.

[0076] If the user wishes to sell an amount of data, the application checks at 504.1 whether an intermediate device is connected to the hotspot device, i.e. the cellular phone

of the seller in the present example. If this is not the case, the user is asked whether they want a dashboard of transactions to be displayed (504.9). If this is the case, the application displays fields for the user to input an amount of data to be sold and a corresponding price (504.2 and 504.3). The application then checks that the user has an account (at 504.4). If
5 not, the user is asked whether they want to create an account (back at 501.3). If the user does have an account, the information concerning the offer is transmitted to the intermediate device and the application waits for the offer to be accepted, at 504.5. Once the offer is accepted, a session password or code is created by the application of the seller at 504.6 and transmitted to the buyer user device and the hotspot device.

10

[0077] In order to preserve anonymity, actual names of sellers are preferably not displayed by the application. Rather, aliases chosen by the sellers are displayed, or not even aliases: #dot controllers and the characteristics of their offering (quantity of GBs, duration of stay in neighborhood) are spotted on a small map in real time, and people can
15 select the #dot they want to connect to by examining this map.

[0078] According to a variant embodiment, only the offers are listed. Names of sellers, whether actual names or aliases, are not displayed according to this variant.

20 [0079] Optionally, at the end of a data sharing session, both the buyer user and the seller can rate each other, through a common 5-star rating scheme for example, in order to appreciate the quality of the service: for example, the buyer can rate the reliability of the initial statement by the seller on their time of presence at the initial location, pricing, and bit rate experienced.

25

The embodiments of Fig. 6 to Fig. 9 describe the use of a server for centralized account creation and offer collection, the principles previously described remaining valid unless mentioned otherwise.

30 [0080] Fig. 6 is a diagram schematically illustrating the use of a cloud server within the system described above according to one embodiment. The seller user device

is paired with an intermediate device, as previously described. According to Fig. 6, seller information is first sent to a cloud server by the seller user device at 601. The information comprises information indicative of the geolocation of the seller user device. Seller information (amount of data offered, price, time of presence...) is then fetched by the
5 buyer user device at 602 from the server 600 based on proximity of the buyer user device to the location of the seller user devices. At 603, the buyer user device sends a message to the cloud server indicating a choice of the buyer concerning an offer and information identifying how payment is to be performed at a later point in time. The cloud server validates the payment information and authorizes the transaction. At 604, the buyer user
10 device then fetches the wireless network credentials corresponding to the intermediate device of the selected seller and at 605, connects to the wireless network using these credentials to benefit from the seller user device's shared connection. At 606, the cloud server obtains the quantity of data consumed by the buyer user device through communication with the application running on the buyer user device. The cloud server
15 checks at 607 whether the amount of data consumed by the buyer user device has reached the threshold, i.e. the acquired amount. If that is the case, the transaction ends and payment is initiated at 608. Pro-rata payment may also be performed in case of an interruption, as previously described.

20 [0081] Fig. 7 is a diagram schematically illustrating the use of a cloud server within the system described above according to another embodiment. The method is similar to that of Fig. 6, with corresponding steps (e.g. 701 corresponding to 601), with seller information being centralized at the server 700. The difference is that at 702, information describing seller user devices and available offers as a function of the
25 geographical position of the buyer user device is obtained from the cloud server through the wireless network of an intermediate device which the buyer user device can connect to, instead of through a direct connection to the cloud server. Else, the method continues as previously described.

30 [0082] Fig. 8 is a diagram schematically illustrating the use of a cloud server within the system described above according to yet another embodiment. According to

this embodiment, payment involves electronic purses located at the seller device and the buyer device. The seller user device is paired with the intermediate device, as previously described. Once the devices are registered with the server and after validation of respective payment information of the buyer and seller user devices by the server,
5 payment is handled locally between the buyer and seller user device purses and does not require interaction with the server during the payment itself.

[0083] Steps 801 to 816 are as follows:

10 (a) Initial registration phase

801. Seller account creation at seller device including: bank certification, seller purse information

802. Registration at the server and creation of seller user ID at server

(A user ID can be used both for selling and buying data allowances, although for
15 the purpose of clarity, the user IDs herein are labelled as buyer (user) ID and seller (user) ID).

803. Seller user ID is transmitted by the cloud server to seller user device

804. Seller payment information (bank certification, seller purse information) is validated (once only) by the cloud server

20 805. Buyer account creation at buyer user device including: bank certification, seller purse information

806. Registration of the buyer at the server and creation of a buyer user ID

807. Buyer user ID is transmitted by the cloud server to the buyer user device

25 808. Buyer payment information (bank certification, seller purse information) is validated (once only) by cloud server

(b) Buyer device connection phase

809. Buyer user device connects to a wireless network of a nearby intermediate device and obtains available seller offer information (quantity of data, selling
30 price, optionally time of presence) for sellers in the vicinity of the buyer user device

810. Buyer selects an offer using buyer user device

811. Local validation of payment from purse by buyer using buyer user device

812. Validation of buyer user ID and purse information and authorization of transaction by the buyer user device.

5 813. Data transfer through the shared connection is now authorized as specified in the accepted offer.

814. Once the connection is interrupted, buyer's purse is updated (e.g. an amount is debited) and seller's purse is updated (e.g. an amount is credited).

10 (c) Bank transfer

The following steps can be implemented at a later stage, for example periodically:

815. Seller device updates online purse/information with server

816. Cloud server initiates payment to seller bank account based on (updated) seller purse content information.

15

[0084] According to a variant embodiment, an optional registration check is implemented. This security check can however be used in conjunction with any of the above embodiments in which the user devices register with a server. A method according to the present embodiment comprises:

20 - The buyer device detects a wireless network of an intermediate device connected to a seller device.

- The buyer device connects to the wireless network of the intermediate device.

- The intermediate device then checks that the buyer was registered with the server.

If this is not the case, the intermediate device disconnects the buyer device.

25 [0085] Verifying registration reduces the connections to the wireless network by devices not using the software application and not having registered with it at the server. The server thus validates the connection of the buyer device, limiting intrusions.

[0086] The check can be carried out as follows:

30 - The buyer device has knowledge of an identifier ('ID key') proving registration of the buyer with the server. Note that this identifier may also serve other purposes (e.g. identifying the buyer in the system).

- When the buyer device is connected to the wireless network, it transmits its ID key to the intermediate device.
- The intermediate device sends the ID key to the server, which responds as to whether the ID key corresponds to a registered buyer or not.
- 5 - The ID key can be provided by the server to the buyer device during the registration process, or vice-versa, or generated and communicated using any appropriate process.

[0087] According to another embodiment, illustrated by the schematic diagram of Fig. 9, the buyer and seller purses are located at the cloud server instead of the buyer and seller user devices. It is then possible for a device, typically the intermediate device 102, to check a buyer purse credit level with the server.

[0088] Both the seller device 101 and the buyer device 103 register with the server 900. In Fig. 9, this stage is illustrated by each of the device users (seller, buyer) creating an account with the server for enabling selling and/or buying of data allowances (see 901, respectively 903), with the account information being maintained by the server (see 902, respectively 904). Account information comprises information necessary for implementing an electronic purse and bank information for crediting the purse, or to the contrary carry out a transfer from the purse to the bank account of a user. A buyer user 20 can for example credit their purse when the buyer user device has connectivity with the server (including when this connectivity is achieved through the intermediate device and seller user device).

[0089] The seller user device is paired with intermediate device 102, as previously described, and has communicated its offer or offers to the server, along with its geographical location. For the sake of providing an illustration of the optional registration check mentioned above, Fig. 9 shows the implementation of such a check. At 905, the buyer user device thus receives an 'ID key' i.e. proof of its registration and identifying the buyer in the system. The buyer can transfer monetary tokens to their electronic purse located as the server, for example at 906, or at another stage. The buyer can then connect 30 (907) to the wireless network of the intermediate device using the software application and request offers. For example, in case wireless networks of distinct intermediate devices

use a same identifier, buyer device 103 can detect the wireless network of intermediate device 102 using the predetermined network identifier and connect to this wireless network.

[0090] Once connected to the wireless network, the buyer user device sends

- 5 - a request for offers to the intermediate device;
- the ID key proving registration;
- its geographical location (which may alternatively be derived by the intermediate device from its own location).

[0091] The embodiment of Fig. 9 also shows an additional option implementing
10 a so-called application key ('App key'). An application key is a code allowing a device to determine that the software application of another device with which it is communicating for the purpose of buying and/or selling data allowances is a genuine application. The application identifier is for example inherent to the application of the buyer device. This application identifier is also transmitted by the buyer user device to
15 the intermediate device.

[0092] Using the information received, the intermediate device uses the shared connection of the seller user device (at 908) to:

- if the option is implemented, check with the server that the buyer is registered, using the ID key and disconnects the buyer user device in case the check result is
20 negative;
- if the option is implemented, check with the server that the application used by the buyer user device is genuine as a function of the application identifier;
- obtain from the server a list of offers from seller user devices in the area as a function of geographical location (noting that this step need not be carried out of
25 any of the optional checks are negative).

[0093] The intermediate device returns the list of offers to the buyer user device. The buyer then validates an offer ('x blocks of data for y value), and this information is returned to the intermediate device. Using the ID key identifying the buyer, the intermediate device checks with the server that the credit level of the buyer's purse is
30 sufficient to pay for the requested amount of data. If that is the case, the intermediate device also validates the offer (909) and opens the access to the shared connection (910).

Else, the intermediate device may ask the buyer user device to reduce the amount of data to be acquired or to credit the purse.

[0094] The intermediate device periodically obtains from the buyer user device a counter value of the amount of data effectively transferred over the shared connection.

5 The server is updated with this amount. The intermediate device also checks whether the amount specified in the validated offer has been reached or not. If the specified amount has not been reached, the intermediate devices iterates on the counter value checks (911, 912). The intermediate device may also send information representative of the unused amount of data in the validated offer to the buyer user device (912), which may display
10 the amount through the software application.

[0095] When the data allowance of the validated offer has been fully used, the intermediate device:

- sends a message to the buyer user device that amount of data in the validated offer has been used;
- 15 - the cuts the access to the shared connection;
- updates the server with the amount of data used.

[0096] Payment may then be made by appropriately updating the purses of the buyer and the seller.

20 [0097] According to another option that can be used with any of the above embodiments, the buyer user device gains limited access to the shared connection of the seller device when connected to the wireless network of the intermediate device, but even before accepting the offer for the purpose of facilitating offer obtention, review and acceptance. For example, the buyer user device may be allowed to connect to a specific
25 URL, such as the URL of the cloud server, when such a cloud server is used, or the URL of a website allowing obtaining the software application or an update thereof.

[0098] According to a variant embodiment, the wireless networks of each intermediate device are assigned distinct network identifiers. These identifiers are
30 broadcast by the intermediate devices and have a format that allows them to be recognized by a buyer user device as corresponding to wireless networks of intermediate devices

through which a buyer user device can potentially obtain connectivity through a shared connection. Advantageously, the identifier format is such that it comprises a predefined code, for example a six-letter code, which indicates that the identifier corresponds to a wireless network of an intermediate device proposing the functionalities described herein.

5 Advantageously, the identifier can comprise additional data characterizing an offer made by the seller user device paired with an intermediate device using this identifier for its wireless network. Additional data can comprise the time interval during which the seller user is present within a certain range. The format may for example be of the type: #dot.dot_Price=0.1_20min_ABCDEF, where '20min' corresponds to the time the seller

10 user is present.

[0099] According to the embodiment described below, no session password or code is used. Tokens validated by the cloud server are used instead. In this embodiment, the seller user device and the buyer user device are both cellular phones.

15

[00100] 1. The server obtains (or already possesses) a list of authorized intermediate devices.

The list may for example comprise identifiers of intermediate devices, such as the MAC IDs of the intermediate devices. The list of MAC IDs can for example be provided to the

20 server by the manufacturer of the intermediate devices.

[00101] 2. The seller must obtain validation from the server that they are a legitimate seller, i.e. their phone number is checked and they are using an authorized intermediate device.

25 (i) The seller provides their phone number of their seller user device through the software application running on the seller user device. The seller user device transmits the phone number to the server. The server sends a one-time code to the seller user device via the cellular network and the seller types the one time code in the software application for transmission to the server: if a valid code is received by the server, the server returns a

30 token to the seller user device called the "valid seller token". If an invalid code is returned, the server does not return anything.

(ii) The seller pairs their intermediate device with their user device using the software application. Once done, the intermediate device sends its MAC ID to the server via the shared connection of the seller user device. If the MAC ID is authorized, i.e. present in the list of authorized intermediate devices, then the server returns a token to the seller user device, called the “authorized intermediate device token”. If the MAC ID is unknown to the server, the server does not return anything.

[00102] 3. The seller sends an offer to the server using the software application running on the seller user device. This offer is accompanied by the valid seller token and authorized intermediate device token. The server checks the tokens, and the offer of the seller will be allowed to appear on the software application of the potential buyers within range of the seller.

[00103] 4. The buyer must obtain validation from the server that they are a valid buyer, i.e. their phone number is checked and there is enough credit in their purse, so that the financial transaction associated with the use of an amount of data from the seller via the service will be doable.

[00104] The buyer user device connects to the paired intermediate device of the seller. The buyer provides their phone number of their buyer user device through the software application running on the buyer user device (e.g. via the shared network connection put in place during the pairing process, which can be used in a limited manner for this purpose). The buyer user device transmits the phone number to the server.

[00105] The server sends a one-time code to the buyer user device via the cellular network and the buyer types the one-time code in the software application. The code is sent to the server, and the amount of data or currency in the purse is checked by the server. If a valid code is received by the server and the amount in the purse is higher than a minimum threshold amount (e.g. 0,20€), the server returns a token to the buyer user device called the “valid buyer token”. If an invalid code is returned, the server does not return anything. Optionally, if the code is valid but the amount in the purse is lower than the threshold amount, the server returns a temporary token that triggers the redirection of the buyer to the page of the software application where they can credit their account to be

above the threshold.

[00106] 5. The buyer user device then sends their valid buyer token to the intermediate device, to request use of the shared connection, with an associated number
5 of requested GBs (i.e. an offer is accepted, as previously described).

[00107] 6. The intermediate device transmits to the server: the request, the valid seller token, the authorized intermediate device token and the valid buyer token.

10 [00108] 7. The server checks the validity of the tokens. If the checks are all positive and the buyer's purse balance is sufficient compared to the accepted offer, the server authorizes the intermediate device to allow use of the shared connection. Else, if the server indicates at least one negative check result or does not confirm, the intermediate device disconnects the buyer user device.

15

[00109] If the buyer user device connects several times to the same intermediate device, or to other intermediate devices, a new buyer authorization token needs to be obtained each time, so that the purse balance is checked every time.

20 [00110] Some or all of the following advantages are provided by the various embodiments described.

[00111] By utilizing the intermediate device and the application, sellers can seamlessly share their surplus of a mobile data plan, while buyers can easily locate and purchase data that precisely fits their requirements. This revolutionizes the way users
25 share and acquire mobile data, offering a flexible, cost-effective, and anonymous solution to the problems associated with wasted data and inflexible data plans.

[00112] Furthermore, limitations of existing methods are overcome by eliminating the need for sellers to share the password of their shared connection or reveal their
30 identity. The seller's anonymity can be preserved, ensuring privacy and security throughout the transaction process.

[00113] Additionally, pro-rata temporis payment calculation can be applied to ensure fair compensation for the shared mobile data, providing an equitable solution for both buyers and sellers.

5

[00114] A rating system may be incorporated, which helps address concerns regarding the reliability of seller information and the quality of service are also addressed. This fosters transparency and trust within the community of intermediate device owners, enhancing the overall user experience.

10

[00115] In conclusion, a comprehensive solution to the technical problems associated with wasted mobile data, inflexible data plans, and the lack of anonymity in data sharing is provided. By leveraging the intermediate device, the application, secure transactions, and rating mechanisms, users are empowered to efficiently share and purchase mobile data, ensuring optimal resource utilization and enhancing the overall connectivity experience.

15

[00116] The present description discloses a peer-to-peer mobile data sharing system, comprising an intermediate device, a dedicated application, and a secure transaction mechanism. Sellers, equipped with an intermediate device, establish a wireless network with a predetermined name to advertise available data for sale. The application allows sellers to specify the quantity of data and set the selling price, enabling buyers to identify suitable sellers.

20

[00117] Buyers can connect to the application, browse the list of sellers, and view their respective selling prices if available, and/or amount of GBs for sale and/or duration of stay within, say, 100 meters of the initial point where the seller started to share their GBs. Upon selecting a seller, a secure transaction is initiated, and future payment authorization is processed. Upon completion of the transaction, a unique session password or code may be generated, granting the buyer access to the shared connection through the wireless network created by the intermediate device. The intermediate device

25

30

acts as a root node, accessing the internet through the seller's smartphone acting as a router. The session password or code can for example be created by the cloud server as a function of an identifier of the buyer user device, an identifier of the seller user device proposing the offer selected by the buyer and an identifier of the intermediate device
5 paired with the seller user device. These identifiers can be the MAC IDs of each device. The session password is sent by the server to the seller user device, which sends it to the intermediate device it is paired with, the intermediate device communicating the session password to the buyer user device. The buyer user device uses this session password to obtain unrestricted access to the wireless network of the intermediate device (i.e. allowing
10 access to the shared connection).

[00118] The quantity of data transacted is determined based on the buyer's connectivity within range of the seller's intermediate device. Payment is calculated pro-rata considering the quantity of data consumed vs the initial amount of data pre-booked
15 by the user, ensuring fair compensation for the shared mobile data. To facilitate buyer selection, sellers are initially requested to declare their expected availability, although this commitment is non-binding. Buyers can consider this information when choosing a seller based on their own anticipated usage duration.

20 [00119] Additionally, a rating system is proposed to assess the quality of service and reliability of seller information. Both buyers and sellers can provide feedback, enhancing transparency and promoting trust within the dot-dot community.

[00120] In conclusion, a system and method for efficient and anonymous peer-to-
25 peer mobile data sharing are introduced. By utilizing an intermediate device, sellers can offer their unused quantities of data for sale, while buyers can easily purchase data tailored to their needs. With a secure transaction mechanism, rating system, and pro-rata temporis payment calculation, the way users share and acquire mobile data is revolutionized, promoting flexibility, cost-effectiveness, and anonymity within the dot-
30 dot community.

EXAMPLES

Example 1 - Method carried out by a first communication device (102), said communication device comprising a processor (201), memory (202) comprising software code, a wireless communication interface (203, 204) for communicating with at least one
5 second device (101), said second device being a cellular phone, said communication interface being further configured to provide a wireless network for access by at least one third device (103), said processor causing the first device to carry out the method when executing said software code, said method comprising:

- 10 - setting up a connection with a given second device in a shared connection mode of the second device;
- receiving from the given second device a message comprising an amount of data to be made available by said second device and a price for said amount of data, wherein said amount of data is representative of data to transit over a cellular network to which the
15 second device is connected;
- creating the wireless network;
- responsive to a request message received over the wireless network from a given third device, sending a message to the given third device comprising at least the amount of data and the price;
- 20 - responsive to information indicating validation of the price by the given third device, providing to said given third device, over the wireless network, access to the shared connection for the amount of data.

The first communication device acts as an intermediary between the cellular phone and a
25 third device requiring connectivity through a shared connection provided by the cellular phone. The second and third devices do not communicate directly. There is no need for a user of the third device to know the real identity of the user or owner of second device, i.e. the user of the second device can remain totally anonymous.

30 Example 2 - The method according to example 1, wherein the message from the given second device (101) further comprises an estimated time of presence of an owner of the

second device at its current location.

Example 3 - The method according to example 1, wherein the wireless network uses a predetermined SSID identifying the wireless network as providing connectivity through a cellular network.

- 5 Example 4 - The method according to example 2, wherein the predetermined SSID is common to a plurality of first communication devices.

This predetermined SSID can thus be known by a third device, e.g. a third device running a software application adapted to allow using the first device as described.

10

Example 5 – The method according to example 2, wherein the predetermined SSID is unique to the first communication device.

Example 6 - The method according to one of the examples 1 to 4, wherein the wireless network is an IEEE802.11 type network.

- 15 Example 7 - The method according to one of the examples 1 to 5, wherein the first device provides to the third device one among an alias representative of a user of the second device, or no information concerning the identity of said user.

Example 8 - The method according to one of the examples 1 to 6, wherein providing access to the shared network connection comprising sending the information indicating validation to the second device, forwarding requests for data from the given third device
20 to the second device and forwarding responses from the second device to the given third device.

- Example 9 - Communication device comprising a processor (201), memory (202) comprising software code, a wireless communication interface (203) for communicating
25 with at least one second device, said second device being a cellular phone (101), said communication interface being further configured to provide a wireless network for access by at least one third device (103), said processor causing the first device to carry out ,when executing said software code, a method according to one of the examples 1 to 8.

30

CLAIMS

1. Method for data transfer over a communication network, in a system comprising:
 - a first communication device (102) comprising a communication interface (203, 204) configured to provide:
 - 5 ○ a wireless connection to a second communication device;
 - a wireless access point for providing a wireless network;the second device (101) comprising a communication interface configured to provide a shared connection to a communication network to the first device, wherein the shared connection is adapted to enable data transfer over the
10 communication network;
 - a third communication device (103) comprising a communication interface to connect to the wireless network of the access point of the first device;the method comprising, at the third device:
 - obtaining, by the third device, information representative of at least one
15 offer for transferring data over the shared connection of the second device;
 - in response to the transmission of a message indicative of acceptance of a received offer, receiving access, by the third device, to the shared connection corresponding to the accepted offer for transferring data according to one or mode conditions of the accepted offer, wherein communication between the second
20 device and the third device, of said data, is performed solely through the first device.
2. The method of claim 1, further comprising, before enabling access, validating a transaction authorizing payment of a price associated with the accepted offer.
25
3. The method of claim 1 or 2, wherein the wireless network has a network identifier indicating to the third device that the first device is adapted to provide access to the shared connection.
- 30 4. The method according to claim 3, wherein the system comprises a plurality of first devices connected to respective second devices, each first device providing a

given wireless network, all given wireless networks using a same network identifier, the network identifier being known to the third device.

5. The method of claim 4, wherein the obtaining, by the third communication device,
5 of information representative of at least one offer for data transfer over the shared connection of the second communication device comprises, at the third device:
 - detecting the wireless network of the first device using the network identifier of the first device;
 - obtaining the information representative of at least one offer for data transfer over
10 the shared connection of the second communication device through the first device.
6. The method according to one of the claims 2 to 5, wherein the information
15 representative of an offer comprises an amount of data to be transferred and the price for enabling transfer of the amount of data.
7. The method according to one of the preceding claims, wherein the information
20 representative of an offer further comprises an estimated time of presence of the second device at a current geographical location.
8. The method according to one of the preceding claims, wherein the information
representative of an offer comprises no information concerning the identity of said user of the first device.
- 25 9. The method according to one of the preceding claims, wherein the communication network is a cellular network and the second device is a cellular phone.
10. The method according to one of the preceding claims combined with claim 2,
30 wherein validating a transaction authorizing payment of a price associated with the accepted offer is performed by a software application executed by the third device, the method further comprising

- transmission of an information indicative of the validation of the transaction by the third device to the first device;
- transmission of the information indicative of the validation of the transaction by the first device to the second device;
- 5 - enabling access to the shared connection by the second device responsive to the information indicative of the validation of the transaction.

11. The method according to one of the preceding claims, further comprising, at the third device,
- 10 - detection of the wireless network of the first device using the predefined network identifier;
- obtaining the information representative of the at least one offer for data transfer through the first device.

- 15 12. The method according to one of the claims 1 to 9, the system further comprising a cloud server (600, 700, 800, 900), the method further comprising:
- obtaining (602), by the third device, from the cloud server, information representative of at least one offer for data transfer of the second device as a function of a geographic location of the second device and a geographic location
- 20 of the third device.

13. The method according to claim 12, further comprising, at the third device:
- sending (603), to the cloud server, an information indicative of the accepted offer;
- 25 - receiving (604), from the cloud server, information enabling the connection of the third device to the wireless network of the first device connected to the second device for the purpose of transferring data over the shared connection;
- connecting (605) to the wireless network using the information enabling the connection.

30

14. The method according to one of the claims 12 or 13, further comprising:

- registration (902, 904) of the third device with the cloud server, comprising setting up a purse for transaction payment at the cloud server.
15. Third communication device (103), comprising a processor and, memory
5 comprising software code, the third communication device being configured to carry out the method according to one of the claims 1 to 14.
16. Method for data transfer over a communication network, in a system comprising:
- a first communication device (102) comprising a communication interface
10 (203, 204) configured to provide:
 - o a wireless connection to a second communication device;
 - o a wireless access point for providing a wireless network;
- the second device (101) comprising a communication interface configured to provide a shared connection to a communication network to the first device,
15 wherein the shared connection is adapted to enable data transfer over the communication network;
- a third communication device (103) comprising a communication interface to connect to the wireless network of the access point of the first device;
- the method comprising, at the second device:
- 20 - enabling the shared connection;
 - configuring the first device to allow the first device to connect to the shared connection;
 - providing information representative of at least one offer for transferring data over the shared connection, for obtention by the third device, wherein
25 communication between the second device and the third device of said data upon acceptance of an offer is performed solely through the first device.
17. The method according to claim 16, the system further comprising a cloud server
30 (600, 700, 800, 900), the method, wherein providing information representative of at least one offer comprises

- transmitting (601, 701) said information, by the second device to the cloud server, wherein information of an offer comprises an amount of data to be transferred and a price for enabling transfer of the amount of data.

5 18. The method according to claim 16 or 17, wherein said information comprises a current geographical location of the second device.

19. The method according to claim 18, wherein said information comprises an estimated time of presence of the second device at the current geographical
10 location.

20. Second communication device (103), comprising a processor and, memory comprising software code, the third communication device being configured to carry out the method according to one of the claims 16 to 19.

15

21. Method for data transfer over a communication network, in a system comprising:
- a first communication device (102) comprising a communication interface (203, 204) configured to provide:

- a wireless connection to a second communication device;
- 20 ○ a wireless access point for providing a wireless network;

the second device (101) comprising a communication interface configured to provide a shared connection to a communication network to the first device, wherein the shared connection is adapted to enable data transfer over the communication network;

25 - a third communication device (103) comprising a communication interface to connect to the wireless network of the access point of the first device;

the method comprising, at the first device:

- connecting to the shared connection of the second device;
- providing said wireless network for connection by the third device;

- responsive to information indicative of acceptance by the third device of an offer for transferring data over the shared connection of the second device, transferring said data between the second device and the third device.
- 5 22. First communication device (103), comprising a processor and, memory comprising software code, the third communication device being configured to carry out the method according to claim 21.
- 10 23. Non-transitory computer-readable storage medium (202) comprising instructions that when executed cause a processor of a computing device to carry out the steps according to one of the methods of claims 1 to 14, 16 to 19 and 21.