

INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD,
AND NON-TRANSITORY STORAGE MEDIUM STORING PROGRAM

BACKGROUND OF THE INVENTION

5

1. Field of the Invention

[0001] The present disclosure relates to information processing devices, information processing methods, and non-transitory storage media storing a program.

2. Description of Related Art

10 **[0002]** A technique of extracting base stations located within a predetermined distance from the vehicle based on position information of base stations and position information of the vehicle and attempting to communicate with the base station having the highest radio wave reception level out of the extracted base stations is known in the art (see, e.g., Japanese Unexamined Patent Application Publication No. 2010-288153 (JP
15 2010-288153 A)).

SUMMARY OF THE INVENTION

[0003] It is an object of the present disclosure to provide a technique that is
20 effective in reducing communication with devices masquerading as base stations.

[0004] An aspect of the present disclosure relates to an information processing device that is mounted on a vehicle and that performs Long-Term Evolution (LTE) wireless communication, the information processing device comprising a processor configured to: send a request for update of a tracking area where the vehicle is located to a
25 first base station in the tracking area where the vehicle is located; determine whether a predetermined condition is satisfied when the information processing device has received from the first base station a signal rejecting the request for a reason that the information processing device is not identifiable; and forbid communication with the first base station when the processor determines that the predetermined condition is satisfied.

[0005] Another aspect of the present disclosure relates to an information processing method in which a computer that is mounted on a vehicle and that performs Long-Term Evolution (LTE) wireless communication is controlled, the information processing method comprising causing the computer to: send a request for update of a tracking area where the vehicle is located to a first base station in the tracking area where the vehicle is located; determine whether a predetermined condition is satisfied when the computer has received from the first base station a signal rejecting the request for a reason that the computer is not identifiable; and forbid communication with the first base station when the computer determines that the predetermined condition is satisfied.

[0006] Another aspect of the present disclosure relates to a non-transitory storage medium mounted on a vehicle and storing a program that causes a computer that performs Long-Term Evolution (LTE) wireless communication to: send a request for update of a tracking area where the vehicle is located to a first base station in the tracking area where the vehicle is located; determine whether a predetermined condition is satisfied when the computer has received from the first base station a signal rejecting the request for a reason that the computer is not identifiable; and forbid communication with the first base station when the computer determines that the predetermined condition is satisfied.

[0007] The present disclosure can also be interpreted as an information processing program that causes a computer mounted on a vehicle and connected to a core network via a base station by Long-Term Evolution (LTE) wireless communication to perform the above information processing method, or as a non-transitory storage medium storing the information processing program.

[0008] The present disclosure can provide a technique that is effective in reducing communication with devices masquerading as base stations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Features, advantages, and technical and industrial significance of exemplary embodiments of the invention will be described below with reference to the

accompanying drawings, in which like signs denote like elements, and wherein:

FIG. 1 shows an overview of a mobile communication system;

FIG. 2 shows an example of a hardware configuration of user equipment;

FIG. 3 is a block diagram showing an example of a functional configuration of the
5 user equipment;

FIG. 4 shows an example of a forbid list;

FIG. 5 is a sequence diagram schematically illustrating the flow of data that is sent
and received by the user equipment and the flow of procedures that are performed by the
user equipment when a first base station is a legitimate base station;

10 FIG. 6 is a sequence diagram schematically illustrating the flow of data that is sent
and received by the user equipment and the flow of procedures that are performed by the
user equipment when the first base station is a fake base station; and

FIG. 7 is a flowchart illustrating the flow of procedures that are performed by the user
equipment in response to a TAI notification signal.

15

DETAILED DESCRIPTION OF EMBODIMENTS

[0010] Mobile communication systems based on the Long-Term Evolution (LTE)
standard include a radio access network (Radio Access Network (RAN)) and a core
20 network (Evolved Packet Core (EPC)) that comply with the specifications of the 3rd
Generation Partnership Project (3GPP).

[0011] The radio access network (RAN) is composed of user equipment (UE) and
base stations (evolved NodeBs (eNodeBs)). The core network (EPC) is composed of a
control plane (Control-plane (C-plane)) function group and a user plane (User-plane
25 (U-plane)) function group. The control plane function group includes a Mobile
Management Entity (MME). The MME is a control entity that manages the movement
and communication path of the user equipment. The user plane function group includes a
Serving Gateway (SGW) that relays user data and a Packet Data Network Gateway (PGW)
that is a relay point to an external network.

[0012] In such a mobile communication system as described above, the position of the user equipment is managed in units called tracking areas (TAs). The tracking area (TA) is composed of one or more cells, and a base station (eNodeB) is located in each cell. The cell is the communication range of the base station. This may be either the designed
5 communication range of the base station or the range actually reachable by radio waves. The base station (eNodeB) in each cell has a function to periodically notify the user equipment located in the cell under the management of this base station of the identifier (Tracking Area Identity (TAI)) of the tracking area (TA) to which the cell belongs. The user equipment that has received the tracking area identifier (hereinafter also referred to as
10 the “TAI”) compares the TAI received last time with the TAI received this time. The TAI received last time and the TAI received this time are different when, for example, the tracking area (TA) where the user equipment is located has changed as the user equipment moves. In such a case, the user equipment sends a request (TAU request) to the MME via the base station (eNodeB). This request (TAU request) is a request for update of the
15 tracking area (TA) where the user equipment is located (Tracking Area Update (TAU)). In response to the TAU request, information regarding the tracking area (TA) where the user equipment is located is updated on the core network (EPC) side including the MME. For example, a procedure of authenticating the user equipment, a procedure of resetting a bearer (logical communication path from the base station (eNodeB) in the tracking area
20 (TA) where the user equipment is located to the external network), etc. are performed on the core network (EPC) side. This allows the user equipment to be connected to the external network even when the user equipment moves to a different tracking area (TA).

[0013] There are cases where a device masquerading as a base station (eNodeB) (hereinafter sometimes referred to as the “fake base station”) is installed in the tracking
25 area by a malicious third party. When the user equipment located in such a tracking area (TA) sends a TAU request to the fake base station, the user equipment may receive a signal rejecting the TAU request for the reason that the user equipment is unidentifiable (e.g., a signal including Reason value #9 as defined in the 3GPP, hereinafter sometimes referred to as the “TAU reject signal”).

[0014] One possible way to reduce unauthorized information leakage by such a fake base station is to forbid communication between the tracking area (TA) where the fake base station is located and the user equipment when the user equipment receives the TAU reject signal. One example is to register the TAI of the tracking area (TA) where the fake base station is located on a forbid list (list on which TAIs of the tracking areas (TAs) to be forbidden are registered) set in each piece of user equipment.

[0015] However, for example, even when the user equipment sends a TAU request to the MME via a legitimate base station (eNodeB) upon returning to the radio access network (RAN) coverage area after moving out of the radio access network (RAN) coverage area, the TAU request may be rejected for the same reason as described above. This is because when the user equipment is located out of the radio access network (RAN) coverage area for a certain period of time (e.g., about 70 minutes) or more, what is called an “implicit detach procedure” is performed. Namely, information on the user equipment registered to the core network (EPC) in the previous attach procedure (e.g., Globally Unique Temporary Identity (GUTI) etc.) is deleted. In such a case, when the user equipment is of a type that can switch between the LTE wireless communication method and the 3rd Generation (3G) wireless communication method, the user equipment will become accessible to the external network by performing an attach procedure using the 3G wireless communication method. However, when the user equipment is of a type capable of only LTE wireless communication, the user equipment may not be accessible to the external network for a long period of time. As a result, the user of the user equipment may not be able to use the Internet etc. for a long period of time. For example, when the user equipment is communication equipment mounted on a vehicle, the user of the user equipment may not be able to use connected services such as emergency calls. It is therefore desired to accurately determine whether the source of the TAU reject signal is a fake base station and effectively forbid communication with the fake base station.

[0016] In an information processing device (corresponding to user equipment mounted on a vehicle) according to the present disclosure, when the tracking area (TA) where the vehicle (information processing device) is located has changed (including the

case where the tracking area (TA) where the vehicle is located upon returning to the radio access network (RAN) coverage area after moving out of the radio access network (RAN) coverage area is different from the last tracking area (TA) where the vehicle was located), a control unit of the information processing device sends a TAU request to a base station
5 (first base station) of the tracking area (TA) where the vehicle is located. When the TAU reject signal is sent from the first base station to the information processing device, the control unit determines whether a predetermined condition is satisfied. The “predetermined condition” herein referred to a condition specific to fake base stations, and for example, is that a signal requesting subscriber identification information (International
10 Mobile Subscriber Identity (IMSI)) assigned to the information processing device has been sent to the information processing device. In addition to the above condition, the predetermined condition may include a condition that the first base station does not start encrypted communication involving an authentication procedure (that is, plaintext data communication is continued between the user equipment and the first base station).
15 Accordingly, the control unit may determine that the predetermined condition is satisfied when the information processing device has received the signal requesting the subscriber identification information (IMSI) from the first base station and/or when the information processing device has received the signal etc. requesting the subscriber identification information (IMSI) from the first base station in the form of plaintext. This makes it
20 possible to accurately determine whether the TAU reject signal has been sent from a fake base station or a legitimate base station. When the control unit determines that the predetermined condition is satisfied, the control unit can determine that the first base station is a fake base station and forbid communication with the first base station.

[0017] According to the present disclosure, since the fake base station can be
25 accurately determined, communication with the fake base station can be suitably reduced.

[0018] In the information processing device according to the present disclosure, when forbidding communication with the first base station, the control unit may only forbid communication with the cell where the first base station is located out of the tracking area (TA) where the vehicle is located. This allows the information processing device to

access an external network via a base station (second base station) in a cell other than the cell where the first base station is located out of the tracking area (TA) where the vehicle is located.

[0019] When the information processing device accesses the external network via the second base station, the control unit may send an attach request to the second base station. The attach request is a request to register the information processing device to the network. This reduces the possibility that communication with the first base station may be unnecessarily continued and the information processing device may become unconnectable to the external network when the first base station is a fake base station.

5 The “attach request” is a signal requesting a procedure (attach procedure) of newly setting a bearer from the base station in the tracking area (TA) where the information processing device is located to the external network and assigning temporary identification information such as GUTI to the information processing device.

10

[0020] There may be cases where there are no cells that are accessible by the information processing device in the tracking area (TA) where the vehicle is located other than the cell where the first base station is located. In such cases, when communication with the cell continues to be forbidden for a long period of time, the information processing device may not be accessible to the external network for a long period of time. Accordingly, when forbidding communication with the first base station, the control unit may forbid communication with the cell where the first base station is located for a predetermined time that is five minutes or less. This allows the information processing device to access the external network via a base station other than the first base station in the cell when the predetermined time has elapsed. At this time, the control unit may send a TAU request to the base station other than the first base station or may send an attach request to the base station other than the first base station.

15

20

25

[0021] When the information processing device has received the TAU reject signal but the predetermined condition is not satisfied, it can be estimated that the first base station is a legitimate base station and not a fake base station. That is, it can be estimated that the TAU reject signal has been sent from the first base station to the information

processing device because an implicit detach procedure for the information processing device was performed on the core network (EPC) side. Accordingly, the control unit may send an attach request to the first base station when the information processing device has received the TAU reject signal but the predetermined condition is not satisfied. This
5 reduces the possibility that communication between the information processing device and the first base station may be unnecessarily forbidden when the first base station is a legitimate base station. As a result, the information processing device can be connected to the external network via the legitimate first base station.

Embodiment

10 **[0022]** Hereinafter, a specific embodiment of the present disclosure will be described with reference to the drawings. The configuration of the following embodiment is illustrative, and the present disclosure is not limited to the configuration of the embodiment.

Overall System Configuration

15 **[0023]** FIG. 1 shows a schematic configuration of a mobile communication system to which the information processing device according to the present disclosure is applied. The mobile communication system of the present embodiment includes a radio access network (RAN) and a core network (EPC).

[0024] The radio access network (RAN) includes user equipment 100 mounted
20 on a vehicle 10 and a plurality of base stations (eNodeBs) 201, 202. The user equipment 100 is communication equipment for connecting various devices mounted on the vehicle 10 to an external network (Packet Data Network (PDN)). The user equipment 100 has an Long-Term Evolution (LTE) wireless communication function and does not have a 3rd Generation (3G) wireless communication function. Such user equipment 100 corresponds
25 to the “information processing device” according to the present disclosure. Only one vehicle 10 equipped with the user equipment 100 is shown on the radio access network (RAN) of FIG. 1. However, there may be a plurality of vehicles on the radio access network (RAN).

[0025] The base stations (eNodeBs) 201, 202 are connected to a Mobile Management Entity (MME) 300 of the core network (EPC) via an S1 interface and send and receive various control signals to and from the MME 300. The base stations (eNodeBs) 201, 202 have a wireless interface function to wirelessly communicate with the user equipment 100 by a wireless communication method complying with the specifications of the 3rd Generation Partnership Project (3GPP). For example, the base stations (eNodeBs) 201, 202 have a function to control wireless connection with the user equipment 100 (Radio Resource Control (RRC)) and a function to periodically notify the user equipment 100 within the cell of the identifier (Tracking Area Identity (TAI)) of the tracking area (TA). The base stations (eNodeBs) 201, 202 may be configured to have functions to encrypt signals handled in wireless communication with the user equipment 100, to compress Internet Protocol (IP) headers, etc.

[0026] One tracking area (TA), two cells (first cell and second cell) in the tracking area (TA), the first base station (eNodeB) 201 located in the first cell, and the second base station (eNodeB) 202 located in the second cell are illustrated in the example of FIG. 1. However, the number of tracking areas (TAs), the number of cells in the tracking area (TA), and the number of base stations (eNodeBs) located in the cell are not limited to those in the example of FIG. 1.

[0027] The core network (EPC) includes the MME 300, a Serving Gateway (SGW) 400, and a Packet Data Network Gateway (PGW) 500. Although only one MME 300, one SGW 400, and one PGW 500 are illustrated on the core network (EPC) of FIG. 1, there may be a plurality of MMEs 300, a plurality of SGWs 400, and a plurality of PGWs 500 on the core network (EPC).

[0028] The MME 300 forms a control plane function group of the core network (EPC) and performs movement control for the user equipment 100 such as position management, paging (simultaneous calling), and handover. For example, in the position management for the user equipment 100, the MME 300 adds and deletes the pieces of user equipment 100 located in each tracking area (TA) to the tracking area list generated for each tracking area (TA). The MME 300 further has a function to perform security

procedures such as mutual authentication with the user equipment 100 and encryption. The MME 300 further has a function to, for example, add the user equipment 100 to the tracking area list and newly set a bearer that is a logical path between the base station (eNodeBs) 201, 202 of the tracking area (TA) where the user equipment 100 is located and the external network (Packet Data Network (PDN)), in response to an attach request from the user equipment 100. The MME 300 further has a function to update the tracking area list, reset the bearer, etc. based on a Tracking Area Update (TAU) request from the user equipment 100. The MME 300 only processes control signals and does not handle user data.

10 **[0029]** The SGW 400 is a gateway that relays packets sent as user data. The SGW 400 is configured to communicate with the base stations (eNodeBs) 201, 202 and can keep track of the user equipment 100 to be handed over. The SGW 400 has a function to newly set or reset a bearer by cooperating with the MME 300.

15 **[0030]** The PGW 500 is a gateway that serves as a connection point to the external network (PDN). Specifically, the PGW 500 has functions such as assigning an IP address to the user equipment 100, user authentication, and packet control at the application level.

20 **[0031]** The external network (PDN) is a network connected to the core network, and is typically the Internet. The external network (PDN) has various servers (web server, mail server, content server, etc.) that communicate with the user equipment 100.

Hardware Configuration of User Equipment

25 **[0032]** FIG. 2 shows an example of a hardware configuration of the user equipment 100. The user equipment 100 of the present embodiment is communication equipment mounted on the vehicle 10, and performs various processes for connecting various devices (e.g., a car navigation system, an immobilizer system, and an emergency call system) mounted on the vehicle 10 to the external network (PDN). As shown in FIG. 2, such user equipment 100 includes a processor 101, a main storage unit 102, an auxiliary storage unit 103, a communication unit 104, etc. The user equipment 100 implements functions that match a predetermined purpose by the processor 101 loading a program

stored in a recording medium into a work area of the main storage unit 102 and executing the program.

[0033] The processor 101 is, for example, a central processing unit (CPU) or a digital signal processor (DSP). The processor 101 controls the user equipment 100 and
5 performs various information processing calculations.

[0034] The main storage unit 102 includes, for example, a random access memory (RAM) and a read only memory (ROM). As described above, the work area where the processor 101 executes the program is set in the main storage unit 102.

[0035] The auxiliary storage unit 103 includes, for example, an erasable
10 programmable ROM (EPROM) or a hard disk drive (HDD). The auxiliary storage unit 103 may include a removable medium, that is, a portable recording medium. The removable medium is, for example, a universal serial bus (USB) memory or a disc recording medium such as compact disc (CD) or digital versatile disc (DVD). The auxiliary storage unit 103 stores various programs, various data, and various tables in the
15 recording medium in a readable and writable manner. The programs stored in the auxiliary storage unit 103 include, in addition to an operating system (OS) etc., programs for implementing various functions for forbidding communication between the user equipment 100 and a fake base station. A part or all of the above information may be stored in the main storage unit 102. The information that is stored in the main storage unit
20 102 may be stored in the auxiliary storage unit 103.

[0036] The communication unit 104 is a wireless communication circuit that performs LTE wireless communication complying with the specifications of the 3GPP. The wireless communication circuit uses LTE mobile communication to communicate with the base stations (eNodeBs) 201, 202 etc.

[0037] The series of procedures that is performed by the user equipment 100
25 configured as described above can be performed by hardware. However, this series of procedures may be performed by software.

Functional Configuration of User Equipment

[0038] An example of a functional configuration of the user equipment 100 according to the present embodiment will be described with reference to FIG. 3. As shown in FIG. 3, the user equipment 100 of the present embodiment includes as its functional components a TAU procedure unit F110, a determination unit F120, an attach procedure unit F130, a TAI storage unit M110, and a forbid list storage unit M120. The TAU procedure unit F110, the determination unit F120, and the attach procedure unit F130 are implemented by the processor 101 executing the program loaded from the auxiliary storage unit 103 into the main storage unit 102. The combination of the TAU procedure unit F110, the determination unit F120, and the attach procedure unit F130 corresponds to the “control unit” according to the present disclosure. One of these three units, the TAU procedure unit F110, the determination unit F120, and the attach procedure unit F130, or a part of these three units may be implemented by the hardware circuit. The TAI storage unit M110 and the forbid list storage unit M120 are storage areas set in the auxiliary storage unit 103.

[0039] The TAI storage unit M110 stores the TAI of the tracking area (TA) where the user equipment 100 (vehicle 10) is located. Data stored in the TAI storage unit M110 is updated, for example, when an attach procedure is completed and when a TAU procedure is completed.

[0040] The forbid list storage unit M120 stores a list on which targets to be forbidden to communicate with the user equipment 100 are registered (hereinafter sometimes referred to as the “forbid list”). In the present embodiment, the targets to be forbidden to communicate with the user equipment 100 are managed by cell rather than by tracking area (TA). The cell to be forbidden to communicate with the user equipment 100 is a cell where a fake base station is located, and is determined by the determination unit F120 that will be described later. The “fake base station” in this example is a device that masquerades as a base station (eNodeB) and that is installed in the tracking area (TA) by a malicious third party.

[0041] FIG. 4 shows an example of the forbid list stored in the forbid list storage unit M120. As shown in FIG. 4, the forbid list has a cell identification (ID) field and a

forbidden time field. The configuration of the forbid list is not limited to the example shown in FIG. 4, and fields can be added, changed, or deleted as appropriate. Information (cell IDs) uniquely identifying the cells to be forbidden to communicate with the user equipment 100 are registered in the cell ID field. The time during which communication
 5 with the cell to be forbidden to communicate with the user equipment 100 is forbidden is registered in the forbidden time field. In the forbidden time field, five minutes is registered as an initial value, and then the remaining time is registered as it is counted down in seconds. When the remaining time for the cell reaches “0 minutes 00 seconds,” the information on this cell is deleted from the forbid list.

10 **[0042]** When the tracking area (TA) where the vehicle 10 (user equipment 100) is located changes, the TAU procedure unit F110 performs a procedure related to updating the tracking area (TA) where the vehicle 10 is located (Tracking Area Update (TAU)). Specifically, when the user equipment 100 receives a TAI notification signal from the base station (eNodeB) 201 or 202 in the tracking area (TA) where the vehicle 10 is located, the
 15 TAU procedure unit F110 compares the received TAI with the TAI stored in the TAI storage unit M110. When the received TAI is different from the TAI stored in the TAI storage unit M110, the TAU procedure unit F110 performs a procedure for establishing a control link (e.g., Radio Resource Control (RRC) connection) between the user equipment 100 and the base station (eNodeB) 201 or 202. At this time, the TAU procedure unit F110
 20 selects, as the base station with which the control link is to be established, the base station that is located in the cell not registered on the forbid list stored in the forbid list storage unit M120 and that has the greatest radio field strength from the base stations (eNodeBs) 201, 202 in the tracking area (TA) where the vehicle 10 is located. When the control link is established between such a base station (eNodeB) 201 or 202 and the user equipment 100,
 25 the TAU procedure unit F110 sends a TAU request using the control link. The TAU request includes temporary identification information (Globally Unique Temporary Identity (GUTI)) etc. assigned to the user equipment 100 by the MME 300.

[0043] The TAU request is sent to the MME 300 on the core network (EPC) via the base station (eNodeB) 201 or 202 with which the control link to the user equipment 100

has been established. In response to the TAU request, the MME 300 acquires information on the IMSI of the user equipment 100 and the bearer etc. based on the GUTI included in the TAU request. The MME 300 updates the tracking area list based on the acquired information. That is, the MME 300 deletes the user equipment 100 from the tracking area
5 list of the last tracking area (TA) where the user equipment 100 was located, and adds the user equipment 100 to the tracking area list of the tracking area (TA) where the user equipment 100 is currently located. The MME 300 also resets the bearer based on the acquired information. That is, the MME 300 releases the bearer from the base station in the last tracking area (TA) where the user equipment 100 was located to the external
10 network (PDN), and newly sets a bearer from the base stations (eNodeBs) 201, 202 in the tracking area (TA) where the user equipment 100 is currently located to the external network (PDN). When the update of the tracking area list and the resetting of the bearer are thus completed, a signal (TAU Accept) indicating that a TAU procedure on the core network (EPC) side is completed is sent from the MME 300 to the user equipment 100 via
15 the base station (eNodeB) 201 or 202. The signal (TAU Accept) includes information on the GUTI newly assigned by the MME 300, etc.

[0044] When the communication unit 104 of the user equipment 100 receives the signal (TAU Accept) indicating that a TAU procedure on the core network (EPC) side is completed, the TAU procedure unit F110 changes (updates) the TAI stored in the TAI
20 storage unit M110 to the TAI of the tracking area (TA) where the user equipment 100 is currently located. The TAU procedure unit F110 also performs a procedure of releasing the RRC connection established between the user equipment 100 and the base station (eNodeB) 201 or 202. When this procedure is completed, the TAU procedure unit F110 sends a signal (TAU Complete) indicating that a TAU procedure on the user equipment
25 100 side is completed to the MME 300 via the base station (eNodeB) 201 or 202.

[0045] There are cases where the MME 300 cannot acquire the information on the IMSI of the user equipment 100 and the bearer based on the GUTI included in the TAU request. For example, when the user equipment 100 for which an attach procedure has been completed returns to the radio access network (RAN) coverage area after moving out

of the radio access network (RAN) coverage area, and the user equipment 100 had been located out of the radio access network (RAN) coverage area for a certain period of time (e.g., about 70 minutes) or more, an implicit detach procedure may be performed on the core network (EPC) side. The “detach procedure” is a procedure of releasing the bearer, unassigning the IP address, unassigning the GUTI, etc. When the implicit detach procedure is performed, the MME 300 cannot acquire the information on the IMSI of the user equipment 100 and the bearer based on the GUTI included in the TAU request. In this case, the MME 300 sends a signal rejecting the TAU request for the reason that the user equipment 100 is unidentifiable (signal including Reason value #9 as defined in the 3GPP (TAU reject signal)) to the user equipment 100 via the base station (eNodeB) 201 or 202.

[0046] There may be cases where a fake base station having greater radio field strength than legitimate base stations has been installed in the tracking area (TA). In such cases, the TAU procedure unit F110 may select the fake base station as the base station with which the control link is to be established. As a result, the TAU request may be sent to the fake base station rather than to a legitimate base station. For example, when either the first base station (eNodeB) 201 or the second base station (eNodeB) 202 installed in the tracking area (TA) shown in FIG. 1 is a fake base station, the TAU request may be sent to the first base station (eNodeB) 201 or the second base station (eNodeB) 202, whichever is the fake base station. When the TAU request is sent to the fake base station, a TAU reject signal based on the same reason as in the case where the implicit detach procedure is performed is sent from the fake base station to the user equipment 100. In this case, it is effective to forbid communication with the fake base station in order to reduce unauthorized information leakage by the fake base station. However, even when the base station that is the source of the TAU reject signal is a legitimate base station (even when the user equipment 100 receives the TAU reject signal because the implicit detach procedure has been performed), communication with this base station will be forbidden. As a result, the user equipment 100 may become unconnectable to the external network (PDN), and an occupant of the vehicle 10 may not be able to use the Internet etc. In particular, the user equipment 100 that only has the LTE wireless communication function and does not have

the 3G wireless communication function tends to be unconnectable to the external network (PDN) for a long period of time. It is therefore necessary to accurately determine whether the TAU reject signal has been sent from a legitimate base station or a fake base station. In this example, when the communication unit 104 has received the TAU reject signal, the

5 TAU procedure unit F110 notifies the determination unit F120 of the fact that the communication unit 104 has received the TAU reject signal.

[0047] The determination unit F120 performs a procedure for determining whether the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is a legitimate base station or a false base station. In this example, the determination unit

10 F120 determines whether the predetermined condition including the following two conditions is satisfied. The predetermined condition may include only one of the following two conditions. (Condition 1) The user equipment 100 has received a signal requesting an IMSI from the base station. (Condition 2) The base station does not start encrypted communication involving an authentication procedure (signals such as the signal

15 requesting the IMSI are sent and received as plaintext data).

[0048] The predetermined condition is a condition specific to fake base stations. Accordingly, when the predetermined condition is satisfied (Conditions 1 and 2 are satisfied), the determination unit F120 determines that the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is a false base station. When the

20 determination unit F120 determines that the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is a false base station, the determination unit F120 registers the cell ID of the cell where this base station (eNodeB) 201 or 202 is located and the initial value (five minutes) of the forbidden time in the forbid list of the forbid list storage unit M120. The determination unit F120 further has a function to update the time registered in

25 the forbidden time field of the forbid list in seconds. Accordingly, the determination unit F120 further has a function to delete information on the cell from the forbid list when the forbidden time for this cell registered in the forbidden time field of the forbid list reaches “0 minutes 00 seconds.” When the predetermined condition is not satisfied, the determination unit F120 determines that the base station (eNodeB) 201 or 202 that is the

source of the TAU reject signal is a legitimate base station. The determination unit F120 sends the determination result to the attach procedure unit F130.

[0049] The attach procedure unit F130 performs an attach procedure based on the determination result received from the determination unit F120. First, when the
 5 determination unit F120 determines that the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is a legitimate base station, the attach procedure unit F130 sends an attach request to the MME 300 via the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal. The attach request is a signal requesting a procedure of newly setting a bearer from the base station (eNodeB) 201 or 202 in the tracking area (TA)
 10 where the user equipment 100 is located to the external network (PDN). The attach request includes the IMSI. The attach request may include information specifying the address of the external network (PDN).

[0050] In response to the attach request, the MME 300 performs security procedures such as mutual authentication with the user equipment 100 and encryption
 15 based on the IMSI. The MME 300 also sends a bearer setting request to the SGW 400 based on the address of the external network (PDN). When the attach request does not include the address of the external network (PDN), the MME 300 sends a bearer setting request to the SGW 400 based on a default address. The SGW 400 sends a request to set a communication path (packet transfer path) between the SGW 400 and the PGW 500 to the
 20 PGW 500. In response to this request, the PGW 500 assigns an IP address to the user equipment 100 and sets a communication path between the SGW 400 and the PGW 500. The MME 300 also sends a bearer setting request including the address of the SGW 400 to the base station (eNodeB) 201 or 202. At this time, the MME 300 also sends a signal (Attach Accept) indicating that an attach procedure is completed, an IP address assigned by
 25 the PGW 500, a GUTI assigned by the MME 300, etc. to the base station (eNodeB) 201 or 202. The base station (eNodeB) 201 or 202 sends the signal (Attach Accept) indicating that an attach procedure is completed, the IP address, the GUTI, etc. to the user equipment 100. The base station (eNodeB) 201 or 202 sets a communication path between the base station (eNodeB) 201 or 202 and the SGW 400. A bearer from the base station (eNodeB)

201 or 202 in the tracking area (TA) where the user equipment 100 is located to the external network (PDN) is newly set in this manner.

[0051] When the communication unit 104 of the user equipment 100 receives the signal (Attach Accept) indicating that an attach procedure is completed, the IP address, the
 5 GUTI, etc., the attach procedure unit F130 registers the tracking area (TA) where the user equipment 100 is located in the TAI storage unit M110.

[0052] According to the above procedures, it is possible to reduce the possibility that the user equipment 100 may become unconnectable to the external network (PDN) when an implicit detach procedure for the user equipment 100 is performed.

10 **[0053]** Next, when the determination unit F120 determines that the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is a fake base station, the attach procedure unit F130 sends an attach request to the MME 300 via the base station (eNodeB) 201 or 202 not determined to be a fake base station (the base station (eNodeB) 201 or 202 in the cell not registered in the forbid list) out of the base stations (eNodeBs)
 15 201, 202 in the tracking area (TA) where the user equipment 100 is located. In this case, a bearer is newly set and an IP address and a GUTI are newly assigned both on the core network (EPC) side by a procedure similar to that in the case where the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is a legitimate base station. This reduces the possibility that communication with a fake base station may be
 20 unnecessarily continued and the user equipment 100 may become unconnectable to the external network (PDN) when the base station (eNodeB) 201 or 202 that is the source of the TAU reject signal is the fake base station.

[0054] The series of procedures that is performed by the user equipment 100 configured as described above can be performed by hardware. However, this series of
 25 procedures may be performed by software. The functional configuration of the user equipment 100 is not limited to the example shown in FIG. 3, and components may be omitted, replaced, or added as appropriate.

Procedure Flow

[0055] Next, an overview of the flow of data that is sent and received by the user equipment 100 and the flow of procedures that are performed by the user equipment 100 of the present embodiment will be given with reference to FIGS. 5 and 6. FIG. 5 is a sequence diagram schematically illustrating the flow of data that is sent and received by the user equipment 100 and the flow of procedures that are performed by the user equipment 100 when a TAU request is sent to a legitimate base station (in the example shown in FIG. 5, the first base station (eNodeB) 201). FIG. 6 is a sequence diagram schematically illustrating the flow of data that is sent and received by the user equipment 100 and the flow of procedures that are performed by the user equipment 100 when a TAU request is sent to a fake base station (in the example shown in FIG. 6, the first base station (eNodeB) 201).

[0056] In FIG. 5, when the first base station (eNodeB) 201 notifies the user equipment 100 of the TAI (S10), the TAU procedure unit F110 of the user equipment 100 compares the received TAI with the TAI stored in the TAI storage unit M110. When the received TAI is different from the TAI stored in the TAI storage unit M110, the TAU procedure unit F110 determines that the tracking area (TA) where the user equipment 100 is located has changed (S11).

[0057] When the TAU procedure unit F110 determines that the tracking area (TA) where the user equipment 100 is located has changed, the TAU procedure unit F110 establishes a control link between the user equipment 100 and the first base station (eNodeB) 201 and sends a TAU request using the established control link (S12). When the radio field strength of the second base station (eNodeB) 202 is greater than the radio field strength of the first base station (eNodeB) 201, the TAU procedure unit F110 may establish a control link between the user equipment 100 and the second base station (eNodeB) 202 and send a TAU request to the second base station (eNodeB) 202.

[0058] When the first base station (eNodeB) 201 is a legitimate base station, the first base station (eNodeB) 201 sends the TAU request received from the user equipment 100 to the MME 300. In the example shown in FIG. 5, since an implicit detach procedure for the user equipment 100 has already been performed, the MME 300 sends a TAU reject signal including Reason value # 9 to the first base station (eNodeB) 201. In this case, the

first base station (eNodeB) 201 transfers the TAU reject signal received from the MME 300 to the user equipment 100 using the above control link (S13).

[0059] In the user equipment 100 that has received the TAU reject signal, the TAU procedure unit F110 notifies the determination unit F120 of the fact that the user
 5 equipment 100 has received the TAU reject signal. The determination unit F120 determines whether the predetermined condition described above is satisfied. In the example shown in FIG. 5, since the user equipment 100 has not received an IMSI request in the form of plaintext data, the determination unit F120 determines that the first base station (eNodeB) 201 is a legitimate base station (S14). The determination unit F120 sends the
 10 determination result to the attach procedure unit F130.

[0060] The attach procedure unit F130 sends an attach request using the control link established between the user equipment 100 and the first base station (eNodeB) 201 (S15). As a result, an attach procedure is performed on the core network (EPC) side. Namely, a bearer from the first base station (eNodeB) 201 to the external network (PDN) is
 15 newly set, and an IP address and a GUTI are newly assigned to the user equipment 100. The user equipment 100 thus becomes connectable to the external network (PDN) even when an implicit detach procedure has been performed due to, for example, the user equipment 100 having been out of the radio access network (RAN) coverage area for a certain period of time or more.

[0061] Next, in FIG. 6, when the second base station (eNodeB) 202 that is a legitimate base station notifies the user equipment 100 of the TAI (S20), the TAU procedure unit F110 compares the received TAI with the TAI stored in the TAI storage unit M110 and determines that the tracking area (TA) where the user equipment 100 is located
 20 has changed (S21).

[0062] When the TAU procedure unit F110 determines that the tracking area (TA) where the user equipment 100 is located has changed, the TAU procedure unit F110 establishes a control link between the user equipment 100 and either the first base station (eNodeB) 201 or the second base station (eNodeB) 202. In the example of FIG. 6, since the radio field strength of the first base station (eNodeB) 201 that is a fake base station is
 25

greater than the radio field strength of the second base station (eNodeB) 202 that is a legitimate base station, the TAU procedure unit F110 establishes a control link between the user equipment 100 and the first base station (eNodeB) 201 and sends a TAU request using the established control link. In this case, the TAU request from the user equipment 100 is
 5 sent to the first base station (eNodeB) 201 that is a fake base station rather than to the second base station (eNodeB) 202 that is a legitimate base station (S22).

[0063] When the first base station (eNodeB) 201 that is a fake base station receives the TAU request, the first base station (eNodeB) 201 sends an IMSI request signal to the user equipment 100 (S23). The IMSI request signal is a signal requesting to send
 10 the IMSI of the user equipment 100 to the first base station (eNodeB) 201. When the user equipment 100 sends a response signal including the IMSI (S24), the first base station (eNodeB) 201 sends a TAU reject signal to the user equipment 100 (S25).

[0064] Since the first base station (eNodeB) 201 that is a fake base station is not connected to the core network (EPC), it is not possible to start encrypted communication
 15 involving mutual authentication with the user equipment 100. The signals sent and received in S23 to S25 of FIG. 6 are therefore signals in the form of plaintext data. As a result, the determination unit F120 of the user equipment 100 determines that the first base station (eNodeB) 201 is a fake base station (S26).

[0065] When the determination unit F120 determines that the first base station
 20 (eNodeB) 201 is a fake base station, the cell ID of the cell (first cell) where the first base station (eNodeB) 201 is located and the initial value of the forbidden time are registered in the forbid list of the forbid list storage unit M120 (S27), and a countdown of the forbid time starts is started (S28). Communication with the cell where the first base station (eNodeB) 201 is located will thus be forbidden for 5 minutes.

[0066] While communication with the cell where the first base station (eNodeB)
 25 201 is located is forbidden, the attach procedure unit F130 sends an attach request to a base station located in other cell. In the example shown in FIG. 6, the attach request is sent to the second base station (eNodeB) 202 located in the second cell (S29). In response to the attach request, a bearer from the second base station (eNodeB) 202 to the external network

(PDN) is newly set, and a GUTI and an IP address are newly assigned to the user equipment 100. This reduces the possibility that the user equipment 100 may unnecessarily continue communication with the first base station (eNodeB) 201 that is a fake base station and that the user equipment 100 may become unconnectable to the external network (PDN).

[0067] When the forbidden time for the first cell registered in the forbid list then reaches “0 minutes 00 seconds,” the determination unit F120 deletes information on the first cell from the forbid list (S30).

[0068] Next, the flow of procedures that are performed by the user equipment 100 of the present embodiment will be described with reference to FIG. 7. FIG. 7 is a flowchart illustrating the flow of procedures that are performed by the user equipment 100 in response to a TAI notification signal. In the example shown in FIG. 7, it is assumed that the user equipment 100 (vehicle 10) is located in the tracking area (TA) shown in FIG. 1 (tracking area (TA) including the first cell and the second cell). It is also assumed that the radio field strength of the first base station (eNodeB) 201 is greater than the radio field strength of the second base station (eNodeB) 202.

[0069] In the procedure flow of FIG. 7, when the communication unit 104 receives a signal notifying the TAI of the tracking area (TA) where the user equipment 100 is located (Step S101), the communication unit 104 sends this signal to the TAU procedure unit F110.

[0070] The TAU procedure unit F110 compares the TAI included in this signal with the TAI stored in the TAI storage unit M110 (hereinafter the TAI stored in the TAI storage unit M110 is sometimes referred to as the “TAIold”). That is, the TAU procedure unit F110 determines whether the TAI and the TAIold match (Step S102). When the TAI and the TAIold match (yes in Step S102), the routine is ended. When the TAI and the TAIold do not match (no in Step S102), Step S103 is performed.

[0071] In Step S103, the TAU procedure unit F110 establishes a control link between the user equipment 100 and the first base station (eNodeB) 201, namely the base station having greater radio field strength out of the first and second base stations

(eNodeBs) 201, 202, and sends a TAU request using the established control link. As described above, the TAU request includes the GUTI assigned to the user equipment 100.

[0072] After Step S103 is performed, the TAU procedure unit F110 determines whether the communication unit 104 has received a TAU reject signal including Reason value #9 as a response signal to the TAU request (Step S104). At this time, the determination result in Step S104 is no when the communication unit 104 has received a signal (TAU Accept) indicating that a TAU procedure on the core network (EPC) side is completed. When no in Step S104, the routine is ended. As described above, the TAU procedure unit F110 then returns a signal (TAU Complete) indicating that a TAU procedure on the user equipment 100 side is completed. On the other hand, the determination result in Step S104 is yes when the communication unit 104 has received a TAU reject signal. When yes in Step S104, Step S105 is performed.

[0073] In Step S105, the determination unit F120 determines whether a predetermined condition is satisfied. The “predetermined condition” in this example is that both Condition 1 and Condition 2 described above are satisfied. As shown in FIG. 6 described above, the determination unit F120 determines that the predetermined condition is satisfied (yes in Step S105) when the communication unit 104 has received an IMSI request signal (Condition 1) and transmission and reception of signals including the IMSI request signal (transmission and reception performed in S23 to S25 in FIG. 6) has been performed in the form of plaintext data (Condition 2).

[0074] When yes in Step S105, the determination unit F120 determines that the first base station (eNodeB) 201 is a fake base station (step S106). In this case, the determination unit F120 registers the cell ID of the cell (first cell) where the first base station (eNodeB) 201 is located and the initial value of the forbidden time in the forbid list of the forbid list storage unit M120 (Step S107). Subsequently, the determination unit F120 starts a countdown of the forbidden time for the first cell in the forbid list (Step S108).

[0075] When Step S108 ends, the attach procedure unit F130 establishes a control link between the user equipment 100 and the second base station (eNodeB) 202 and sends an attach request using the established control link (Step S109). The attach request is thus

sent to the MME 300 via the second base station (eNodeB) 202. Accordingly, on the core network (EPC) side, a bearer from the second base station (eNodeB) 202 to the external network (PDN) is newly set, and a GUTI and an IP address are newly assigned to the user equipment 100. This reduces the possibility that the user equipment 100 may
 5 unnecessarily continue communication with the first base station (eNodeB) 201 that is a fake base station and that the user equipment 100 may become unconnectable to the external network (PDN).

[0076] When Step S109 ends, the determination unit F120 determines whether the forbidden time for the first cell registered in the forbid list has reached “0 minutes 00
 10 seconds” (step S110). When no in Step S110, Step S110 is repeated. On the other hand, when yes in Step S110, the determination unit F120 deletes information on the first cell from the forbid list (Step S111). When Step S111 ends, the procedure flow is ended. There may be a situation where a legitimate base station is also located in the same first cell as the first base station (eNodeB) 201 and there is no cells that are accessible by the user
 15 equipment 100 other than the first cell. When communication with the first cell continues to be prohibited for a long period of time in such a situation, the user equipment 100 may be unconnectable to the external network (PDN) for a long period of time. However, setting the forbidden time for the first cell to a time as short as about 5 minutes allows a TAU request or an attach request to be sent to the legitimate base station in the first cell after the
 20 elapse of the forbidden time. This also reduces the possibility that the user equipment 100 may become unconnectable to the external network (PDN) for a long period of time.

[0077] When the determination unit F120 determines in Step S105 that the predetermined condition is not satisfied (no in Step S105), it can be estimated that an implicit detach procedure has been performed on the core network (EPC) side. The
 25 determination unit F120 therefore determines that the first base station (eNodeB) 201 is a legitimate base station (Step S112).

[0078] When the determination unit F120 determines that the first base station (eNodeB) 201 is a legitimate base station, the attach procedure unit F130 sends an attach request using a control link established between the user equipment 100 and the first base

station (eNodeB) 201 (Step S113). When Step S113 is completed, the procedure flow is ended. This reduces the possibility that communication with the first base station (eNodeB) 201 that is a legitimate base station may be unnecessarily forbidden when a TAU reject signal is issued for a legitimate reason such as when an implicit detach process has
5 been performed. As a result, the possibility that the user equipment 100 may become unconnectable to the external network (PDN) is reduced.

[0079] According to the procedure flow of FIG. 7, it is possible to accurately determine whether a TAU reject signal including Reason value #9 is a signal sent from a fake base station. It is therefore possible to forbid communication between the user
10 equipment 100 and the fake base station when the source of the TAU reject signal is the fake base station. As a result, the possibility that communication between the user equipment 100 and the fake base station may be unnecessarily continued is reduced. When communication between the user equipment 100 and the fake base station is forbidden, the user equipment 100 sends an attach request to the MME 300 via a legitimate
15 base station different from the fake base station. This reduces the possibility that the user equipment 100 may become unconnectable to the external network (PDN). The possibility that communication between the user equipment 100 and a legitimate base station may be unnecessarily forbidden is also reduced when the TAU reject signal including Reason value #9 is a signal sent from the legitimate base station. The user
20 equipment 100 can thus send an attach request to the MME 300 via the legitimate base station. This reduces the possibility that the user equipment 100 may become unconnectable to the external network (PDN) when the TAU reject signal including Reason value #9 is sent from the legitimate base station.

[0080] According to the present embodiment, the possibility that the user
25 equipment 100 may become unconnectable to the external network (PDN) is reduced regardless of whether the source of the TAU reject signal is a fake base station or a legitimate base station. Therefore, communication between the user equipment 100 and the fake base station can be effectively reduced. As a result, the possibility that an occupant of the vehicle 10 may not be able to use the Internet etc. is reduced.

Others

[0081] The above embodiment is illustrative only, and the present disclosure may be modified as appropriate without departing from the spirit and scope of the present disclosure. The procedures and configurations described in the present disclosure can be
5 combined as desired as long as no technical contradiction occurs. The procedures described as being performed by one device may be allocated to and performed by a plurality of devices. Alternatively, the procedures described as being performed by different devices may be performed by one device. The type of hardware configuration that is used to implement each function in the computer system can be flexibly changed.

10 **[0082]** The present disclosure can also be implemented by supplying computer programs implementing the functions described in the above embodiment to a computer, and causing one or more processors of the computer to read and execute the programs. Such computer programs may be provided to the computer by a non-transitory computer-readable storage medium that can be connected to a system bus of the computer,
15 or may be provided to the computer via a network. The non-transitory computer-readable storage medium is a recording medium that can store information such as data and programs electrically, magnetically, optically, mechanically, or chemically and that can be read by a computer etc. Such a non-transitory computer-readable storage medium is a disc or disk of any type such as magnetic disk (e.g., floppy (registered trademark) disk or hard
20 disk drive (HDD)) or optical disc (e.g., compact disc read-only memory (CD-ROM), DVD, or Blu-ray disc). The non-transitory computer-readable storage medium may be a medium such as ROM, RAM, EPROM, electrically erasable programmable read-only memory (EEPROM), magnetic card, flash memory, optical card, or solid-state drive (SSD).

CLAIMS

1. An information processing device that is mounted on a vehicle and that performs Long-Term Evolution wireless communication, the information processing device characterized by comprising a processor configured to

send a request for update of a tracking area where the vehicle is located to a first base station in the tracking area where the vehicle is located,

determine whether a predetermined condition is satisfied when the information processing device has received from the first base station a signal rejecting the request for a reason that the information processing device is not identifiable, and

forbid communication with the first base station when the processor determines that the predetermined condition is satisfied.

2. The information processing device according to claim 1, wherein the predetermined condition includes a condition that the information processing device has received from the first base station a signal requesting subscriber identification information assigned to the information processing device.

3. The information processing device according to claim 2, wherein the predetermined condition further includes a condition that the first base station does not start encrypted communication involving an authentication procedure.

4. The information processing device according to any one of claims 1 to 3, wherein the processor is configured to forbid communication with a cell where the first base station is located in the tracking area where the vehicle is located when forbidding the communication with the first base station.

5. The information processing device according to claim 4, wherein the processor is configured to send an attach request to a second base station located in a cell different

from the cell where the first base station is located when the communication with the cell where the first base station is located has been forbidden.

6. The information processing device according to claim 4 or 5, wherein the processor is configured to forbid the communication with the cell for a predetermined time when forbidding the communication with the first base station.

7. The information processing device according to any one of claims 1 to 6, wherein the processor is configured to send the attach request to the first base station when the processor determines that the predetermined condition is not satisfied.

8. An information processing method in which a computer that is mounted on a vehicle and that performs Long-Term Evolution wireless communication is controlled, the information processing method characterized by comprising causing the computer to

send a request for update of a tracking area where the vehicle is located to a first base station in the tracking area where the vehicle is located,

determine whether a predetermined condition is satisfied when the computer has received from the first base station a signal rejecting the request for a reason that the computer is not identifiable, and

forbid communication with the first base station when the computer determines that the predetermined condition is satisfied.

9. The information processing method according to claim 8, wherein the predetermined condition includes a condition that the computer has received from the first base station a signal requesting subscriber identification information assigned to the computer.

10. The information processing method according to claim 9, wherein the predetermined condition further includes a condition that the first base station does not start encrypted communication involving an authentication procedure.

11. The information processing method according to any one of claims 8 to 10, wherein the computer forbids communication with a cell where the first base station is located in the tracking area where the vehicle is located when forbidding the communication with the first base station.

12. The information processing method according to claim 11, further comprising causing the computer to send an attach request to a second base station located in a cell different from the cell where the first base station is located when the communication with the cell where the first base station is located has been forbidden.

13. The information processing method according to claim 11 or 12, wherein the computer forbids the communication with the cell for a predetermined time when forbidding the communication with the first base station.

14. The information processing method according to any one of claims 8 to 13, further comprising causing the computer to send the attach request to the first base station when the computer determines that the predetermined condition is not satisfied.

15. A non-transitory storage medium mounted on a vehicle and storing a program that causes a computer that performs Long-Term Evolution wireless communication to
send a request for update of a tracking area where the vehicle is located to a first base station in the tracking area where the vehicle is located,
determine whether a predetermined condition is satisfied when the computer has received from the first base station a signal rejecting the request for a reason that the computer is not identifiable, and

forbid communication with the first base station when the computer determines that the predetermined condition is satisfied.

16. The non-transitory storage medium according to claim 15, wherein the predetermined condition includes a condition that the computer has received from the first base station a signal requesting subscriber identification information assigned to the computer.

17. The non-transitory storage medium according to claim 16, wherein the predetermined condition further includes a condition that the first base station does not start encrypted communication involving an authentication procedure.

18. The non-transitory storage medium according to any one of claims 15 to 17, wherein the program causes the computer to forbid communication with a cell where the first base station is located in the tracking area where the vehicle is located when forbidding the communication with the first base station.

19. The non-transitory storage medium according to claim 18, wherein the program further causes the computer to send an attach request to a second base station located in a cell different from the cell where the first base station is located when the communication with the cell where the first base station is located has been forbidden.

20. The non-transitory storage medium according to any one of claims 15 to 19, wherein the program further causes the computer to send the attach request to the first base station when the computer determines that the predetermined condition is not satisfied.