(12) UK Patent (19) GB (11) 2601372 (13) B

(45) Date of B Publication **14.12.2022**

(54) Title of the Invention: Wireless telecommunications network

(51) INT CL: ***H04W 52/28*** (2009.01) ***H04W 12/63*** (2021.01) ***H04W 16/28*** (2009.01) ***H04W 88/08*** (2009.01)

(21) Application No: **2018792.8**

(22) Date of Filing: **30.11.2020**

(60) Parent of Application No(s)
2114573.5 under section 15(9) of the Patents Act 1977

(43) Date of A Publication **01.06.2022**

(56) Documents Cited:

EP 3739781 A1	**CN 110996254 A**
US 20200077257 A1	**US 20140329485 A1**

(58) Field of Search:
As for published application 2601372 A viz:
INT CL **H04B, H04K, H04W**
Other: **WPI, EPODOC**
updated as appropriate

Additional Fields
Other: **None**

(72) Inventor(s):
Farhad Mehran
Richard Mackenzie

(73) Proprietor(s):
British Telecommunications Public Limited Company
1 Braham Street, London, E1 8EE, United Kingdom

(74) Agent and/or Address for Service:
British Telecommunications Public Limited Company
Intellectual Property Department, 9th Floor,
One Braham, Braham Street, London, E1 8EE,
United Kingdom

GB 2601372 B

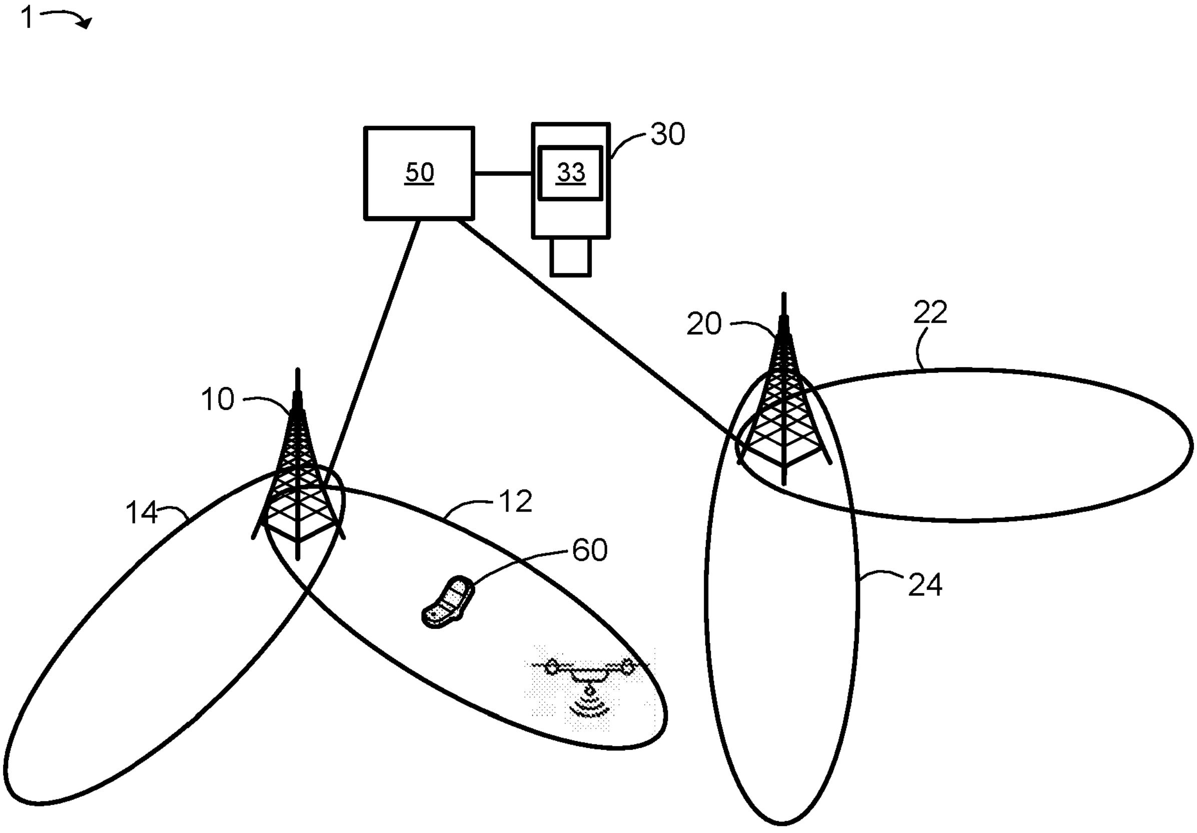

Figure 1

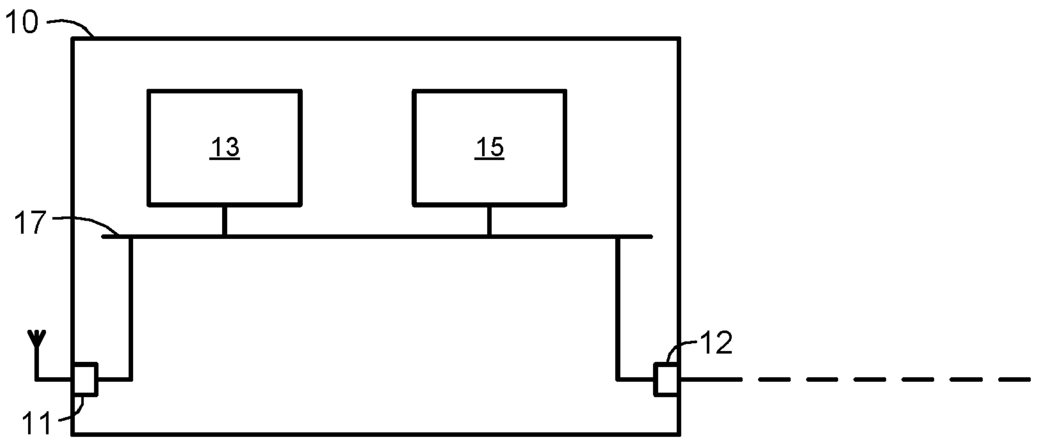

Figure 2

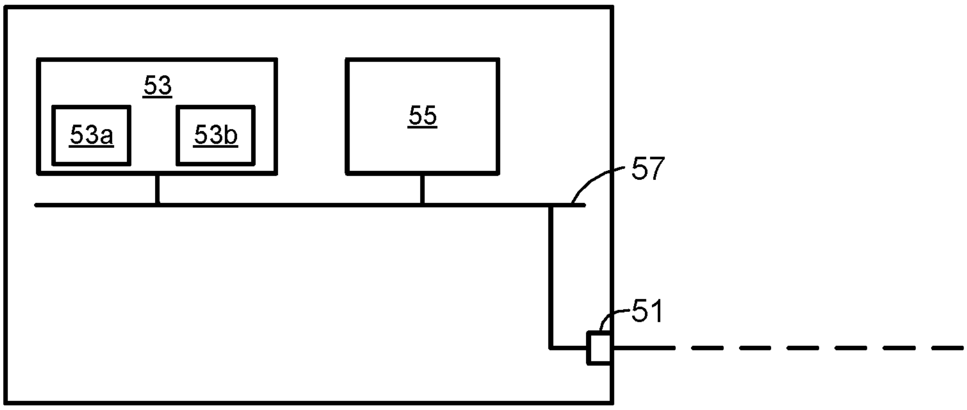

Figure 3

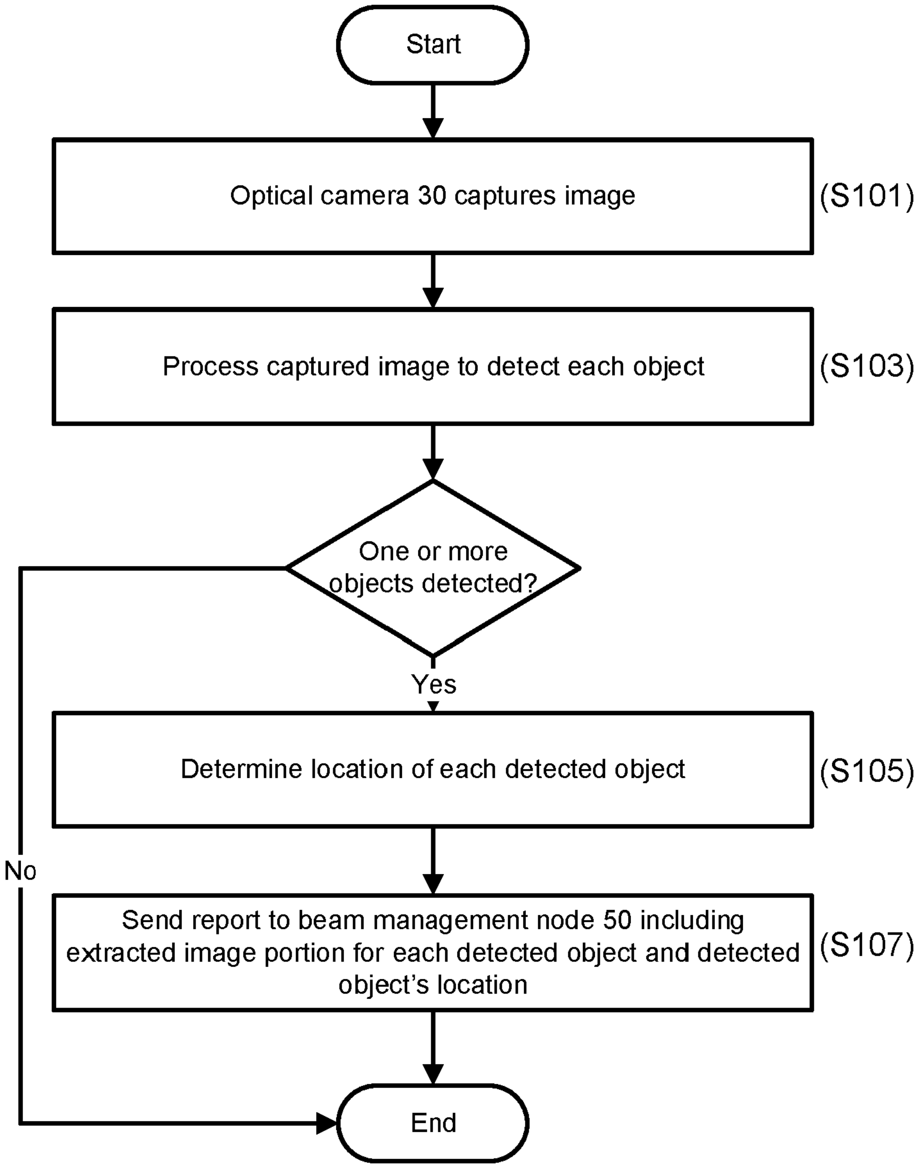
Start
Optical camera 30 captures image
(S101)
Process captured image to detect each object
(S103)
One or more objects detected?
Yes
No
Determine location of each detected object
(S105)
Send report to beam management node 50 including extracted image portion for each detected object and detected object’s location
(S107)
End

Figure 4

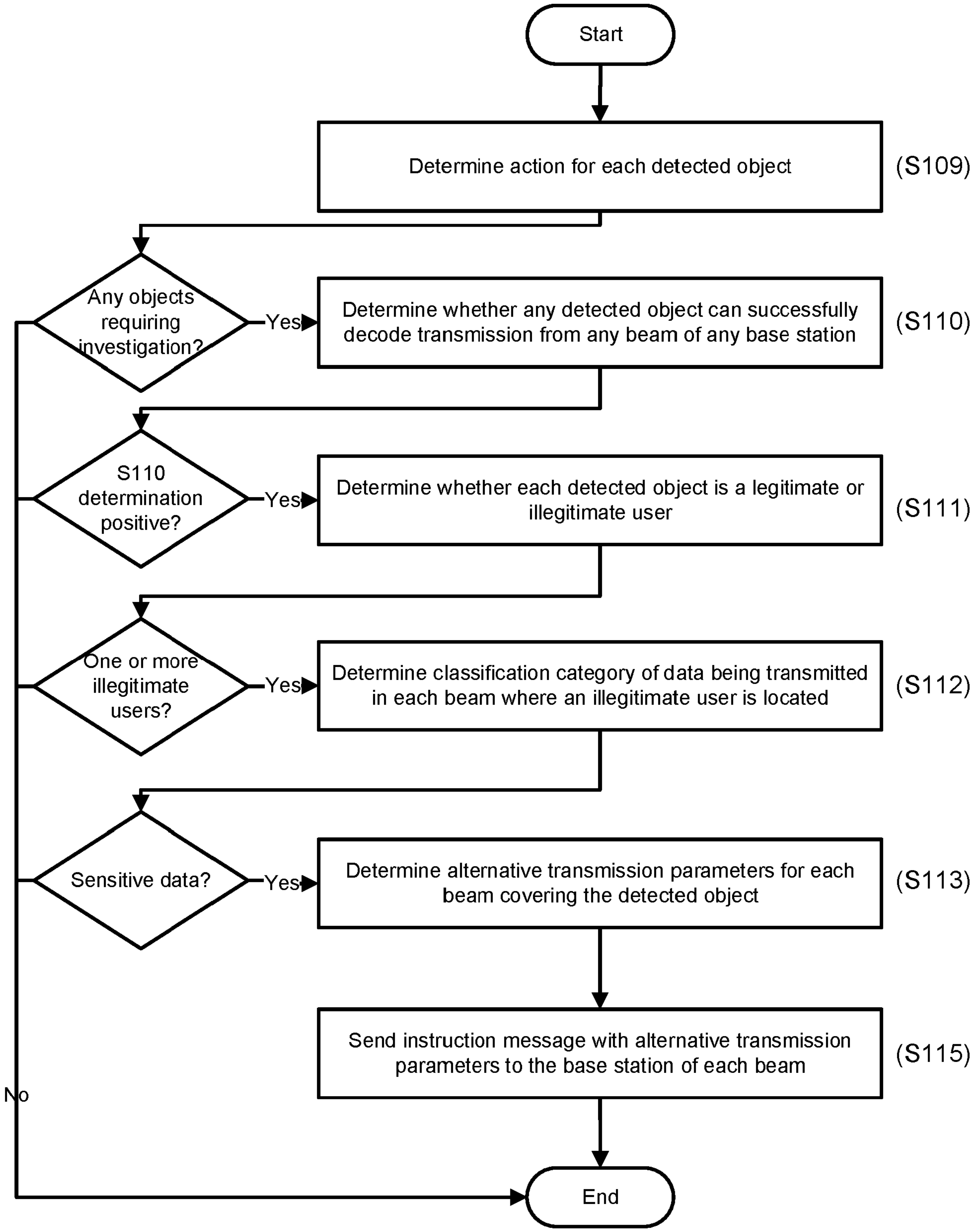
Start
Determine action for each detected object
(S109)
Any objects requiring investigation?
Yes
Determine whether any detected object can successfully decode transmission from any beam of any base station
(S110)
S110 determination positive?
Yes
Determine whether each detected object is a legitimate or illegitimate user
(S111)
One or more illegitimate users?
Yes
Determine classification category of data being transmitted in each beam where an illegitimate user is located
(S112)
Sensitive data?
Yes
Determine alternative transmission parameters for each beam covering the detected object
(S113)
Send instruction message with alternative transmission parameters to the base station of each beam
(S115)
No
End

Figure 5

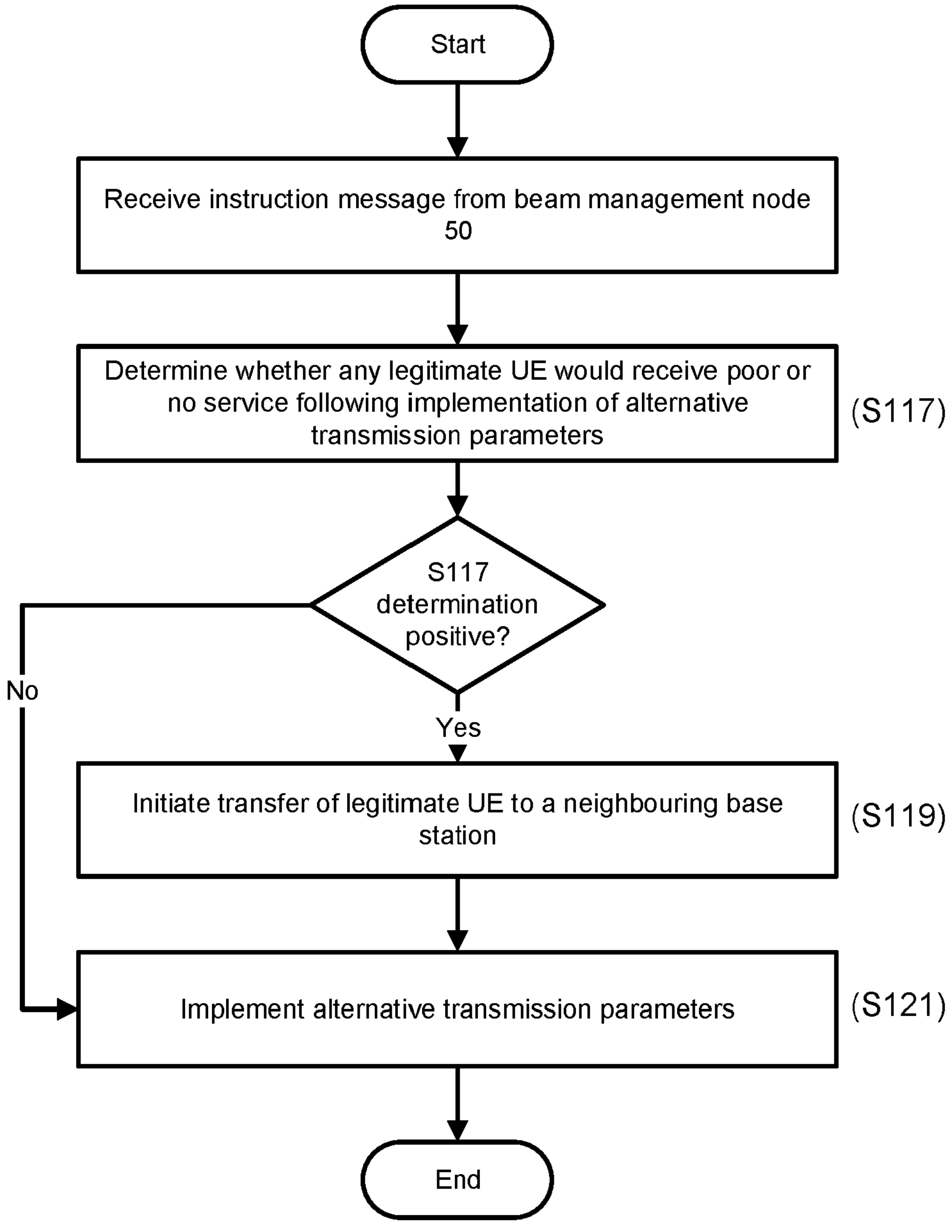
Start
Receive instruction message from beam management node 50
Determine whether any legitimate UE would receive poor or no service following implementation of alternative transmission parameters
(S117)
S117 determination positive?
No
Yes
Initiate transfer of legitimate UE to a neighbouring base station
(S119)
Implement alternative transmission parameters
(S121)
End

Figure 6

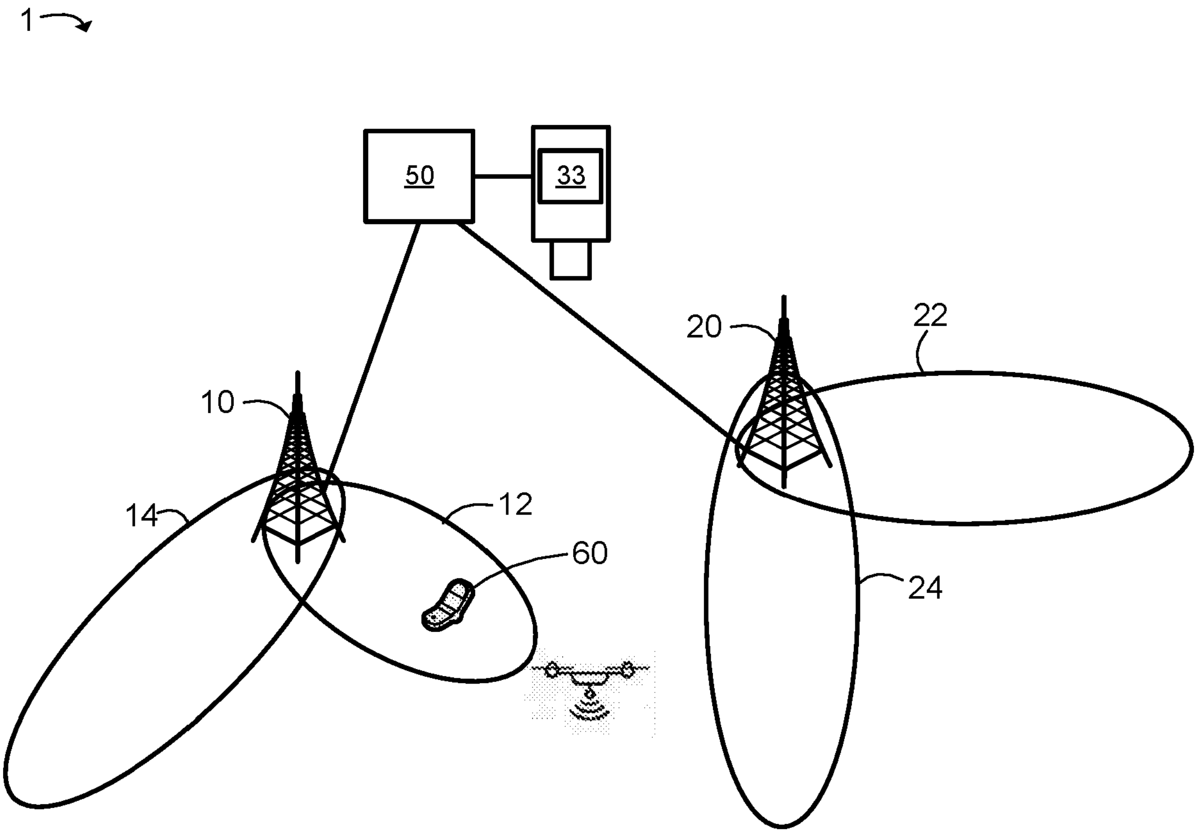

Figure 7

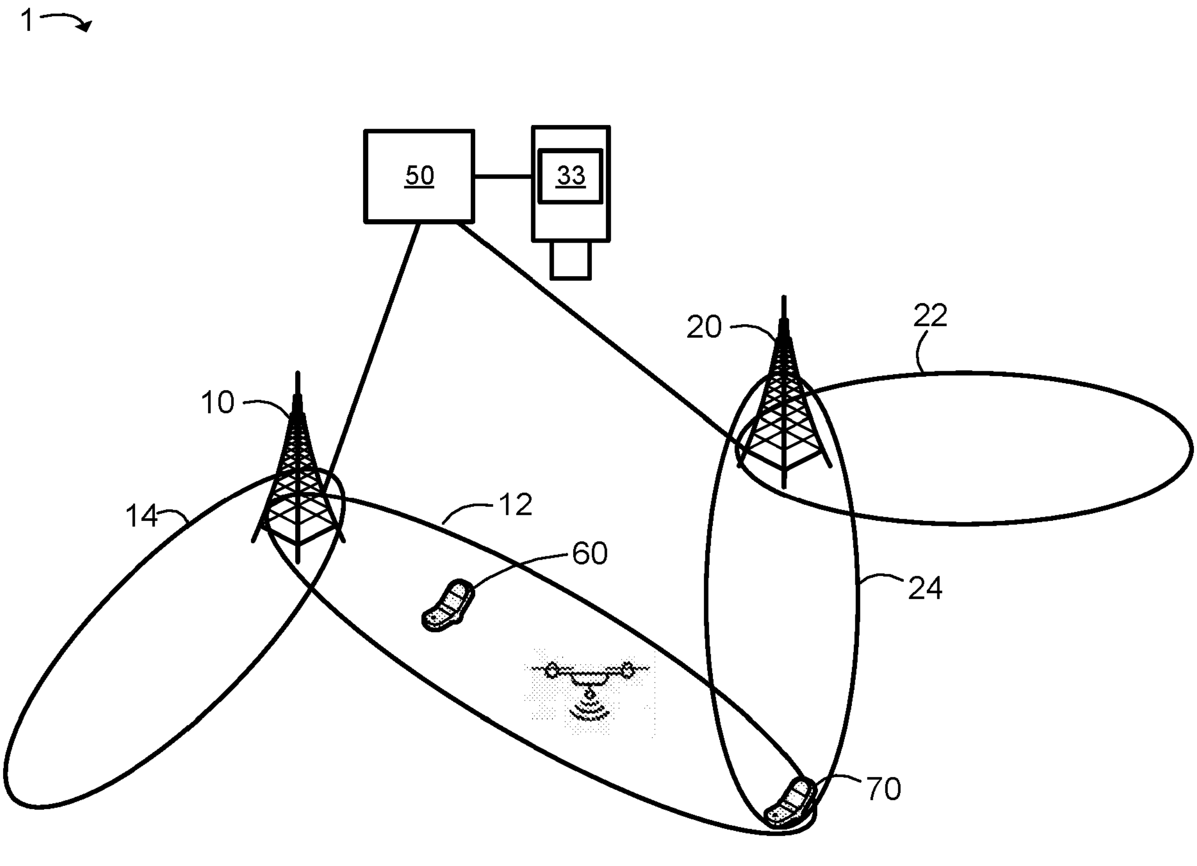

Figure 8

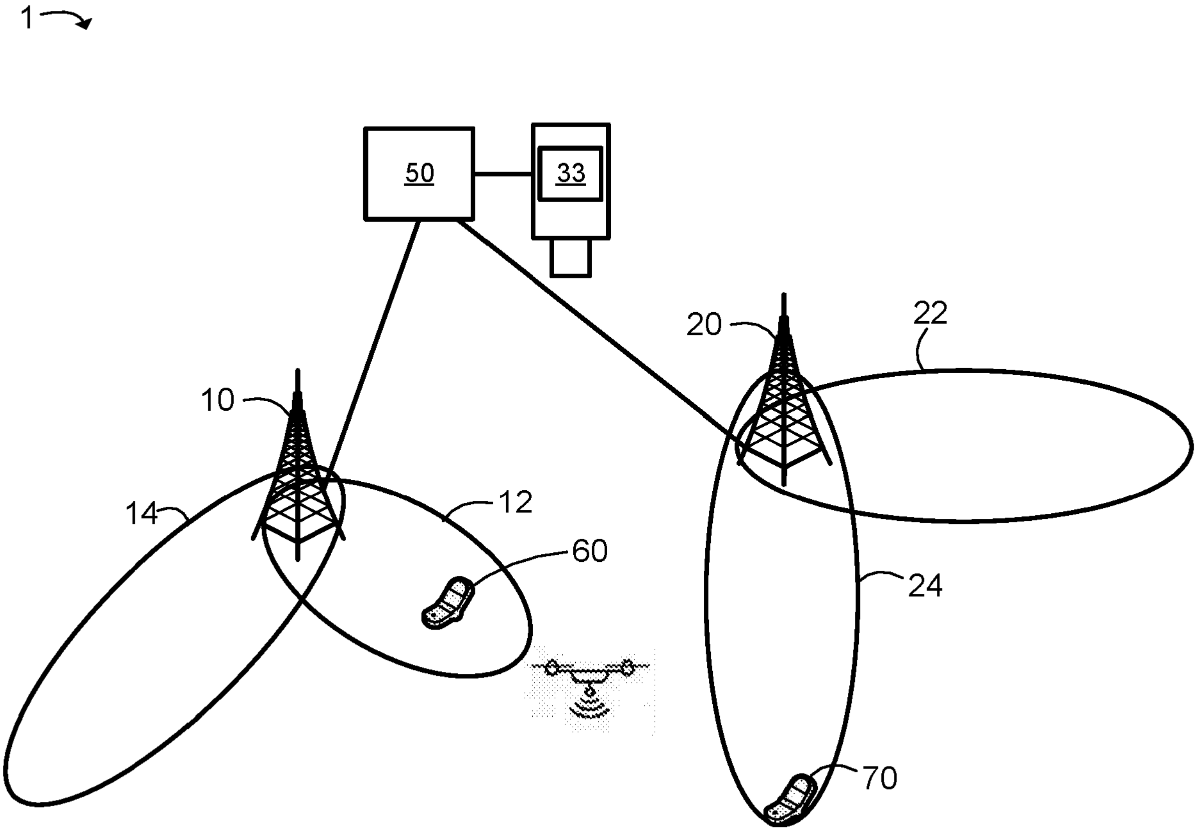

Figure 9

WIRELESS TELECOMMUNICATIONS NETWORK

Field of the Invention

The present invention relates to a wireless telecommunications network.

Background

In wireless telecommunications networks, access points and users communicate using wireless signals which may be intercepted by an eavesdropper. To prevent the eavesdropper from decoding a user's data, an encryption method may be used. Furthermore, wireless networks may be designed so that the wireless signals do not propagate outside a particular area (e.g. outside a building) so that physical access controls may also be used to prevent eavesdroppers from intercepting these signals. This may help prevent unauthorised receipt of user data where an encryption method is not being used or the encryption method has an unpatched or unknown vulnerability. This technique is also particularly relevant to modern wireless telecommunications networks utilising highly directional phased-array antennas, as the coverage areas of these antennas may be accurately defined. The present inventors have realised that these security techniques relying on coverage area configuration may now be compromised by the use of Unmanned Vehicles (UVs), such as Unmanned Aerial Vehicles (UAVs), which may gain unauthorised physical access to the coverage area of the wireless telecommunications network (that may have previously been inaccessible – such as a rooftop) and may intercept these wireless signals using an on-board User Equipment (UE).

Summary of the Invention

According to a first aspect of the invention, there is provided a method of operating a network node in a wireless telecommunications network, wherein the wireless telecommunications network includes a first access point having a first transmitter configured to transmit in a first coverage area, the method comprising the steps of: receiving, from a sensor, data indicative of an object within the first coverage area of the first access point’s first transmitter; determining, from the data, that the object is an illegitimate user; and, in response, causing a modification of the first access point so that the object cannot successfully receive a transmission from the first transmitter.

The data may identify a location of the object within the first coverage area of the first access point's first transmitter, and the step of causing a modification of the first access point may include reducing a value of signal strength of the transmission from the first transmitter at the object's location to below a signal strength threshold representing a minimum signal strength required to successfully receive the transmission from the first transmitter.

The first access point may serve a legitimate User Equipment, UE, and the method may further comprise the step of continuing service to the legitimate UE.

The step of continuing service may be achieved by causing a modification of the first access point so that a value of signal strength of the first transmitter at the legitimate UE's location is above the signal strength threshold. This step may be implemented where the legitimate UE is located closer to the first transmitter than the illegitimate UE.

The step of continuing service may be achieved by causing a transfer of the legitimate UE to a second transmitter in the wireless telecommunications network. This step may be implemented where the legitimate UE is located further away from the first transmitter than the illegitimate UE.

The step of causing the modification of the first access point may be to implement an encryption technique for the transmission from the first transmitter or to switch to a more secure encryption technique for the transmission from the first transmitter.

The method may further comprise the step of monitoring a location of the object, wherein the step of receiving data indicative of the object is part of the monitoring step.

The object may be an Unmanned Vehicle, UV, such as an Unmanned Aerial Vehicle, UAV.

According to a second aspect of the invention, there is provided a computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the steps of the first aspect of the invention. The computer program may be stored on a computer readable carrier medium.

According to a third aspect of the invention, there is provided a node for a wireless telecommunications network having a transceiver, memory and processor configured to cooperate to implement the steps of the method of the first aspect of the invention.

Brief Description of the Figures

In order that the present invention may be better understood, embodiments thereof will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 is a schematic diagram of a cellular telecommunications network of a first embodiment of the present invention;

Figure 2 is a schematic diagram of a first base station of the network of Figure 1;

Figure 3 is a schematic diagram of a beam management node of the network of Figure 1;

Figure 4 is a flow diagram of a process implemented by an optical camera in a first embodiment of a method of the present invention;

Figure 5 is a flow diagram of a process implemented by the beam management node in the first embodiment of the method of the present invention;

Figure 6 is a flow diagram of a process implemented by the first base station in the first embodiment of the method of the present invention;

Figure 7 is a schematic diagram of the network of Figure 1 following implementation of the method of Figures 4 to 6;

Figure 8 is a schematic diagram of a cellular telecommunications network of an enhancement to the first embodiment of the present invention, in a first state; and

Figure 9 is a schematic diagram of the network of Figure 9 in a second state.

Detailed Description of Embodiments

A first embodiment of a wireless telecommunications network of the present invention will now be described with reference to Figures 1 to 3. In this embodiment, the wireless telecommunications network is a cellular telecommunications network 1 including a first base station 10, second base station 20, an optical camera 30, a beam management node 50, and a first legitimate UE (the term “legitimate” will become clear following review of this description) 60. The first and second base stations 10, 20 are both configured for communications according to a cellular telecommunications protocol, such as the 5th Generation (5G) protocol defined by the 3rd Generation Partnership Project (3GPP). The first and second base stations 10, 20 include backhaul connections to a cellular core network (not shown).

As shown in Figure 1, the first and second base stations 10, 20 each include a plurality of transceivers that are configured for beamforming, so that distinct beams 12, 14, 22, 24 may be formed to provide voice and/or data service to users within the geographical areas defined by each beam. The first and second base stations 10, 20 may create, reconfigure and remove each beam of their respective sets of beams. One operating parameter of each transceiver of the plurality of transceivers for the first and second base station 10, 20 is the transmission power. Generally, increasing the transmission power of a transceiver increases both the capacity and the range of the transmissions. The signal strength of these transmissions decreases with distance from the transceiver (for example, by an inverse square law for propagation in free space or by some other function in a real-world example) such that each beam has a maximum coverage area outside of which the signal strength is below a signal strength threshold representing a minimum signal strength required for another wireless device to successfully decode these transmissions. The coverage area of each beam is also defined by other transmission parameters, such as its angle. In this embodiment, the first legitimate UE 60 is located within and connected to the first beam of the first base station 10.

Figure 1 further illustrates an optical camera 30. The optical camera 30 is configured to capture images or video (i.e. a sequence of images) in the visible spectrum (that is, electromagnetic radiation having wavelengths in the range of around 400 to 700 nanometres). The optical camera 30 is in a fixed location and is positioned so as to capture images or video of a geographical area that includes the first and second base stations 10, 20. The optical camera 30 includes a processor 33 for processing captured images, which will be explained in more detail below. The optical camera 30 also includes a Global Navigation Satellite System (GNSS) module, such as the Global Positioning System (GPS) module, to determine the coordinates of its location.

The first base station 10 is shown in more detail in Figure 2. The first base station includes a first communications interface 11 (connectable to an antenna), a second communications interface 12 (connectable to a core network via a backhaul connection), a processor 13 for processing wireless signals received/transmitted via the first and second communications interfaces, and memory 15, all connected via bus 17. The second base station 20 is substantially the same as the first base station 10.

The cellular telecommunications network 1 further includes a beam management node 50, residing in the core network and connected to both the first and second base stations 10, 20. As shown in more detail in Figure 3, the beam management node 50 includes a communications interface 51, a processor 53 and memory 55, all connected via bus 57. Memory 55 includes a database of visual training data for a computer vision learning agent. In this embodiment, memory 55 includes a database storing:

1. An identifier for a type of object (e.g. an Unmanned Aerial Vehicle, UAV);
2. One or more training images of that type of object (e.g. including a number of variations of that type of object, such as different UAV models and images at different angles); and
3. An action identifier (e.g. investigate, no investigation necessary) for that type of object.

The database may be periodically updated with new images.

The action identifier may be used to tailor the response of the beam management node 50 to different types of object that may be detected in the geographical area and their corresponding risk of being an eavesdropper. For example, a UAV may be high risk and therefore warrant further investigation to determine whether the UAV is a legitimate or an illegitimate entity, whereas an animal may be zero risk and so no further investigation is necessary.

In this embodiment, the processor 53 of beam management node 50 implements a computer vision process by a learning agent 53a and an inference agent 53b. The learning agent 53a is configured to train a machine learning algorithm, in this case a classification model, based on the visual training data in the database. The classification model maps between each training image from the database and the corresponding identifier for that type of object. The trained classification model may then be used by the inference agent 53b.

The learning agent 53a performs periodic learning operations to update the classification algorithm, thus adapting to any new images of objects.

The inference agent 53b uses the trained classification model in order to map between an input image (e.g. an image captured by the optical camera 30) and an object identifier (and therefore the action identifier associated with that object identifier).

A first embodiment of a method of the present invention will now be described with reference to Figures 1 and 4 to 7. Figure 1 illustrates the network 1 in an initial state, Figures 4 to 6 are flow diagrams of processes of this first embodiment of the method of the present invention implemented by the optical camera 30, beam management node 50 and first base station 10 respectively, and Figure 7 illustrates the network 1 in a final state following implementation of this first embodiment of the method of the present invention.

In a first step, S101, the optical camera 30 captures an image of the geographical region (that includes the first and second base station 10, 20). In step S103, the optical camera's processor 33 processes the image to detect each object in the image. If no objects are detected, then the process ends or loops back to step S101. In this example, the image includes a first detected object – the legitimate UE 60, and a second detected object – a UAV. In step S105, the optical camera's processor 33 determines the location of each detected object. In this embodiment, this is achieved using a phase detection focus technique to determine the distance between the optical camera 30 and each detected object, and further using the optical camera's location (captured by GPS). Suitable phase detection techniques include those described in International Patent Application Publication No. WO2017/052923A1, US Patent No. 10044926 and paper, "Depth map generation using a single image sensor with phase masks", Jinbeum Jang et al., Image Processing and Intelligent System Laboratory Graduate School of Advanced Imaging Science and Film.

In step S107, the optical camera sends a report to the beam management node 50 including, for each detected object, an extracted image portion of that detected object (being a portion of the captured image that includes the detected object), and the detected object's location (determined in step S105).

Turning to Figure 5, in step S109, the beam management node 50 receives the extracted image portion of each detected object and inputs each extracted image portion to the inference agent 53b. The inference agent 53b uses its trained classification model to output an object type identifier and an action identifier for that object. In this example in which the image includes two detected objects – the legitimate UE 60 and the UAV – the inference agent 53b outputs an object type identifier for the legitimate UE 60 as "User Equipment" and corresponding action identifier "Investigate", and further outputs an object identifier for the UAV as "UAV" and corresponding action identifier "Investigate". If there are no objects requiring further investigation, then the process ends or loops back to step S101.

In step S110, the beam management node 50 determines, for each detected object requiring further investigation, whether the detected object is able to successfully decode a transmission from any beam of the first and/or second base station (in other words, whether it is positioned within one or more beams of the first and/or second base station 10, 20). This may be achieved via several methods:

1) the beam management node 50 receives update messages identifying the coverage area of each beam of the first and second base station 10, 20 (within which the signal strength of a transmission from the transmitting base station is above a minimum signal strength threshold required for successful reception by a receiving node). The coverage area of each beam may be reported to the beam management node 50 as an explicit indication of the geographical area (e.g. a set of GPS coordinates defining a boundary line of the coverage area);
2) the beam management node 50 may receive transmission parameters for each beam of the first and second base stations (e.g. transmit power, antenna angle, etc.) and estimate the signal strength of a transmission from the transmitting node and the location of the detected object.

If none of the detected objects can successfully decode a transmission from any beam of either the first or second base station (that is, they are all located outside all coverage areas of all beams of the first and second base station 10, 20) then the process ends or loops back to step S101. If one or more detected objects can successfully decode a transmission from any beam of either the first or second base station, then the process proceeds to step S111. In this example, both detected objects are able to decode transmissions of the first beam of the first base station 10.

In step S111, the beam management node 50 determines whether each detected object (that can successfully decode a transmission of a beam of either the first or second base station, as determined in step S110) is a legitimate user or an illegitimate user. In this embodiment, this is achieved by receiving periodic location reports from all users of all base stations and performing a matching operation between the location of the detected object (sent to the beam management node 50 in step S107) and the location of the user in the periodic location report. If there is a match, then the detected object is deemed a legitimate user. If not (that is, the location of the detected objection from step S107 does not match any location of any user of the periodic location reports), then the detected object is deemed an illegitimate user. If all detected objects are deemed legitimate users, then the process ends or loops back to step S101. If at least one detected object is deemed an illegitimate user, then the process continues to step S112. In this example, the legitimate UE 60 is deemed a legitimate user and the UAV is deemed an illegitimate user.

In step S112, the beam management node 50 determines the classification category of the data being transmitted in each beam where an illegitimate user is located (the first beam of the first base station 10 in this example). This may be achieved by request-response messaging with the base station transmitting each beam. If the data being transmitted is not sensitive, then the process ends or loops back to step S101. If the data is sensitive, then the process proceeds to step S113. In this example, the data transmitted in the first beam of the first base station 10 is sensitive.

In step S113, the beam management node 50 determines alternative parameters for each beam that contains an illegitimate user and is transmitting sensitive information (determined in steps S110 to S112 – the first beam of the first base station 10 in this example). These alternative parameters are determined so that the illegitimate UE cannot successfully receive a transmission from the beam. In this embodiment, this is implemented by reducing the signal strength of transmissions of that beam are below (preferably by a configurable factor) the minimum signal strength threshold required for successful reception by a receiving node at the location of the illegitimate user. In this example, the alternative parameter is the transmission power, so that only the range of the beam is reduced.

In step S115, the beam management node 50 sends an instruction message to each base station of each beam identified in step S110, instructing the base station to implement the alternative transmission parameters determined for the identified beam. Turning to Figure 6, in step S117, each base station determines whether there are any legitimate UE (such as the first legitimate UE 60) that would receive poor or no service following implementation of the alternative transmission parameters. If so, then the process continues to step S119. In this example, the first base station 10 determines that there are no UE that would receive poor or no service following implementation of the alternative transmission parameters, so the process continues to step S121.

In step S121, each base station implements the alternative transmission parameters. In this example, the first base station 10 implements the alternative transmission parameters so as to reduce the transmission power of the antenna that transmits the first beam (or of the plurality of antennas that cooperate to transmit the first beam) so that the coverage area of the first beam no longer covers the illegitimate user (or, in other words, so that the signal strength of the first beam at the location of the illegitimate user is less than the minimum signal strength required to successfully decode a transmission of the first beam). The state of the network following this reconfiguration is shown in Figure 7. Figure 7 also illustrates the first legitimate UE 60 remaining within the first beam of the first base station 10, such that it may continue to successfully receive transmissions of the first beam following the reconfiguration.

An enhancement to the above embodiment will now be described with reference to Figure 8 and 9, which illustrate a network prior to reconfiguration and following reconfiguration respectively. The network includes both a first legitimate UE 60 and second legitimate UE 70 that are both connected to the first beam 12 prior to the reconfiguration. As in the embodiment above, the first legitimate UE 60 is positioned between the illegitimate user and the first base station 10. However, the second legitimate UE is positioned further away from the first base station 10 than the illegitimate user, such that, following the reconfiguration of step S121, the second legitimate UE 70 would be outside the coverage area of the first beam. The reconfiguration would cause the radio link between the second legitimate UE and the first base station 10 to fail so, to avoid this, in step S119 (as shown in Figure 6), the first base station 10 initiates a transfer of the second legitimate UE 70 to a neighbouring base station. In this embodiment, this is achieved by instructing the second legitimate UE 70 to prepare and report measurements of its neighbouring base stations. The first base station 10 reviews this report and determines that the second base station 20 is a target base station for a handover of the second legitimate UE and therefore sends a handover request to the second base station 20. If the second base station 20 accepts the handover request (which should be based on its state following any reconfiguration instructed by the beam management node 50), then the second legitimate UE is transferred to the second base station 20. The second legitimate UE may also be transferred by a cell reselection process.

The skilled person will understand that there are other parameters, other than transmission power, that may be changed so that, following the reconfiguration, the illegitimate user can no longer successfully receive transmissions. These may be, for example, the angle of the beam or the shape of the beam. Furthermore, the change in angle/shape of the beam may be so as to provide coverage for all legitimate users, but no coverage for illegitimate users, so as to provide continuity of service without having to transfer any legitimate user to another access point. The parameter may also include, additionally or alternatively to a change in the transmission parameters of the beam, the use of an encryption method or switch to a more secure encryption method, such as switching from Advanced Encryption Standard (AES)-128 to AES-192 or AES-256 (such that the coverage area of the beam does not change, but an encryption method in the coverage area is made more secure).

In a further enhancement to the above embodiment, the beam management node 50 may track the location of the UAV (e.g. by instructing the optical camera 30 to track the UAV and periodically report its location), and take pre-emptive action to adjust the coverage area of any beam/base station that the UAV is an illegitimate user of so that the UAV does not receive service or is able to receive from any beam/base station. The beam management node 50 may also instruct other optical cameras to track the UAV if, for example, the UAV moves out of view of the optical camera 30. This function may be limited to objects having a particular action identifier, such as “Investigate and Monitor”.

The skilled person will understand that the above embodiment applies to any form of wireless telecommunications network, such as a wireless local area network or wireless wide area network.

The skilled person will also understand that it is non-essential for the beam management node 50 to further investigate whether an object is legitimate or not. That is, the beam management node 50 may classify a particular object type (e.g. UAV) as illegitimate in all circumstances and therefore skip step S111. In the above embodiments, the beam management node 50 determines whether the UE is a legitimate UE or an illegitimate UE based on a comparison of its location with the locations of all known legitimate users. The skilled person will understand that this test may be implemented in other ways, such as a comparison of the image of the UAV under investigation with images of known legitimate UAVs and/or known illegitimate UAVs.

Furthermore, the skilled person will understand that it is non-essential for the beam management node 50 to determine whether the information being transmitted by a beam is sensitive or not. This step may be skipped so as to always take responsive action to in response to detecting an illegitimate user.

In the above embodiments, the beam management node 50 is a core networking node. However, this is non-essential. For example, the beam management node may be a module of a Radio Access Node (RAN) Intelligent Controller (RIC).

In the above embodiment, an optical camera is used to detect an object in the coverage area of a base station. However, this is non-essential, and any other suitable sensor for detecting an object and estimating the location of the object may be used (such as a LIDAR sensor).

The skilled person will understand that any combination of features is possible within the scope of the invention, as claimed.

CLAIMS

1. A method of operating a network node in a wireless telecommunications network, wherein the wireless telecommunications network includes a first access point having a first transmitter configured to transmit in a first coverage area, wherein the first access point serves a legitimate User Equipment, UE, the method comprising the steps of:

receiving, from a sensor, data indicative of an object within the first coverage area of the first access point's first transmitter, the data identifying a location of the object within the first coverage area of the first access point's first transmitter;

determining, from the data, that the object is an illegitimate user; and, in response,

causing a modification of the first access point so that the object cannot successfully receive a transmission from the first transmitter by reducing a value of signal strength of the transmission from the first transmitter at the object's location to below a signal strength threshold representing a minimum signal strength required to successfully receive the transmission from the first transmitter, and

continuing service to the legitimate UE by causing a transfer of the legitimate UE to a second transmitter in the wireless telecommunications network.

2. A method as claimed in Claim 1, wherein the step of causing the modification of the first access point also includes implementing an encryption technique for the transmission from the first transmitter or switching to a more secure encryption technique for the transmission from the first transmitter.

3. A method as claimed in any one of the preceding claims, further comprising the step of monitoring a location of the object, wherein the step of receiving data indicative of the object is part of the monitoring step.

4. A method as claimed in any one of the preceding claims, wherein the object is an Unmanned Vehicle, UV.

5. A method as claimed in Claim 4, wherein the object is an Unmanned Aerial Vehicle, UAV.

6. A computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the steps of any one of the preceding claims.

7. A computer readable carrier medium comprising the computer program of Claim 6.

8. A node for a wireless telecommunications network having a transceiver, memory and processor configured to cooperate to implement the steps of any one of Claims 1 to 5.