(54) Title: DETECTING ROGUE RADIO FREQUENCY BASED TAGS BASED ON LOCATIONING
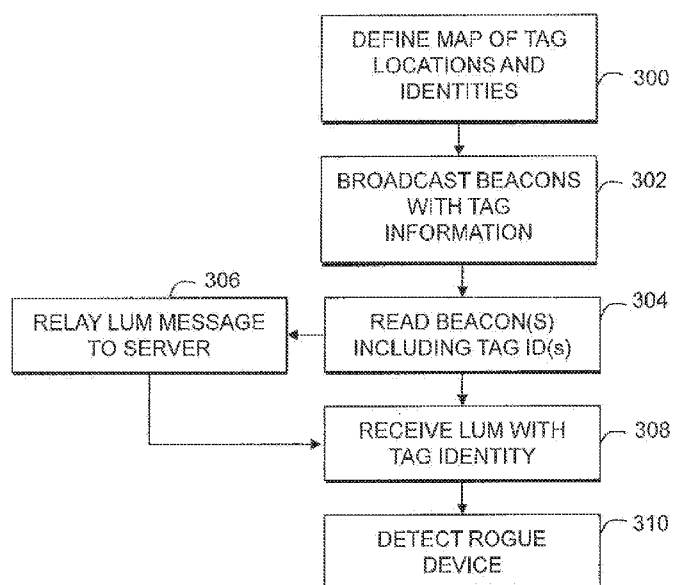
FIG. 3

(57) Abstract: A method and system for detecting
rogue radio frequency based devices includes a plur-
ality of radio frequency based tags disposed at dif-
ferent locations within an area and operable to peri-
odically broadcast information in a beacon, the in-
formation including each tag's unique identity in-
formation. A map of the area specifies identified ra-
dio frequency based tags and their respective loca-
tions within the area. A mobile device reads beacons
in proximity to the radio frequency based tags and
sends location update messages to a server that de-
tects rogue radio frequency based devices within the
area based on the location update messages and the
map.

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *with amended claims (Art. 19(1))*

(88) Date of publication of the international search report:
3 July 2014

Date of publication of the amended claims: 31 July 2014

1. A system for detecting rogue radio frequency based devices (112), comprising:

a plurality of radio frequency based tags (106) configured to be disposed at different locations within an area and operable to periodically broadcast information in a beacon (108), the information including each tag's unique identity information, respectively;

a map of the area, the map for specifying identified radio frequency based tags and their respective locations within the area;

a mobile device (104) operable to read at least one beacon (108) in proximity to at least one of the radio frequency based tags (106) and send at least one location update message (110), respectively; and

a server (100) operable to detect rogue radio frequency based devices within the area based on an incorrect location update message and the map.

2. The system of claim 1, further comprising at least one access point (103) operable to relay the at least one location update message to the server, wherein each access point is operable to serve a subset area (200) of the map.

3. The system of claim 1, wherein the server is also operable to associate a location of the mobile device to the mapped location of the radio frequency based tag identified in the at least one location update message (110).

4. The system of claim 1, wherein the server is further operable to receive subsequent location update messages from the mobile device and associate these subsequent location update messages to detect the rogue radio frequency based device.

5. The system of claim 4, wherein the server is operable to check that the reported tags create a correct sequential navigation path of neighboring tags.

6. The system of claim 2, wherein the at least one access point is operable to measure a received signal strength indicator of the location update message from the mobile device, and wherein the server is further operable to validate whether the received signal strength for a reported tag is appropriate for that AP and the map location of the tag.

7. The system of claim 1, wherein when at least one sequential location update message includes the identities of at least two tags, the server is operable to determine from the map whether any reported tags are distal from each other, indicating the existence of a rogue device.

8. The system of claim 1, wherein when at least one sequential location update message includes the identities of at least two tags, the server is operable to determine whether these tag identities that have not been historically included together, indicating the existence of a rogue tag.

9. The system of claim 1, wherein the server receiving an unknown tag identity in the location update message indicates the existence of a rogue tag.

10. The system of claim 1, wherein the server receiving a known tag identity, but determining that the tag is in an improper location, indicates the existence of a rogue tag.

11. The system of claim 1, wherein the server is further operable to locate a rogue device using an access point coverage area and a legitimate location of a mobile device proximal in time to detecting the rogue device.

12. The system of claim 1, wherein the information includes a battery status, and wherein the server is further operable to determine if a battery level of an identified tag keeps changing between different battery levels, indicating a rogue tag.

13. The system of claim 1, wherein the information includes a sequence number, and wherein the server is further operable to determine if a sequence number of an identified tag becomes out of sequence, indicating a rogue tag.

14. A method for detecting rogue radio frequency based devices, comprising:

defining (300) a map of an area, the map specifying identified radio frequency based tags and their respective locations within the area;

the radio frequency based tags periodically broadcasting (302) information in respective beacons, the information including each tags unique identity information, respectively;

reading (304) at least one beacon by a mobile device in proximity to at least one of the radio frequency based tags, respectively;

receiving (308) at least one location update message from the mobile device, the message including identity information in the beacon; and

detecting (310) rogue radio frequency based devices within the area based on an incorrect location update message and the map.

15. The method of claim 14, further comprising the step of relaying (306) the message to an area server, and wherein the detecting step is performed by the server.