



(51) International Patent Classification:
B60R 25/24 (2013.01)

(21) International Application Number:
PCT/EP2017/082004

(22) International Filing Date:
08 December 2017 (08.12.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1700300.5 09 January 2017 (09.01.2017) GB

(71) Applicant: **JAGUAR LAND ROVER LIMITED**
[GB/GB]; Abbey Road Whitley, Coventry Warwickshire
CV3 4LF (GB).

(72) Inventors: **CORNE, Hester**; c/o Jaguar Land Rover,
Patents Department W/1/073 Abbey Road, Whitley, Coventry
Warwickshire CV3 4LF (GB). **BRADLEY, Andrew**; c/
o Jaguar Land Rover, Patents Department W/1/073 Abbey
Road, Whitley, Coventry Warwickshire CV3 4LF (GB).

(74) Agent: **CHANG, Seon-Hee**; Jaguar Land Rover, Patents
Department W/1/073 Abbey Road, Whitley, Coventry War-
wickshire CV3 4LF (GB).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, 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,

(54) Title: VEHICLE KEYLESS ENTRY SYSTEMS

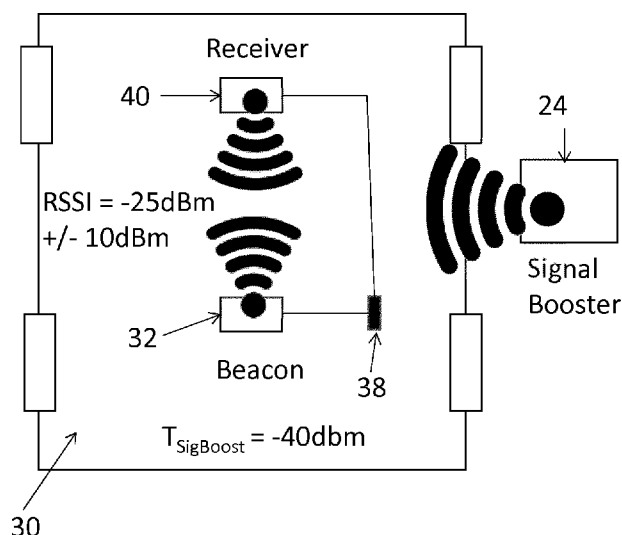


Figure 4

(57) Abstract: A method of detecting a relay attack in a vehicle (10) equipped with a passive entry system (99), the method comprising: sending a passive entry communication signal from a transmitter (14) within the vehicle (10); receiving the passive entry communication signal from the transmitter (14) at a receiver (20) within the vehicle (10); comparing the signal strength of the received passive entry communication signal to a predetermined threshold signal strength value; determining a relay attack in the event that the received signal strength exceeds the predetermined threshold signal strength value.

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))*

VEHICLE KEYLESS ENTRY SYSTEMS

TECHNICAL FIELD

- 5 The present disclosure relates to vehicle keyless entry systems and particularly, but not exclusively, to a passive entry system for a vehicle. Aspects of the invention relate to a method of determining a relay attack, to a control module for a passive entry system, to a passive entry system for a vehicle and to a vehicle.

10 BACKGROUND

- In existing passive entry systems it is possible to gain authorised access to a vehicle and, in some systems, start the vehicle's engine without any interaction on the part of the authorised user or vehicle owner with a key fob. Such systems work by the vehicle
15 sending a radio signal to the key fob which the key fob then responds to by sending an unlock request. The challenge signal from the vehicle may be sent in response to a door handle being pulled, for example.

- Such systems are potentially vulnerable to relay attacks where a signal booster is used
20 to relay the challenge signal from the vehicle and/or the challenge response signal from the key fob over larger distances such that a third party can gain authorised access to the vehicle.

- The present invention has been devised to mitigate or overcome at least some of the
25 above-mentioned problems.

SUMMARY OF THE INVENTION

- According to an aspect of the present invention there is provided a method of detecting
30 a relay attack on a vehicle equipped with a passive entry system, the method comprising: sending a passive entry communication signal from a transmitter within the vehicle; receiving a passive entry communication signal associated with the transmitter at a receiver within the vehicle; comparing the signal strength of the received passive entry communication signal to a predetermined threshold signal strength value; and

determining a relay attack in the event that the signal strength of the received passive entry communication signal exceeds the predetermined threshold signal strength value.

- 5 The present invention provides a method of determining an occurrence of a relay attack on a passive entry system by monitoring the signal strength of a passive entry communication signal issued by a transmitter in the vehicle via a receiver within the vehicle. In the normal course of operation the vehicle would send out a passive entry communication signal as part of the vehicle unlock process. Such a signal may be sent
10 either periodically prior to any specific user interaction or in response to a user interaction with the vehicle such as pulling a door handle. The receiver within the vehicle would therefore receive such a signal as well as the vehicle key fob. Since the relationship between the transmitter and receiver within the vehicle is fixed the receiver would, in the normal course of events, receive a signal at an expected signal strength
15 or within an expected signal strength range.

However, in the event of a relay attack, the signal strength of the passive entry communication signal received at the receiver would increase as a result of the signal booster being used by the relay attacker. Exceeding a predetermined threshold for the
20 received signal would trigger a determination that a relay attack is occurring. In response to determining that a relay attack is occurring the method may comprise outputting a suitable notification signal or control signal.

When used herein and throughout the specification, "associated with" is intended to
25 cover a passive entry communication signal sent by the transmitter and received by the receiver directly, and/or a passive entry communication signal received at the receiver indirectly via an external device. For example, the external device may comprise a signal booster or the like used to relay a passive entry communication signal sent from the transmitter, and relay said signal to the receiver at the same or
30 different frequency and/or amplitude/signal strength.

Optionally, the comparing step comprises measuring a received signal strength indication (RSSI) of the received signal and comparing the measured RSSI to the threshold signal strength value.

Optionally, the passive entry communication signal is sent from the transmitter in response to a door unlock request.

- 5 Optionally, the passive entry communication signal is sent periodically from the transmitter. For example, the passive entry communication signal may be sent approximately every second. Other time periods between the passive entry communication signal being sent by the transmitter are envisaged.
- 10 Optionally, the transmitted passive entry communication signal comprises a Bluetooth® or Bluetooth low energy (Bluetooth LE®) signal, the transmitter comprises a Bluetooth® beacon and the receiver comprises a Bluetooth® receiver.

- 15 Optionally, the transmitted passive entry communication signal comprises a low frequency (LF) signal, the transmitter comprises an LF transmitter and the receiver comprises an LF receiver.

- 20 Optionally, the method comprises immobilising the vehicle in the event that a relay attack is determined.

Optionally the method comprises sending a notification signal to a key device in the event that a relay attack is determined.

- 25 Optionally, the method comprises sending a notification signal to a cloud based alarm system in the event that a relay attack is determined.

Optionally the method comprises sending a control signal to sound a vehicle alarm in the event that a relay attack is determined.

- 30 Optionally the method comprises sending a control signal to the vehicle locking system to maintain vehicle doors in a locked state or locking a vehicle door in the event that a relay attack is determined.

According to a further aspect of the present invention there is provided a control module for a passive entry system for a vehicle, the control module comprising: an input arranged to receive data relating to a passive entry communication signal, the passive entry communication signal being sent from a transmitter within the vehicle;
5 and a processor arranged to compare a signal strength of a received passive entry communication signal associated with the transmitter to a predetermined threshold signal strength value and to determine a relay attack in the event that the signal strength of the received signal exceeds the predetermined threshold signal strength value.

10

Optionally, the control module comprises an output for outputting a notification signal indicative of a relay attack.

Optionally, the control module is configured to output the notification signal to a key
15 device in the event that a relay attack is determined.

Optionally, the control module is configured to output the notification signal to a cloud based alarm system in the event that a relay attack is determined.

20 According to a yet further aspect of the invention there is provided a passive entry system for a vehicle, the passive entry system comprising: a receiver arranged to receive a passive entry communication signal associated with a transmitter within the vehicle; and a control module according to a further aspect of the present invention.

25 According to a further aspect of the invention there is provided a computer program product comprising instructions which, when the program is executed by a computer or control module, cause the computer to carry out a method according to an aspect of the invention.

30 According to a further aspect of the invention there is provided a computer-readable storage medium comprising instructions which, when executed by a computer or control module, cause the computer to carry out a method according to an aspect of the invention.

Optionally, the computer-readable storage medium comprises a non-transitory computer-readable medium.

According to a further aspect of the invention there is provided a vehicle comprising a
5 passive entry system according to an aspect of the present invention.

According to a further aspect of the invention there is provided a control module for a passive entry system as described above, wherein: a processor for receiving one or more passive entry communication signals comprises an electronic processor having
10 an electrical input for receiving said one or more signals; and an electronic memory device electrically coupled to the electronic processor and having instructions stored therein, wherein the control module is arranged to detect that a relay attack is occurring based on the signal strength of the received passive entry communication signals and the electronic processor is configured to access the memory device and
15 execute the instructions stored therein such that the control module is operable to detect that the vehicle is experiencing a relay attack based on the signal strength of the received passive entry communication signals; and output a notification signal indicative of a relay attack.

20 Within the scope of this application it is expressly intended that the various aspects, embodiments, examples and alternatives set out in the preceding paragraphs, in the claims and/or in the following description and drawings, and in particular the individual features thereof, may be taken independently or in any combination. That is, all embodiments and/or features of any embodiment can be combined in any way and/or
25 combination, unless such features are incompatible. The applicant reserves the right to change any originally filed claim or file any new claim accordingly, including the right to amend any originally filed claim to depend from and/or incorporate any feature of any other claim although not originally claimed in that manner.

30 BRIEF DESCRIPTION OF THE DRAWINGS

One or more embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a representation of a known passive entry system;

Figure 2 is a representation of a Bluetooth LE[®] based passive entry system;

- 5 Figures 3 and 4 are schematic representations of the Bluetooth LE[®] system of Figure 2 in accordance with an embodiment of the present invention; and

Figure 5 is a flow chart illustrating a relay attack detection method in accordance with an embodiment of the present invention.

10

DETAILED DESCRIPTION

Figure 1 shows a known passive entry system between a vehicle 10 and a key fob 12. The vehicle 10 comprises a first low frequency (LF) transmitter 14 which may be located in the engine compartment of the vehicle and a second LF transmitter 16 which may be located in a door handle 18 of the vehicle. It is noted that only two transmitters 14, 16 are shown in Figure 1 for clarity and in certain arrangements each door handle may comprise a transmitter. In other arrangements, the transmitter 14 located in the engine compartment may not be present and the passive entry system may, for example, rely on the door handle based transmitters for operation, although other locations within or on the vehicle are envisaged.

20

The passive entry system further comprises a radio frequency (RF) receiver 20 and a control module 22.

25

The transmitters 14, 16 are arranged to output radio signals at a frequency of 125 kHz. The key fob 12 is configured to receive signals at 125 kHz and transmit signals at a frequency of 433 MHz. The RF receiver 20 is configured to receive signals at a frequency of 433 MHz.

30

It is noted that the above frequency values are provided by way of example only and may vary between different vehicle markets. The low frequency range, for example, is generally taken to encompass the range of 30 kHz to 300 kHz. The radio frequency range is generally taken to encompass the range of 3 kHz to 300 GHz. The RF

frequency described herein is 433 MHz, but other frequencies are envisaged. For example, the system may operate at 315 MHz.

5 In a normal unlock mode of operation, a user in possession of the key fob 12 approaches the vehicle and pulls a door handle 18. A sensor (not shown) in the door handle sends a signal to the control module 22 which arranges for the transmitter 14, 16 to send an LF signal which is received by the key fob 12. In some arrangements, the LF signal is generated in response to detection of the user grasping or otherwise touching the exterior door handle of the vehicle. This physical contact with the user's
10 hand is detected by sensors in the handle arranged to detect a change in capacitance or resistance. In this way, the system can respond more quickly in normal use, but if the handle fails to detect the touch of the user's hand, for example if the user is wearing gloves, then the system will detect when the user pulls on the handle and the system will respond, albeit with some delay, as normal.

15 In response to receiving the LF signal from the vehicle 10, the key fob is arranged to send an unlock request to the vehicle on the RF signal frequency. The RF signal is received by the receiver 20 which sends the received signal to the control unit 22 which then sends a door unlock signal to the doors.

20 In a relay attack, a signal booster 24 may be used to relay the LF signal sent from the transmitters 14, 16 to the key fob 12 when the key fob is located outside a usual passive entry range of operation. The key fob 12 may then receive a communication from the vehicle 10 when it is further away from the vehicle than usual, e.g. inside a
25 house when the car is on the drive or across a car park.

In this relay attack scenario, the key fob 12 may then send an unlock request over the RF frequency. The unlock request is sent by the key fob at a higher power than the LF signals. This means the vehicle 10 will receive the unlock request and the vehicle
30 doors will unlock without necessitating that the unlock request to be similarly boosted. In an alternative scenario, a further signal booster (not shown) may also be used to relay the unlock request from the key fob 12.

Figure 2 shows a Bluetooth low energy (Bluetooth LE®/BLE) passive entry system in which a vehicle 30 comprises a Bluetooth® beacon 32 which is in communication with a smart device 34 (e.g. a smartphone, smartwatch or other suitably Bluetooth® enabled device). As shown, the smart device 34 may display a virtual representation of a key fob 36. For example, the key fob 36 may be part of a computer application on the smart device 34 that has been configured such that the smart device in question is paired with the vehicle.

In vehicle 30, the beacon 32 periodically broadcasts a signal over Bluetooth LE® (~2.4 GHz). When the smart device 34 is in range of the Bluetooth® beacon 32 the computer application on the smart device and a control module 38 associated with the beacon may exchange messages to identify each other and an unlock request may be sent to the vehicle. It is noted that the unlock request may be configured to be sent automatically or via a user interaction with the virtual key fob 36.

A relay attack may however be arranged to operate in a similar manner to Figure 2 in which a signal booster 24 is used to relay signals to and/or from the vehicle 30/smart device 34 when the two are outside their normal range of operation.

Figure 3 shows a Bluetooth LE® enabled passive entry system in accordance with an embodiment of the present invention. In the illustrated embodiment, the vehicle 30 is equipped with a Bluetooth® receiver 40 that is located within the vehicle at a different location to the beacon 32.

The signal strength of the Bluetooth LE® signal associated with the beacon 32 and received at the receiver 40 has a received signal strength indication (RSSI) of -50dBm (+/- 10 dBm) and this value is monitored by the control module 38.

In the event that a signal booster 24 is brought into the vicinity of the vehicle, as shown in Figure 4, the RSSI of the Bluetooth® signal received at the receiver 40 and measured at the control module 38 increases to -25dBm (+/-10dBm). This results from a Bluetooth® signal sent from the beacon 32 being relayed by the signal booster 24 at an increased signal strength.

The control module 38 is arranged to compare the RSSI of the received signal to a threshold value T. In the case of Figure 4 this threshold $T = -40\text{dBm}$. The control module 38 is arranged to determine that a relay attack is in progress in the event the RSSI exceeds the predetermined threshold T.

5

It is noted that the above RSSI signal strengths and the threshold T are provided by way of example only. Different vehicles and vehicle configurations may result in different RSSI values to those shown above and the threshold T may be selected in a given vehicle configuration to any appropriate value that enables a relay attack to be detected.

10

Once a relay attack has been detected the control module 38 may be arranged to output a notification signal to be sent to the smart device 34 and/or to a cloud based security system. The notification signal is indicative of a relay attack. Additionally or alternatively, the vehicle alarm may be triggered.

15

Figure 5 shows a relay attack detection method in accordance with an embodiment of the present invention and in accordance with the vehicle 30 shown in Figures 3 and 4.

20 The receiver 40 receives 100 a Bluetooth® signal associated with the beacon 32. The Bluetooth® signal may be received directly from the beacon 32, or indirectly via an external device, such as a signal booster. In step 102, the control module 38 determines if the RSSI of the received signal exceeds a predetermined threshold T. In the event that the threshold is exceeded, the control module 38 determines 104 that a relay attack is in progress. In step 106, an alert/notification signal may be sent to the smart device 34 and/or the vehicle alarm may be sounded.

25

It is noted that a similar detection method may be used in the vehicle 10 of Figure 1. In Figure 1, the transmitters 14, 16 and receiver 20 operate on different frequencies. Therefore, a further receiver configured to detect LF signals at 125 kHz may be installed in the vehicle. The control module 22 may then be configured to operate the detection method of Figure 5, using a comparison of LF signal strength, additionally or alternatively to a Bluetooth® or Bluetooth LE® signal, in order to detect relay attacks.

30

It is noted that vehicles fitted with an immobiliser may already comprise an LF transceiver for engine start requests that is already be capable of receiving the LF signal from the LF transmitters 14, 16. In such vehicles, the control module 22 may be configured to receive data from the immobiliser transceiver in order to determine if a
5 relay attack is occurring. Advantageously, this employs existing vehicle hardware in a new role to achieve an improved resistance to relay attacks.

Many modifications may be made to the above examples without departing from the scope of the present invention as defined in the accompanying claims.

10

CLAIMS

1. A method of detecting a relay attack on a vehicle equipped with a passive entry system, the method comprising:
 - 5 sending a passive entry communication signal from a transmitter within the vehicle;
 - receiving a passive entry communication signal associated with the transmitter at a receiver within the vehicle;
 - comparing the signal strength of the received passive entry communication
 - 10 signal to a predetermined threshold signal strength value; and
 - determining a relay attack in the event that the signal strength of the received passive entry communication signal exceeds the predetermined threshold signal strength value.
- 15 2. A method as claimed in Claim 1, wherein the comparing step comprises measuring a received signal strength indication, RSSI, of the received signal and comparing the measured RSSI to the threshold signal strength value.
3. A method as claimed in Claim 1 or Claim 2, wherein the passive entry
- 20 communication signal is sent from the transmitter in response to a door unlock request.
4. A method as claimed in Claim 1 or Claim 2, wherein the passive entry communication signal is sent periodically from the transmitter.
- 25 5. A method as claimed in Claim 4, wherein the passive entry communication signal is sent approximately every second.
6. A method as claimed in any preceding claim, wherein the transmitted passive
- 30 entry communication signal comprises a Bluetooth low energy (Bluetooth LE®) signal, the transmitter comprises a Bluetooth® beacon and the receiver comprises a Bluetooth® receiver.

7. A method as claimed in any one of Claims 1 to 5, wherein the transmitted passive entry communication signal comprise a low frequency, LF, signal, the transmitter comprises an LF transmitter and the receiver comprises an LF receiver.
- 5 8. A method as claimed in any preceding claim, comprising immobilising the vehicle in the event that a relay attack is determined.
9. A method as claimed in any preceding claim, comprising sending a notification signal to a key device in the event that a relay attack is determined.
- 10 10. A method as claimed in any preceding claim, comprising sending a notification signal to a cloud based alarm system in the event that a relay attack is determined.
11. A method as claimed in any preceding claim, comprising sounding a vehicle
15 alarm in the event that a relay attack is determined.
12. A method as claimed in any preceding claim, comprising maintaining a vehicle door in a locked state or locking a vehicle door in the event that a relay attack is determined.
- 20 13. A control module for a passive entry system for a vehicle, the control module comprising:
an input arranged to receive data relating to a passive entry communication signal, the passive entry communication signal being sent from a transmitter within the
25 vehicle; and
a processor arranged to compare a signal strength of the received passive entry communication signal associated with the transmitter to a predetermined threshold signal strength value and to determine a relay attack in the event that the signal strength of the received signal exceeds the predetermined threshold signal
30 strength value.
14. A control module as claimed in Claim 13, comprising an output for outputting a notification signal indicative of a relay attack.

15. A control module as claimed in Claim 14, wherein the control module is configured to output the notification signal to a key device in the event that a relay attack is determined.
- 5 16. A control module as claimed in Claim 14 or Claim 15, wherein the control module is configured to output the notification signal to a cloud based alarm system in the event that a relay attack is determined.
- 10 17. A passive entry system for a vehicle, the passive entry system comprising:
a receiver arranged to receive a passive entry communication signal associated with a transmitter within the vehicle; and
a control module as claimed in any of Claims 13 to 16.
- 15 18. A vehicle comprising a control module according to any of Claims 13 to 16, or a passive entry system according to Claim 17.
19. A computer program product comprising instructions which, when the program is executed by a computer, cause the computer to carry out the method of claims 1 to 12.
- 20 20. A computer-readable storage medium comprising instructions which, when executed by a computer, cause the computer to carry out the method of claims 1 to 12; optionally the computer-readable storage medium comprises a non-transitory computer readable medium.

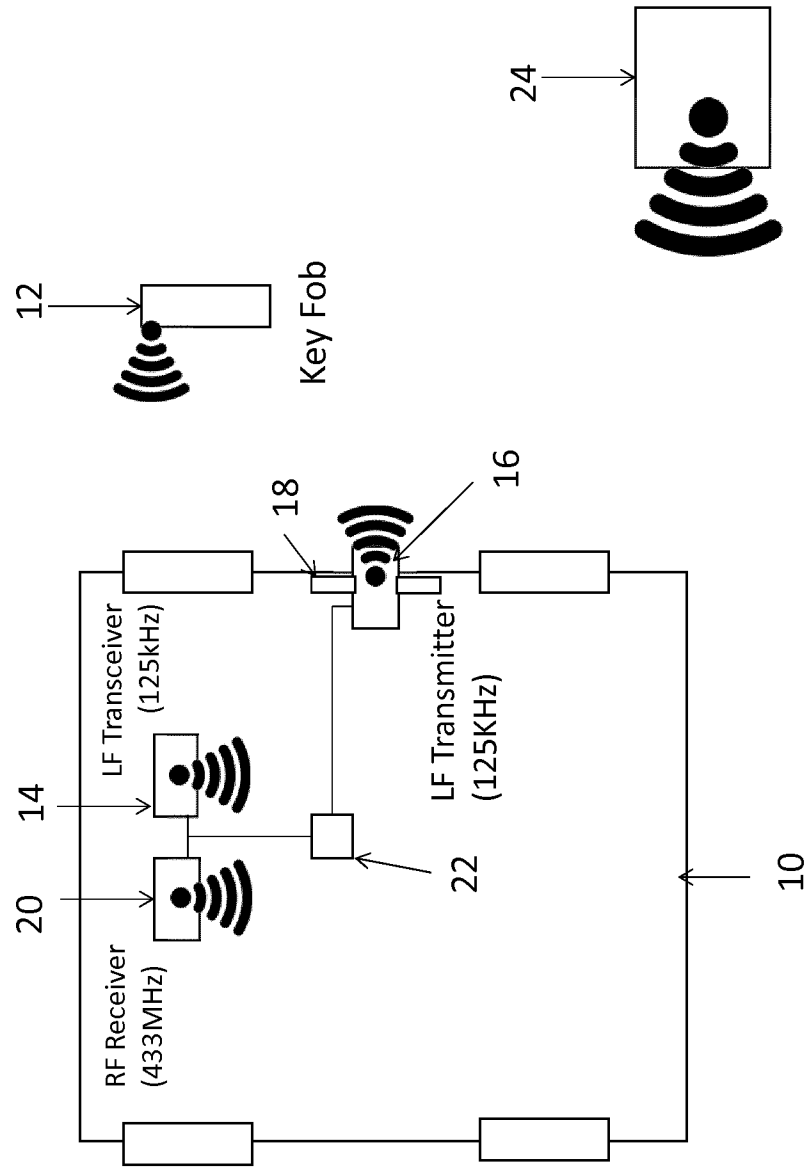


Figure 1

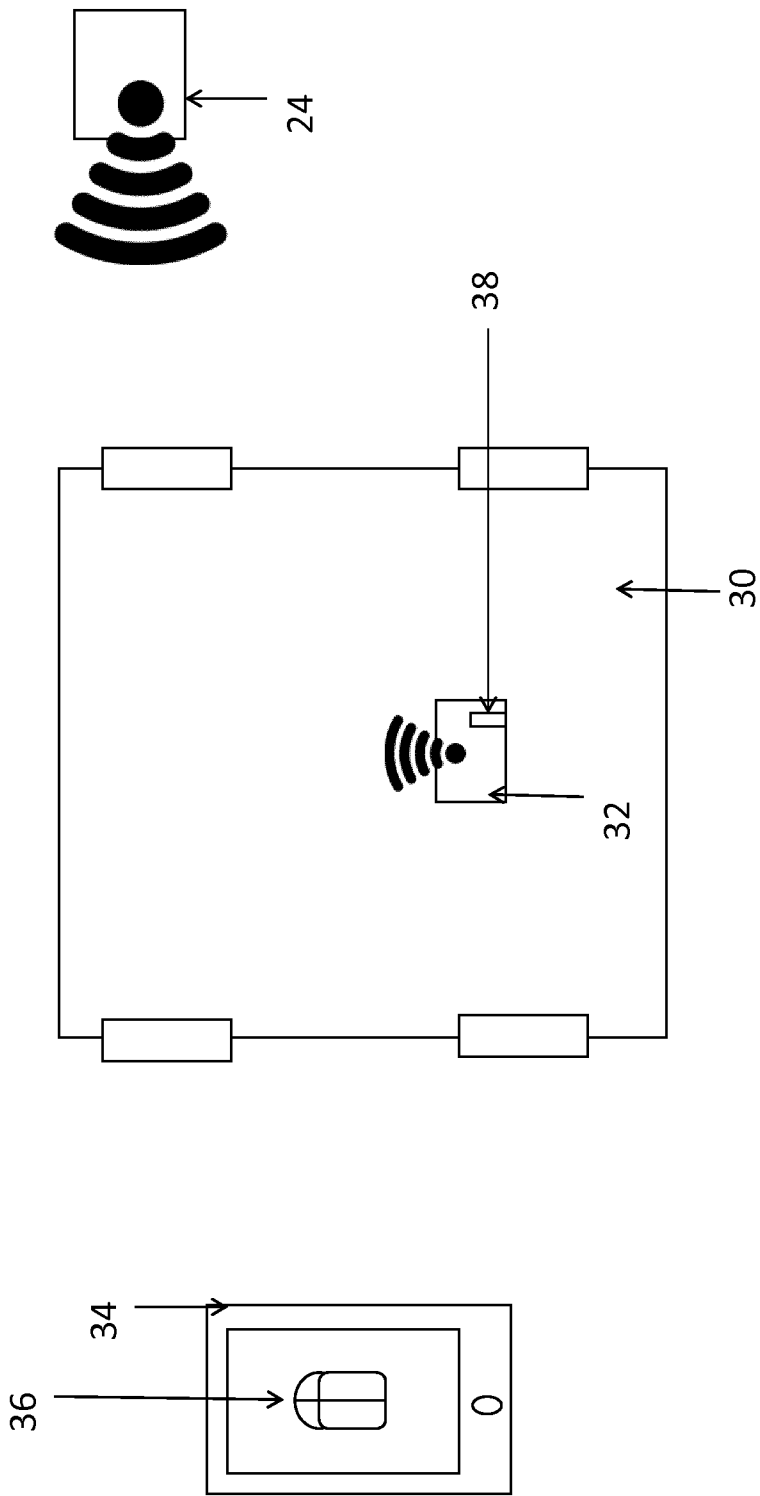


Figure 2

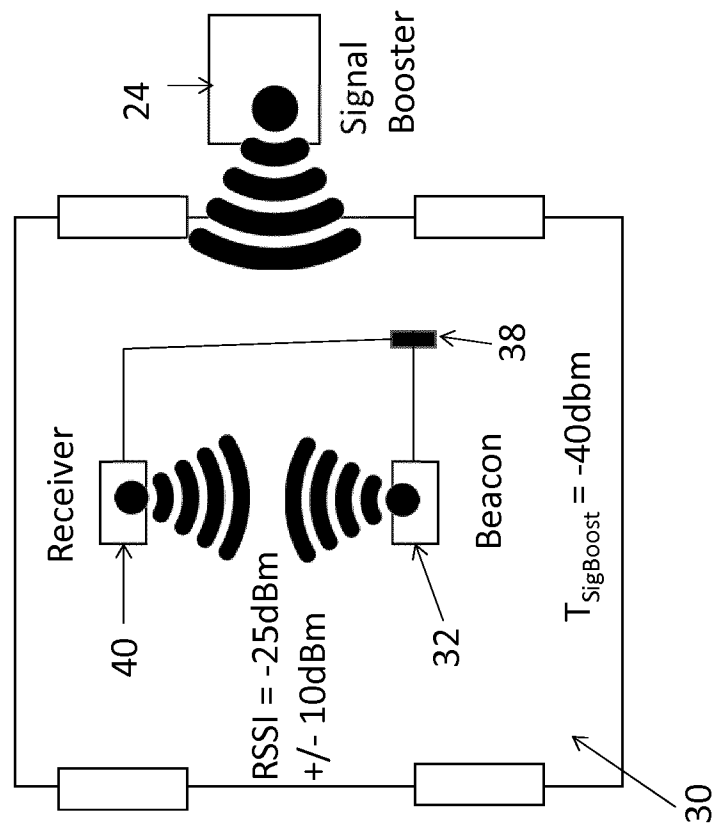


Figure 4

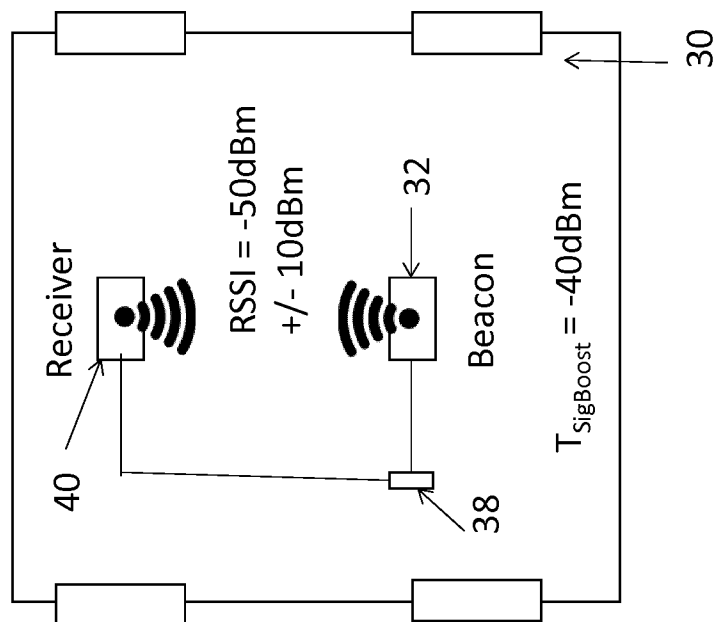


Figure 3

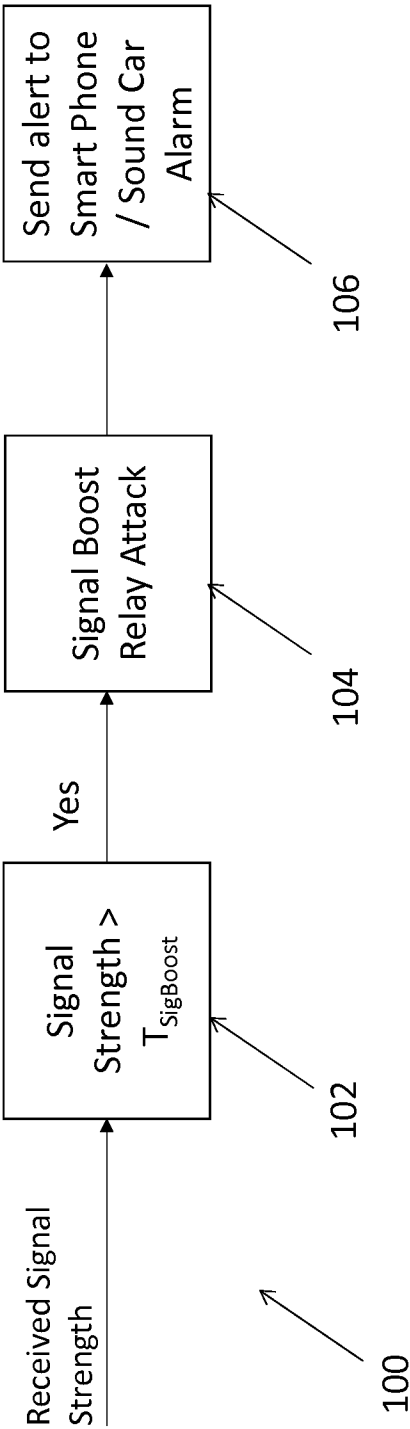


Figure 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/082004

A. CLASSIFICATION OF SUBJECT MATTER
INV. B60R25/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015/302673 A1 (SEIBERTS KLAUS [DE] ET AL) 22 October 2015 (2015-10-22) paragraph [0021] - paragraph [0025] paragraph [0036] -----	1-20
A	US 2012/286927 A1 (HAGL ANDREAS [DE]) 15 November 2012 (2012-11-15) paragraph [0044] paragraph [0016] - paragraph [0018] -----	1-20
A	US 2010/305779 A1 (HASSAN HASIB [US] ET AL) 2 December 2010 (2010-12-02) paragraph [0083] - paragraph [0087] paragraph [0112] - paragraph [0149] -----	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

5 February 2018

Date of mailing of the international search report

12/02/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Standring, Michael

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/082004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015302673 A1	22-10-2015	CN 104240340 A	24-12-2014
		US 2014375420 A1	25-12-2014
		US 2015302673 A1	22-10-2015

US 2012286927 A1	15-11-2012	NONE	

US 2010305779 A1	02-12-2010	NONE	
