Brandon J. Witkow (SBN 210443)
bw@witkowlaw.com
Cory A. Baskin (SBN 240517)
cb@witkowlaw.com
witkow | baskin
21031 Ventura Boulevard, Suite 700
Woodland Hills, California 91364
Tel: 818.296.9508
Fax: 818.296.9510

Attorneys for *Plaintiff*
2BCOM, LLC

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

2BCOM, LLC, a Delaware limited liability company,

Plaintiff,

vs.

KIA MOTORS AMERICA, INC., a California corporation,

Defendant.

Case No. 8:20-cv-00676

COMPLAINT FOR PATENT INFRINGEMENT

JURY TRIAL DEMANDED

witkow | baskin

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff 2BCom, LLC ("Plaintiff" or "2BCom") files this Complaint against Defendant Kia Motors America, Inc. ("Defendant") for patent infringement and by and through its undersigned attorneys, hereby prays to this honorable Court for relief and remedy based on the following:

NATURE OF THE CASE

1. This is an action for patent infringement arising under the patent laws of the United States, 2BCom holds the rights in U.S. Patent Nos. 6,831,444 ("the '444 patent"), 6,928,166 ("the '166 patent"), 7,127,210 ("the '210 patent"), and 7,184,707 ("the '707 patent"). The United States patent laws grant the holder of a patent the right to exclude infringers from making, using, selling or importing the invention claimed in a patent, and to recover damages for the infringer's violations of these rights, and to recover treble damages where the infringer willingly infringed the patent. Under 35 U.S.C. § 282(a), the '444 patent, the '166 patent, the '210 patent, and the '707 patent are entitled to a presumption of validity. 2BCom is suing Defendant for infringing its patent and doing so willfully. 2BCom seeks to recover damages from Defendant, including treble damages for willful infringement.

THE PARTIES

2. 2BCom, LLC is a company, organized and existing under the laws of Delaware, having a place of business at 1603 Orrington Ave, Suite 600, Evanston, Illinois 60201.

3. Upon information and belief, Defendant Kia Motors America, Inc. ("Kia") is a California corporation with a principal place of business at 111 Peters Canyon Road, Irvine, California 92606.

4. Upon information and belief, Defendant manufactures, imports, and/or sells audio and multimedia integration systems which have been installed in Kia branded vehicles, including the Kia Bluetooth system.

witkow | baskin

5. The Kia Bluetooth system is sold in all models of Kia vehicles, including Soul, Seltos, Sportage, Niro, Sorento, Telluride, Rio, Forte, Optima, Stinger, Cadenza, K900, Optima Hybrid, Niro Plug-In Hybrid, Optima Plug-In Hybrid, Niro EV, Rio 5-door, and Sedona ("Accused Products").

JURISDICTION

6. This is an action for patent infringement arising under the patent laws of the United States of America, more specifically under 35 U.S.C. § 100, *et seq.*, including 35 U.S.C. §271. Subject matter jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 and 1338.

7. The Court has personal jurisdiction over Defendant because Defendant, among other things, conducts business in, and avails itself of the laws of the State of California. Upon information and belief, Defendant has a principal place of business in this District. In addition, upon information and belief, Defendant through its own acts and/or through the acts of its affiliated companies (acting as its agents or alter egos) makes, uses, offers to sell, sells (directly or through intermediaries), imports, licenses and/or supplies, in this District and elsewhere in the United States, products, through regular distribution channels, knowing such products would be used, offered for sale and/or sold in this District. Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of California and in this District.

VENUE

8. Venue properly lies within this judicial district and division, pursuant to 28 U.S.C. §§ 1391(b), (c), and (d), and 1400(b).

9. Upon information and belief, Defendant has a principal place of business in this District. Thus, Defendant resides in this District for the purposes of venue and has committed acts of infringement within this judicial District, does business in this District, and maintains a regular and established place of business in this District.

witkow | baskin

INFRINGEMENT OF U.S. PATENT NO. 6,831,444

10. 2BCom incorporates by reference the allegations set forth in the preceding paragraphs.

11. On December 14, 2004, the '444 patent, entitled "External Storage Device And Remaining Battery Amount Notifying Method In The Same," was duly and lawfully issued based upon an application filed by the inventors, Koichi Kobayashi and Kazunari Tanzawa. A true and correct copy of the '444 Patent is attached hereto as **Exhibit 1**.

12. 2BCom is the assignee and the owner of all right, title and interest in and to the '444 patent and has the right to sue and recover damages for infringement thereof.

13. Upon information and belief, Defendant has been and continues to be engaged in making, using, importing, selling and/or offering for sale infringing products, including, but not limited to, the Accused Products in the United States generally, and in the Central District of California specifically. The Accused Products are available for retail purchase through the www.kia.com website, as well as Kia retailers in the United States.

14. Upon information and belief, by acts including, but not limited to use, making, importation, offers to sell, sales and marketing of products that fall within the scope of at least claim 1 of the '444 patent, Defendant has directly infringed literally and/or upon information and belief, equivalently, and is continuing to infringe the '444 patent and is thus liable to 2BCom pursuant to 35 U.S.C. § 271.

15. As a non-limiting example of Defendant's infringement of the '444 patent, set forth in **Exhibit 5**, is a preliminary claim chart showing Defendant's infringement of exemplary claim 1 of the '444 patent by the Kia Bluetooth system.

16. Defendant has indirectly infringed and continues to infringe at least claim 1 of the '444 patent by inducement under 35 U.S.C. § 271(b). Defendant has induced

witkow | baskin

and continues to induce users and retailers of the Accused Products to directly infringe at least claim 1 of the '444 patent.

17. Upon information and belief, Defendant's knowingly induced customers to use its Accused Products, including, for example, by promoting such products online (e.g., www.kia.com) and/or providing customers with instructions and/or manuals for using the Accused Products through websites such as https://www.kia.com. Likewise, Defendant knowingly induced retailers to market and sell the Accused Products.

18. Defendant has been on notice of the '444 patent and Defendant's respective infringement of the '444 patent, since, at least, January 27, 2020 via letter sent to Mr. Yoon notifying of the patent and infringement.

19. Defendant's infringement of the '444 patent is without consent of, authority of, or license from 2BCom.

20. Upon information and belief, Defendant's infringement of the '444 patent is willful. This action, therefore, is "exceptional" within the meaning of 35 U.S.C. § 285 entitling 2BCom to its attorneys' fees and expenses.

21. As a result of Defendant's acts of infringement, 2BCom has suffered and will continue to suffer damages in an amount to be proven at trial.

INFRINGEMENT OF U.S. PATENT NO. 6,928,166

22. 2BCom incorporates by reference the allegations set forth in the preceding paragraphs.

23. On August 9, 2005 the '166 patent, entitled "Radio Communication Device And User Authentication Method For Use Therewith," was duly and lawfully issued based upon an application filed by the inventor Junichi Yoshizawa. A true and correct copy of the '166 Patent is attached hereto as Exhibit 2.

24. 2BCom is the assignee and the owner of all right, title and interest in and to the '166 patent and has the right to sue and recover damages for infringement thereof.

witkow | baskin

25. Upon information and belief, Defendant has been and continues to be engaged in making, using, importing, selling and/or offering for sale infringing products, including, but not limited to, the Accused Products in the United States generally, and in the Central District of California specifically. The Accused Products are available for retail purchase through the www.kia.com website, as well as Kia retailers in the United States.

26. Upon information and belief, by acts including, but not limited to use, making, importation, offers to sell, sales and marketing of products that fall within the scope of at least claim 1 of the '166 patent, Defendant has directly infringed literally and/or upon information and belief, equivalently, and is continuing to infringe the '166 patent and is thus liable to 2BCom pursuant to 35 U.S.C. § 271.

27. As a non-limiting example of Defendant's infringement of the '166 patent, set forth in **Exhibit 6**, is a preliminary claim chart showing Defendant's infringement of exemplary claim 1 of the '166 patent by the Kia Bluetooth system.

28. Defendant has indirectly infringed and continues to infringe at least claim 1 of the '166 patent by inducement under 35 U.S.C. 271(b). Defendant has induced and continues to induce users and retailers of the Accused Products to directly infringe at least claim 1 of the '166 patent.

29. Upon information and belief, Defendant knowingly induced customers to use its Accused Products, including, for example, by promoting such products online (e.g., www.kia.com) and/or providing customers with instructions and/or manuals for using the Accused Products through websites such as https://www.kia.com. Likewise, Defendant knowingly induced retailers to market and sell the Accused Products.

30. Defendant has been on notice of the '166 patent and Defendant's respective infringement of the '166 patent, since, at least, January 27, 2020 via letter sent to Mr. Yoon notifying of the patent and infringement.

31. Defendant's infringement of the '166 patent is without consent of, authority of, or license from 2BCom.

witkow | baskin

32. Upon information and belief, Defendant's infringement of the '166 patent is willful. This action, therefore, is "exceptional" within the meaning of 35 U.S.C. § 285 entitling 2BCom to its attorneys' fees and expenses.

33. As a result of Defendant's acts of infringement, 2BCom has suffered and will continue to suffer damages in an amount to be proven at trial.

INFRINGEMENT OF U.S. PATENT NO. 7,127,210

34. 2BCom incorporates by reference the allegations set forth in the preceding paragraphs.

35. On October 24, 2006 the '210 patent, entitled "Wireless Communication Apparatus," was duly and lawfully issued based upon an application filed by the inventor Kazunori Aoyagi. A true and correct copy of the '210 Patent is attached hereto as **Exhibit 3**.

36. 2BCom is the assignee and the owner of all right, title and interest in and to the '210 patent and has the right to sue and recover damages for infringement thereof.

37. Upon information and belief, Defendant has been and continues to be engaged in making, using, importing, selling and/or offering for sale infringing products, including, but not limited to, the Accused Products in the United States generally, and in the Central District of California specifically. The Accused Products are available for retail purchase through the www.kia.com website, as well as Kia retailers in the United States.

38. Upon information and belief, by acts including, but not limited to use, making, importation, offers to sell, sales and marketing of products that fall within the scope of at least claim 20 of the '210 patent, Defendant has directly infringed literally and/or upon information and belief, equivalently, and are continuing to infringe the '210 patent and are thus liable to 2BCom pursuant to 35 U.S.C. § 271.

witkow | baskin

39. As a non-limiting example of Defendant's infringement of the '210 patent, set forth in **Exhibit 7**, is a preliminary claim chart showing Defendant's infringement of exemplary claim 20 of the '210 patent by the Kia Bluetooth system.

40. Defendant has indirectly infringed and continues to infringe at least claim 20 of the '210 patent by inducement under 35 U.S.C. 271(b). Defendant has induced and continues to induce users and retailers of the Accused Products to directly infringe at least claim 20 of the '210 patent.

41. Upon information and belief, Defendant knowingly induced customers to use its Accused Products, including, for example, by promoting such products online (e.g., www.kia.com) and/or providing customers with instructions and/or manuals for using the Accused Products through websites such as https://www.kia.com. Likewise, Defendant knowingly induced retailers to market and sell the Accused Products.

42. Defendant has been on notice of the '210 patent and defendant's respective infringement of the '210 patent, since, at least, January 27, 2020 via letter sent to Mr. Yoon notifying of the patent and infringement.

43. Defendant's infringement of the '210 patent is without consent of, authority of, or license from 2BCom.

44. Upon information and belief, Defendant's infringement of the '210 patent is willful. This action, therefore, is "exceptional" within the meaning of 35 U.S.C. § 285 entitling 2BCom to its attorneys' fees and expenses.

45. As a result of Defendant's acts of infringement, 2BCom has suffered and will continue to suffer damages in an amount to be proven at trial.

INFRINGEMENT OF U.S. PATENT NO. 7,184,707

46. 2BCom incorporates by reference the allegations set forth in the preceding paragraphs.

47. On February 27, 2007 the '707 patent, entitled "Communication Device And A Method For Controlling The Communication Device," was duly and lawfully issued based upon an application filed by the inventors, Masahiro Tada, Ikuo Sako,

witkow | baskin

and Koichi Yata. A true and correct copy of the '707 Patent is attached hereto as **Exhibit 4**.

48. 2BCom is the assignee and the owner of all right, title and interest in and to the '707 patent and has the right to sue and recover damages for infringement thereof.

49. Upon information and belief, Defendant has been and continues to be engaged in making, using, importing, selling and/or offering for sale infringing products, including, but not limited to, the Accused Products in the United States generally, and in the Central District of California specifically. The Accused Products are available for retail purchase through the www.kia.com website, as well as Kia retailers in the United States.

50. Upon information and belief, by acts including, but not limited to use, making, importation, offers to sell, sales and marketing of products that fall within the scope of at least claim 1 of the '707 patent, Defendant has directly infringed literally and/or upon information and belief, equivalently, and are continuing to infringe the '707 patent and are thus liable to 2BCom pursuant to 35 U.S.C. § 271.

51. As a non-limiting example of Defendant's infringement of the '707 patent, set forth in **Exhibit 8**, is a preliminary claim chart showing Defendant's infringement of exemplary claim 1 of the '707 patent by the Kia Bluetooth system.

52. Defendant has indirectly infringed and continues to infringe at least claim 1 of the '707 patent by inducement under 35 U.S.C. § 271(b). Defendant has induced and continues to induce users and retailers of the Accused Products to directly infringe at least claim 1 of the '707 patent.

53. Upon information and belief, Defendants knowingly induced customers to use its Accused Products, including, for example, by promoting such products online (e.g., www.kia.com) and/or providing customers with instructions and/or manuals for using the Accused Products through websites such as

witkow | baskin

https://www.Kia.com. Likewise, Defendants knowingly induced retailers to market and sell the Accused Products.

54. Defendant has been on notice of the '707 patent and defendant's respective infringement of the '707 patent, since, at least, January 27, 2020 via letter sent to Mr. Yoon notifying of the patent and infringement.

55. Defendant's infringement of the '707 patent is without consent of, authority of, or license from 2BCom.

56. Upon information and belief, Defendant's infringement of the '707 patent is willful. This action, therefore, is "exceptional" within the meaning of 35 U.S.C. § 285 entitling 2BCom to its attorneys' fees and expenses.

57. As a result of Defendant's acts of infringement, 2BCom has suffered and will continue to suffer damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, 2BCom requests this Court enter judgment as follows:

A. That the '444 patent, '166 patent, '210 patent, and the'707 patents are valid and enforceable;

B. That Defendant has directly and indirectly infringed at least claim 1 of the '444 patent, at least claim 1 of the '166 patent, at least claim 20 of the '210 patent, and at least claim 1 of the '707 patent,;

C. That such infringement is willful;

D. That Defendant account for and pay to 2BCom all damages pursuant to 35 U.S.C. § 284 to adequately compensate 2BCom for Defendant's infringement of the '444 patent, '166 patent, '210 patent, and the '707 patent, , but in no event less than a reasonable royalty for the use made by Defendant of the invention set forth in the '444 patent, '166 patent, '210 patent, and the '707 patent;

E. That 2BCom receives enhanced damages, in the form of treble damages, pursuant to 35 U.S.C. § 284;

F. That this is an exceptional case under 35 U.S.C. § 285;

witkow | baskin

G. That Defendant pay 2BCom all of 2BCom's reasonable attorneys' fees and expenses pursuant to 35 U.S.C. § 285;

H. That 2BCom be granted pre-judgment and post-judgment interest in accordance with 35 U.S.C. § 284 on the damages caused to it by reason of Defendant's infringement of the '444 patent, '166 patent, '210 patent, and the '707 patent, including pre-judgment and post-judgment interest on any enhanced damages or attorneys' fees award;

I. That costs be awarded in accordance with 35 U.S.C. § 284 to 2BCom; and

J. That 2BCom be granted such other and further relief as the Court may deem just and proper under the circumstances.

DEMAND FOR JURY TRIAL

2BCom hereby demands a trial by jury on all issues so triable in this action.

Dated: April 7, 2020

witkow | baskin

By: /s/ Brandon J. Witkow
Brandon J. Witkow
Cory A. Baskin

Attorneys for *Plaintiff* 2BCOM, LLC.

witkow | baskin

EXHIBIT 1

US006831444B2

(12) **United States Patent**
Kobayashi et al.

(10) **Patent No.: US 6,831,444 B2**
(45) **Date of Patent: Dec. 14, 2004**

(54) **EXTERNAL STORAGE DEVICE, AND REMAINING BATTERY AMOUNT NOTIFYING METHOD IN THE SAME**

(75) Inventors: **Koichi Kobayashi**, Tachikawa (JP); **Kazunari Tanzawa**, Nishitokyo (JP)

(73) Assignee: **Kabushiki Kaisha Toshiba**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **10/235,914**

(22) Filed: **Sep. 6, 2002**

(65) **Prior Publication Data**

US 2003/0141849 A1 Jul. 31, 2003

(30) **Foreign Application Priority Data**

Jan. 30, 2002 (JP) 2002-022316

(51) **Int. Cl.**[7] **H02J 7/00**
(52) **U.S. Cl.** **320/136**
(58) **Field of Search** 320/136, 132, 320/107, 112, 113, 114, 115; 340/636, 988, 995, 457.4; 701/213

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,608,324 A * 3/1997 Yoshida 324/426
6,005,367 A * 12/1999 Rohde 320/106
6,173,350 B1 * 1/2001 Hudson et al. 710/100
6,323,775 B1 * 11/2001 Hansson 340/636
6,385,721 B1 * 5/2002 Puckette 713/2

FOREIGN PATENT DOCUMENTS

JP 2000-32320 1/2000

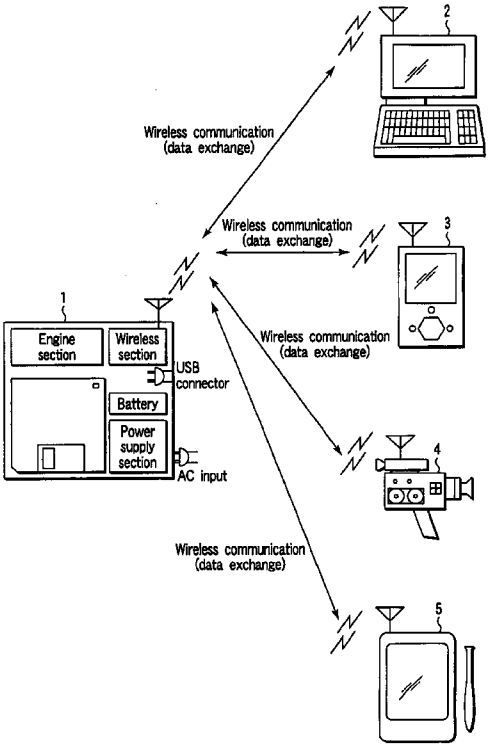
* cited by examiner

Primary Examiner—Pia Tibbits
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett, & Dunner, L.L.P.

(57) **ABSTRACT**

This invention relates to a portable external storage device including a battery which supplies power to a communication section which communicates with a plurality of information processing apparatuses, a detection unit which detects a remaining amount of the battery, a storage unit which stores setting information representing a notifying method for information about a remaining amount of the battery transmitted from the information processing apparatus serving as a host device, and a remaining amount of the battery at which a warning is generated, and a notifying unit which notifies the host device of information about the remaining amount of the battery detected by the detection unit on the basis of the setting information stored in the storage unit.

9 Claims, 15 Drawing Sheets



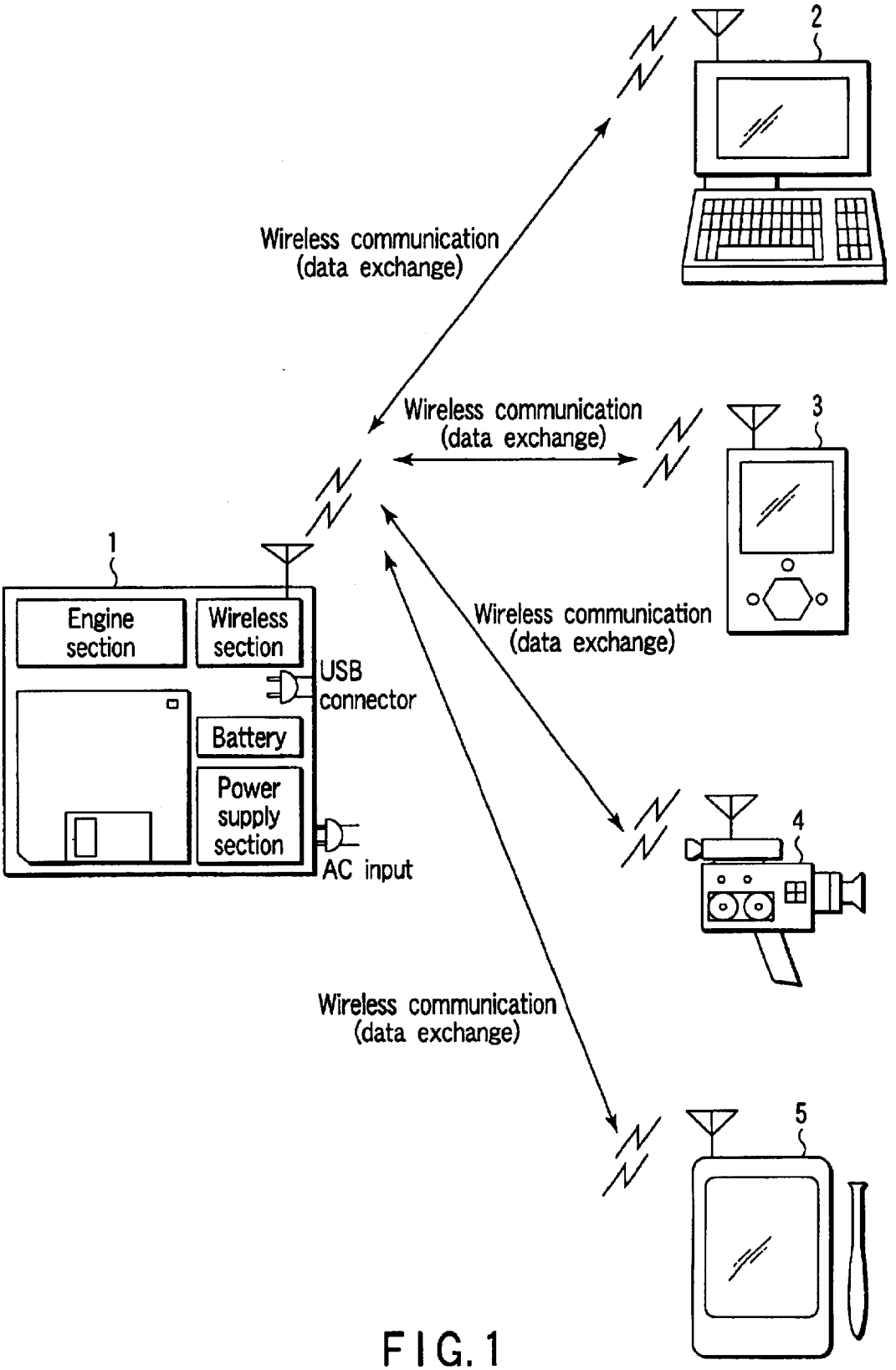

2
Wireless communication
(data exchange)
Wireless communication
(data exchange)
3
1
Engine section
Wireless section
USB connector
Battery
Power supply section
AC input
Wireless communication
(data exchange)
4
Wireless communication
(data exchange)
5

FIG. 1

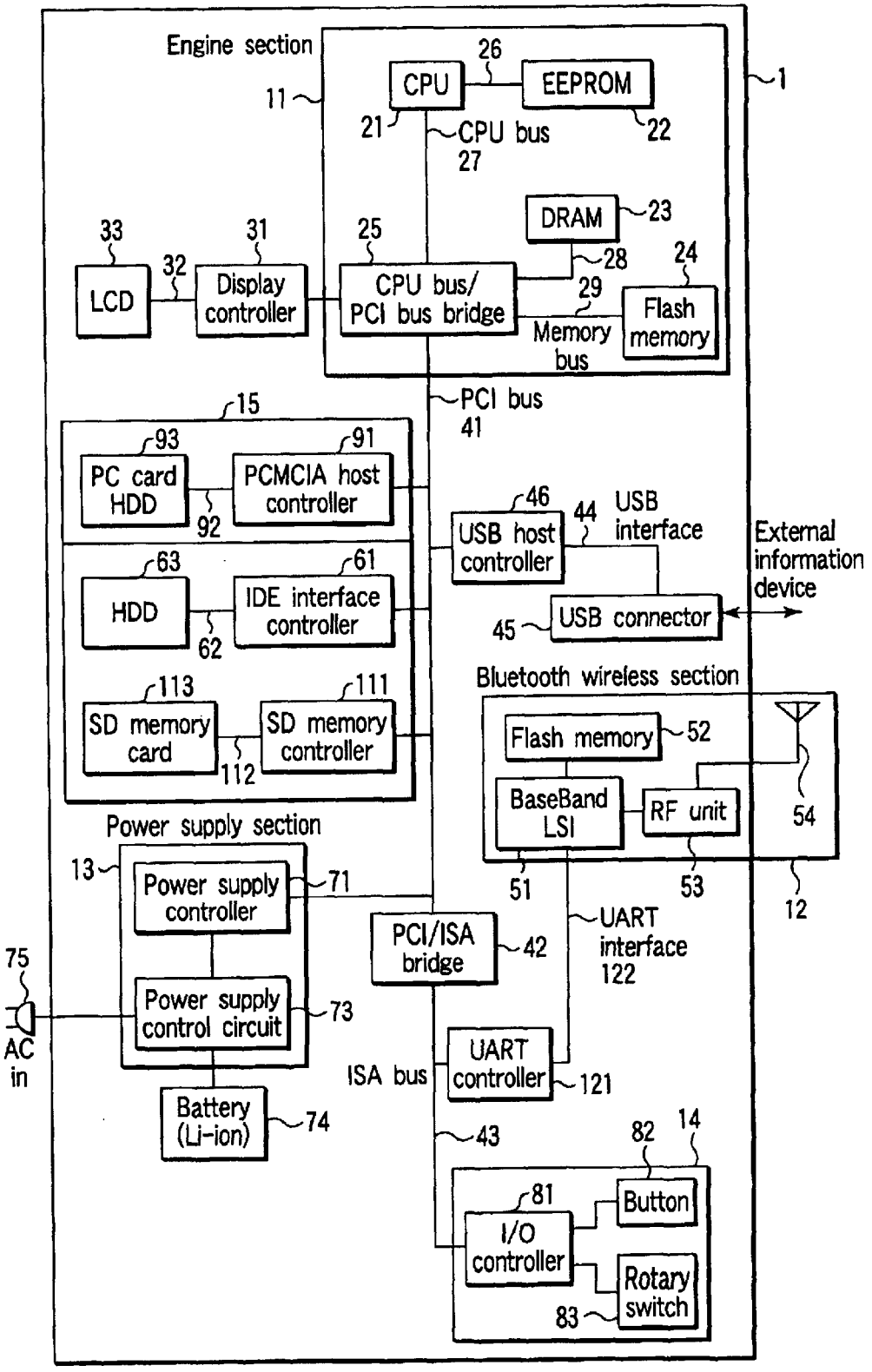

Engine section
11
CPU
26
EEPROM
22
21
CPU bus
27
1
DRAM
23
33
31
25
28
24
32
LCD
Display controller
CPU bus/ PCI bus bridge
29
Memory bus
Flash memory
PCI bus
41
15
93
91
PC card HDD
92
PCMCIA host controller
46
44
USB interface
USB host controller
External information device
63
61
HDD
62
IDE interface controller
45
USB connector
Bluetooth wireless section
113
111
SD memory card
112
SD memory controller
Flash memory
52
BaseBand LSI
RF unit
54
Power supply section
13
Power supply controller
71
51
53
12
PCI/ISA bridge
42
UART interface
122
75
AC in
Power supply control circuit
73
ISA bus
UART controller
121
Battery (Li-ion)
74
43
82
14
81
Button
I/O controller
Rotary switch
83

FIG. 2

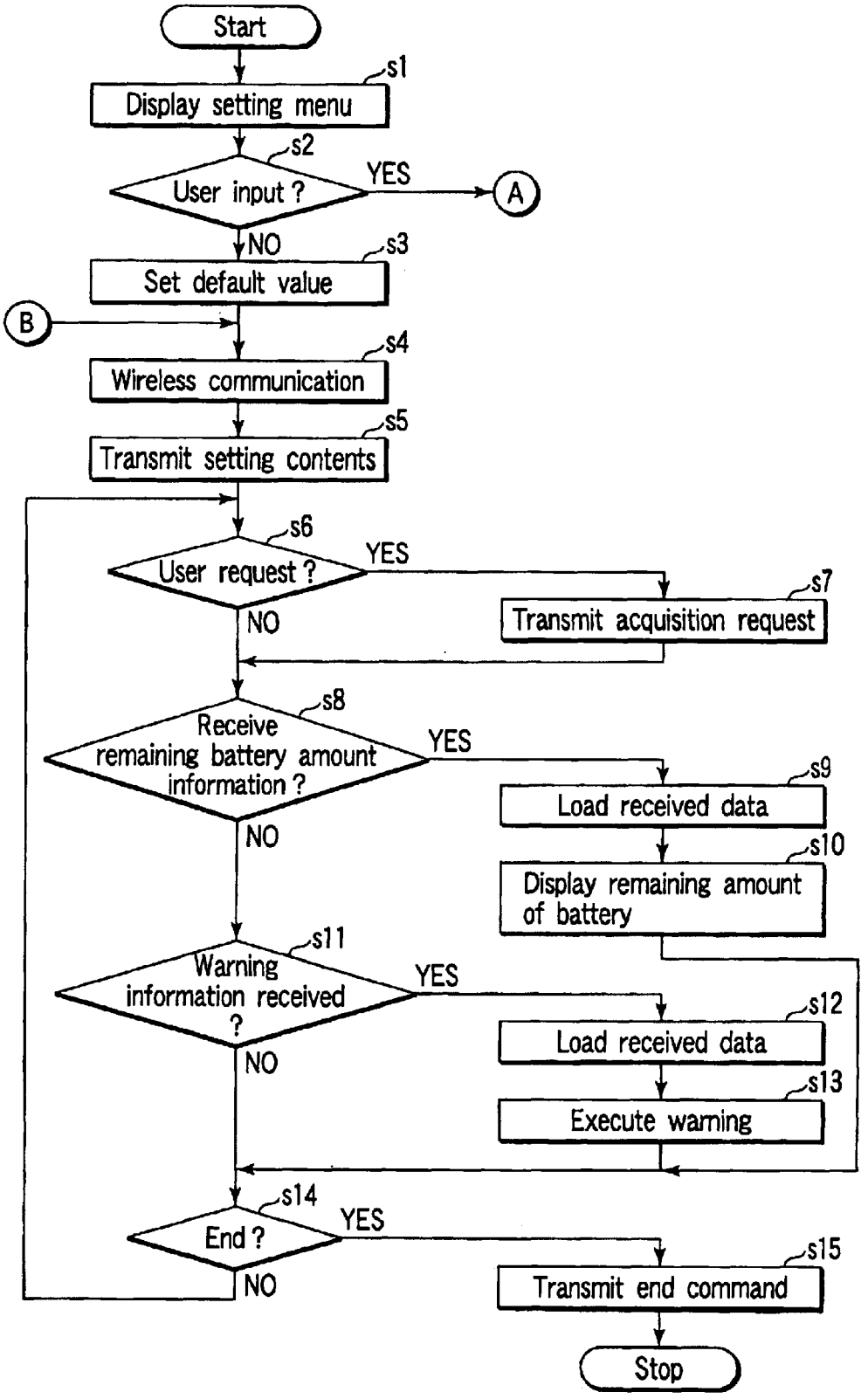

Start
s1
Display setting menu
s2
User input ?
YES
A
NO
s3
Set default value
B
s4
Wireless communication
s5
Transmit setting contents
s6
User request ?
YES
s7
Transmit acquisition request
NO
s8
Receive remaining battery amount information ?
YES
s9
Load received data
s10
Display remaining amount of battery
NO
s11
Warning information received ?
YES
s12
Load received data
s13
Execute warning
NO
s14
End ?
YES
s15
Transmit end command
NO
Stop

FIG. 3

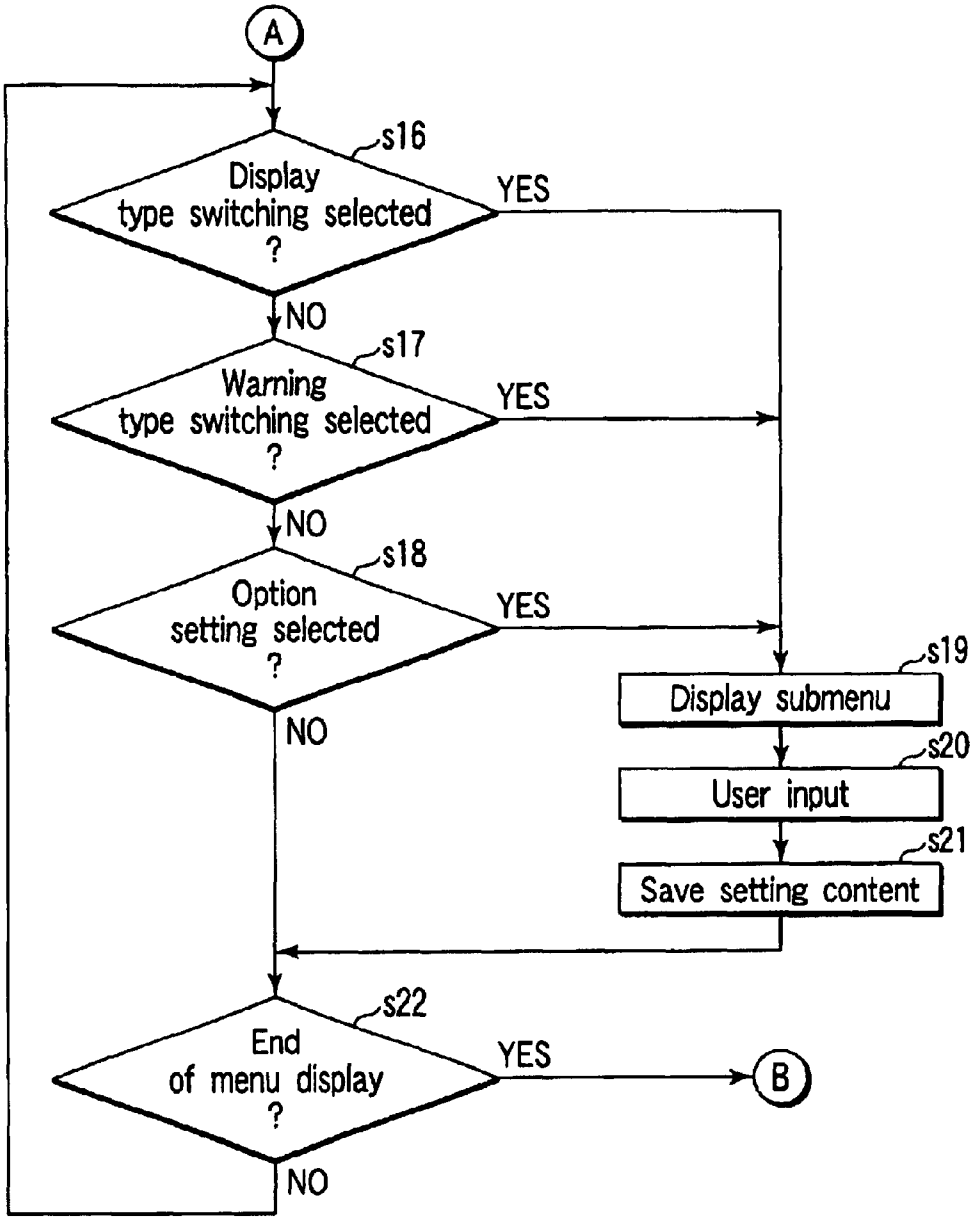

A
s16
Display type switching selected ?
YES
NO
s17
Warning type switching selected ?
YES
NO
s18
Option setting selected ?
YES
NO
s19
Display submenu
s20
User input
s21
Save setting content
s22
End of menu display ?
YES
B
NO

FIG. 4

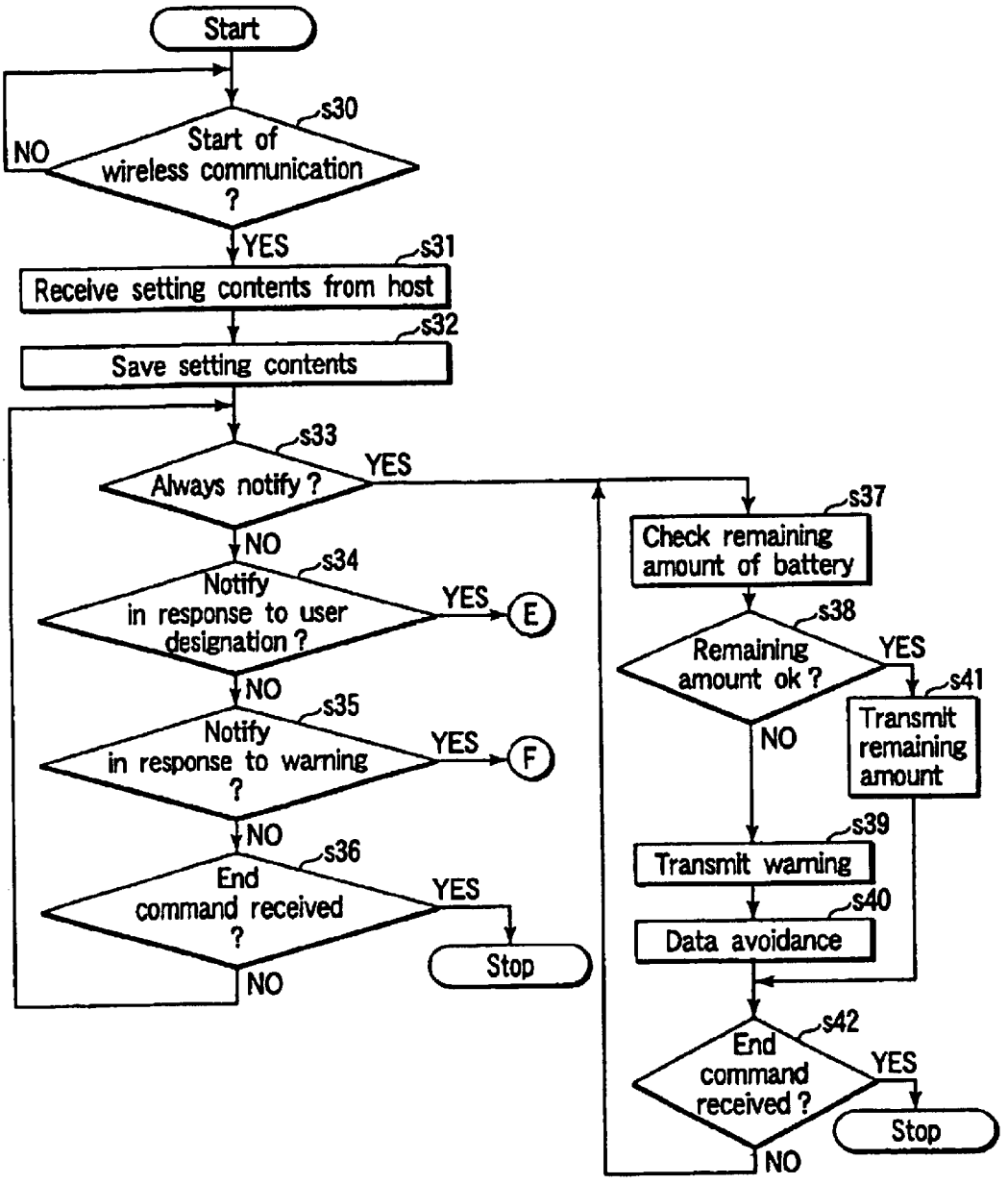

Start
s30
Start of wireless communication ?
NO
YES
s31
Receive setting contents from host
s32
Save setting contents
s33
Always notify ?
YES
NO
s34
Notify in response to user designation ?
YES
E
NO
s35
Notify in response to warning ?
YES
F
NO
s36
End command received ?
YES
Stop
NO
s37
Check remaining amount of battery
s38
Remaining amount ok ?
YES
s41
Transmit remaining amount
NO
s39
Transmit warning
s40
Data avoidance
s42
End command received ?
YES
Stop
NO

FIG. 5

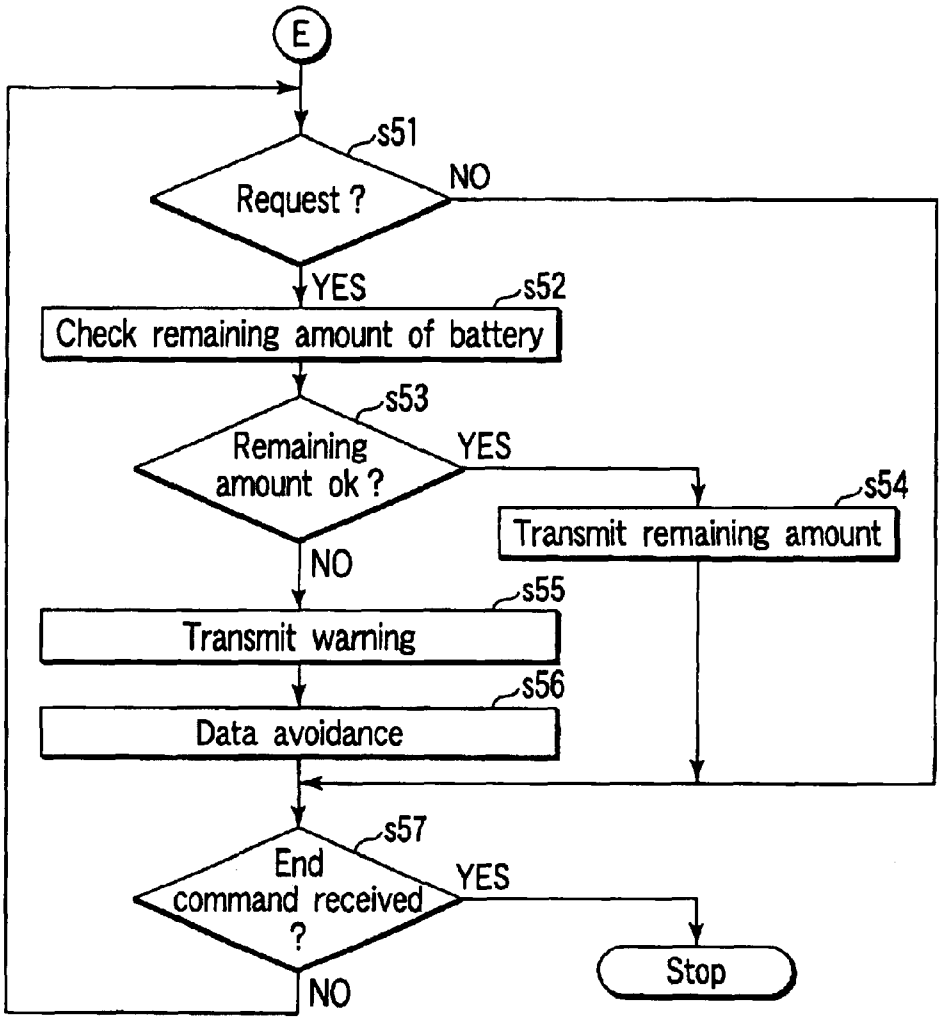

E
s51
Request ?
NO
YES
s52
Check remaining amount of battery
s53
Remaining amount ok ?
YES
s54
Transmit remaining amount
NO
s55
Transmit warning
s56
Data avoidance
s57
End command received ?
YES
Stop
NO

FIG. 6

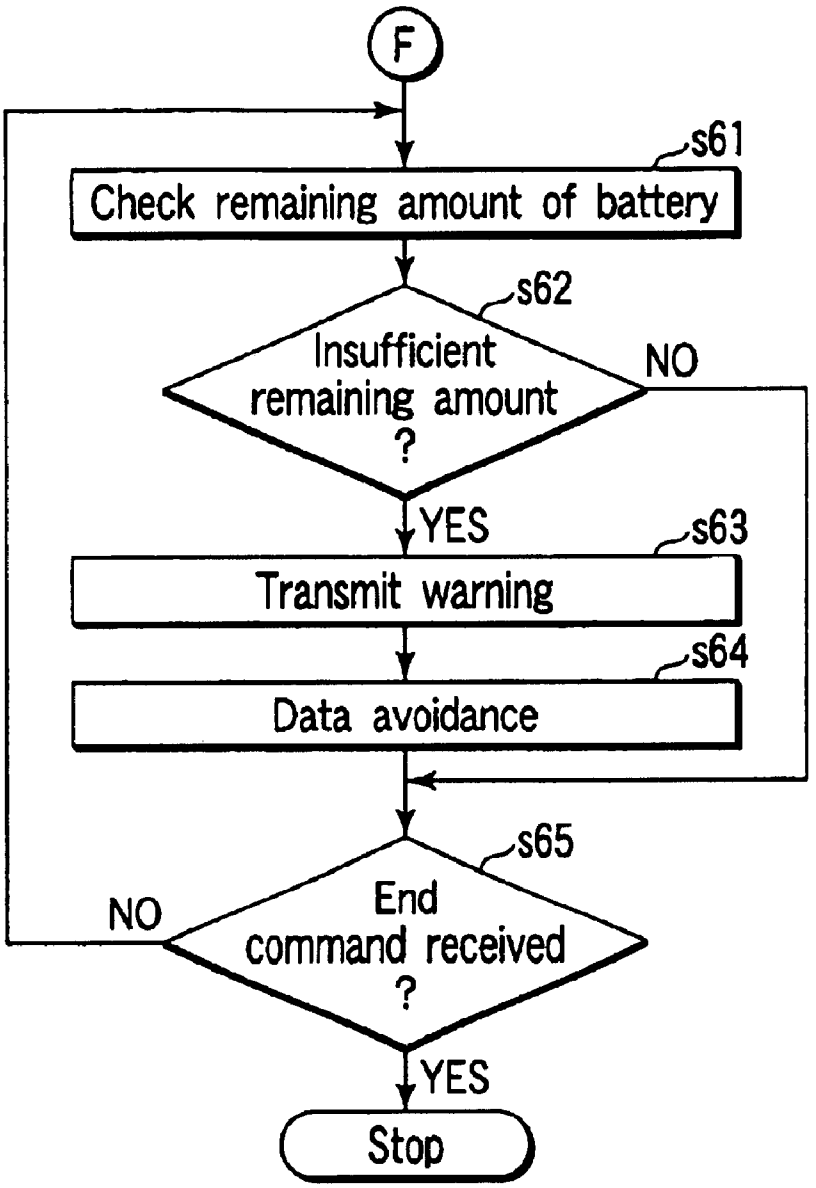

F
s61
Check remaining amount of battery
s62
Insufficient remaining amount ?
NO
YES
s63
Transmit warning
s64
Data avoidance
s65
End command received ?
NO
YES
Stop

FIG. 7

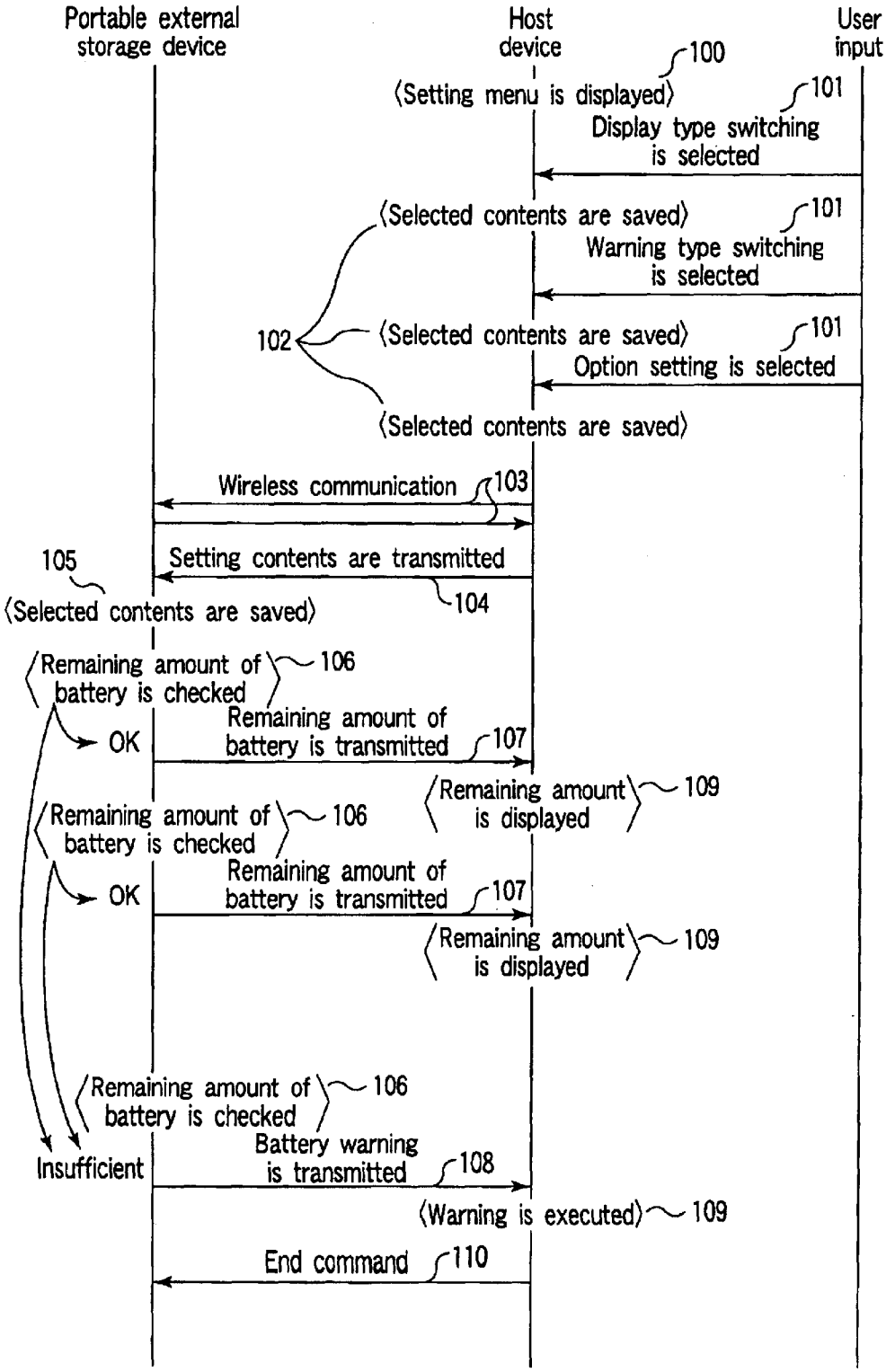

Portable external storage device
Host device
User input
100
⟨Setting menu is displayed⟩
101
Display type switching is selected
⟨Selected contents are saved⟩
101
Warning type switching is selected
102
⟨Selected contents are saved⟩
101
Option setting is selected
⟨Selected contents are saved⟩
Wireless communication
103
105
Setting contents are transmitted
104
⟨Selected contents are saved⟩
⟨Remaining amount of battery is checked⟩
106
OK
Remaining amount of battery is transmitted
107
⟨Remaining amount is displayed⟩
109
⟨Remaining amount of battery is checked⟩
106
OK
Remaining amount of battery is transmitted
107
⟨Remaining amount is displayed⟩
109
⟨Remaining amount of battery is checked⟩
106
Insufficient
Battery warning is transmitted
108
⟨Warning is executed⟩
109
End command
110

FIG. 8

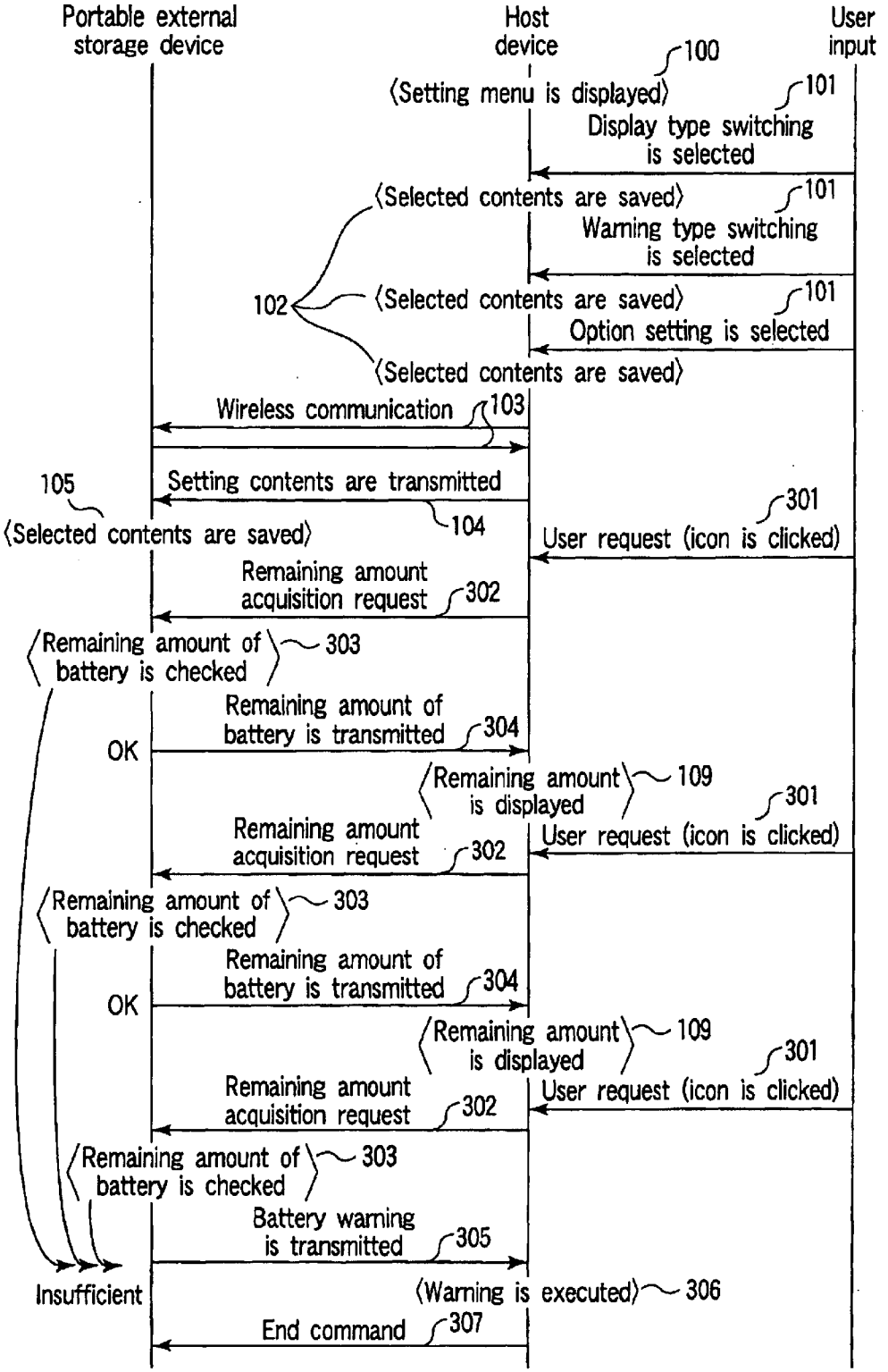

Portable external storage device
Host device
User input
100
〈Setting menu is displayed〉
101
Display type switching is selected
〈Selected contents are saved〉
101
Warning type switching is selected
102
〈Selected contents are saved〉
101
Option setting is selected
〈Selected contents are saved〉
Wireless communication
103
105
Setting contents are transmitted
104
〈Selected contents are saved〉
301
User request (icon is clicked)
Remaining amount acquisition request
302
〈Remaining amount of battery is checked〉
303
Remaining amount of battery is transmitted
304
OK
〈Remaining amount is displayed〉
109
301
Remaining amount acquisition request
302
User request (icon is clicked)
〈Remaining amount of battery is checked〉
303
Remaining amount of battery is transmitted
304
OK
〈Remaining amount is displayed〉
109
301
Remaining amount acquisition request
302
User request (icon is clicked)
〈Remaining amount of battery is checked〉
303
Battery warning is transmitted
305
Insufficient
〈Warning is executed〉
306
End command
307

FIG. 9

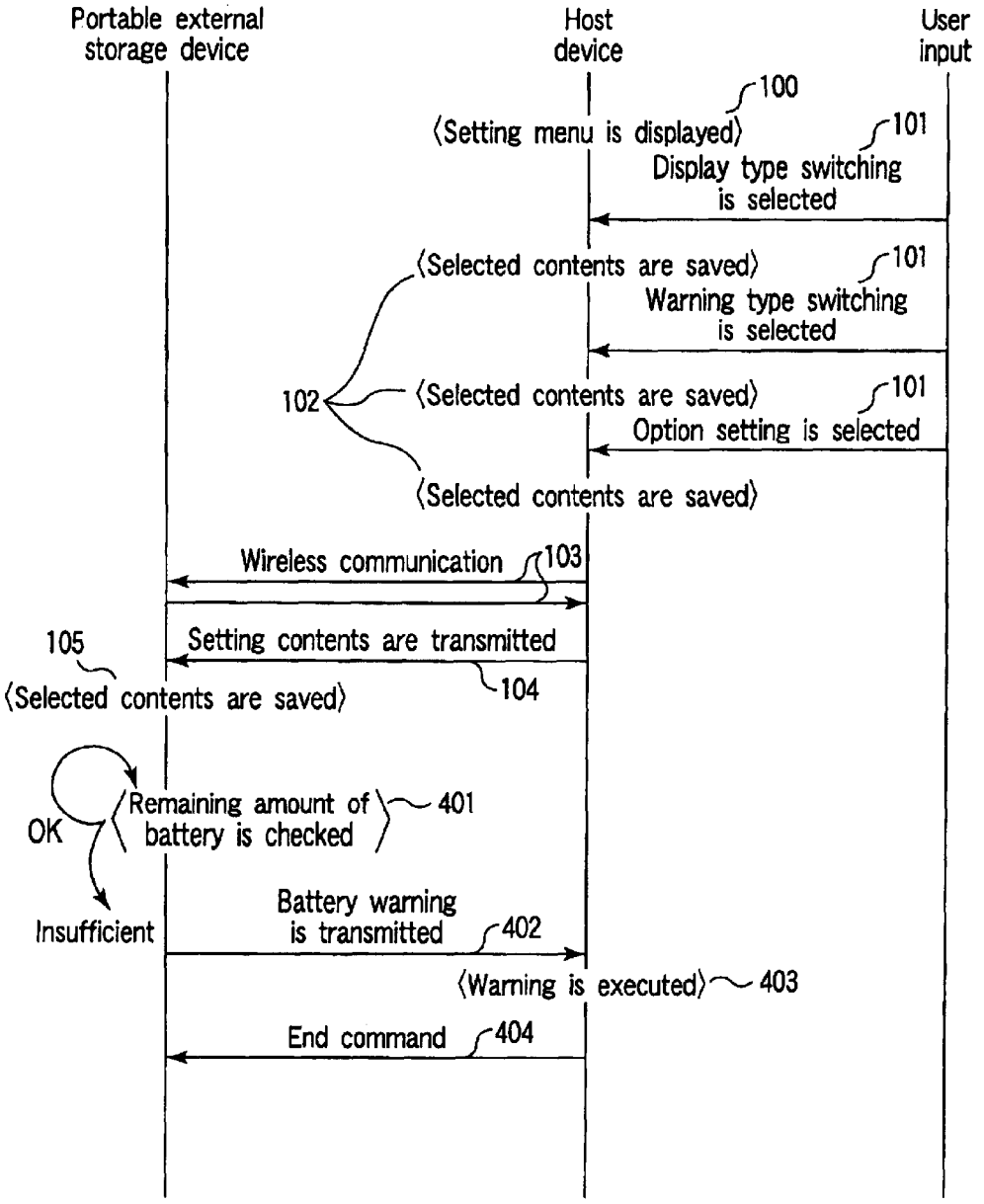

Portable external storage device
Host device
User input
100
〈Setting menu is displayed〉
101
Display type switching is selected
〈Selected contents are saved〉
101
Warning type switching is selected
102
〈Selected contents are saved〉
101
Option setting is selected
〈Selected contents are saved〉
Wireless communication
103
Setting contents are transmitted
104
105
〈Selected contents are saved〉
Remaining amount of battery is checked
401
OK
Insufficient
Battery warning is transmitted
402
〈Warning is executed〉
403
End command
404

FIG. 10

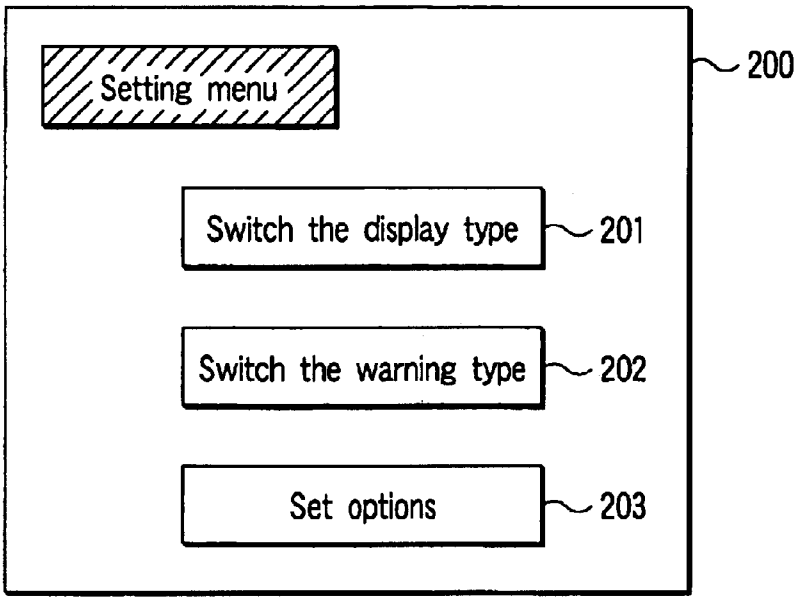

Setting menu
200
Switch the display type
201
Switch the warning type
202
Set options
203

FIG. 11

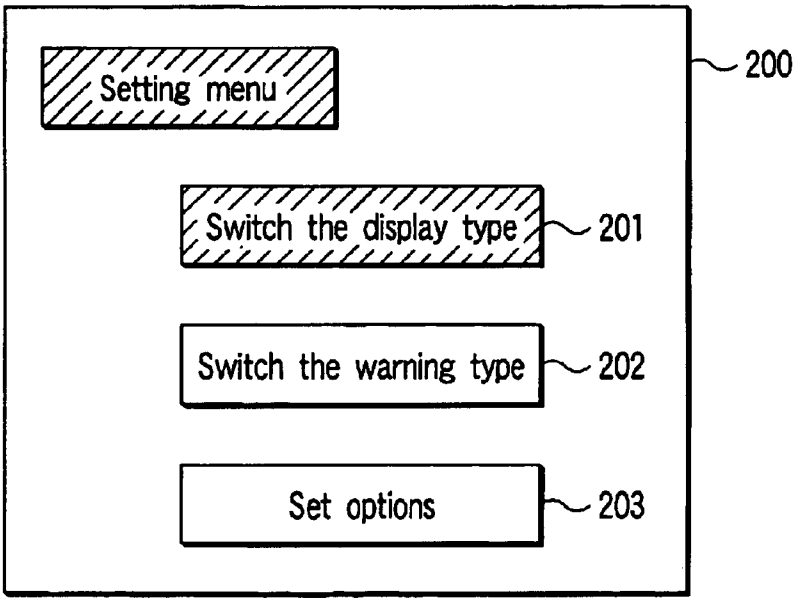

Setting menu
200
Switch the display type
201
Switch the warning type
202
Set options
203

FIG. 12

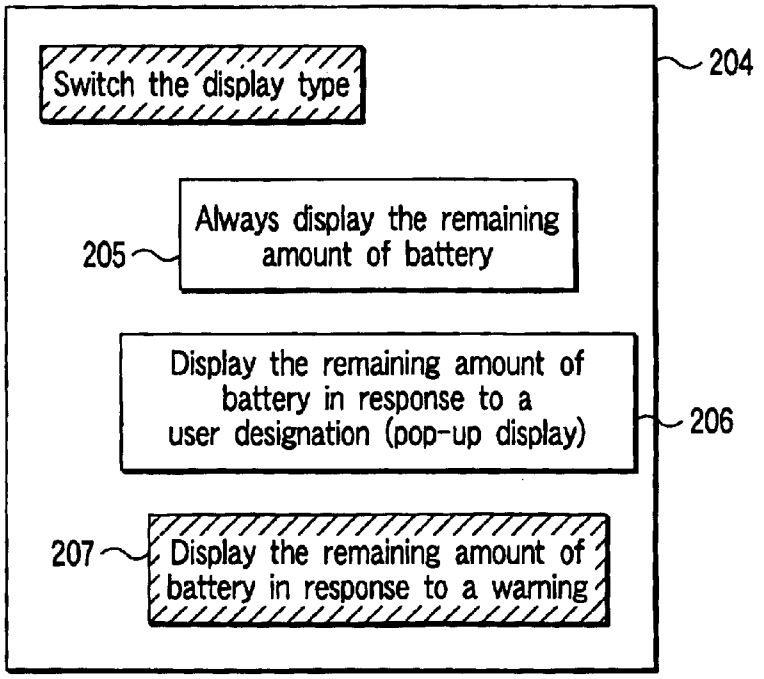

Switch the display type
204
205
Always display the remaining amount of battery
Display the remaining amount of battery in response to a user designation (pop-up display)
206
207
Display the remaining amount of battery in response to a warning

FIG. 13

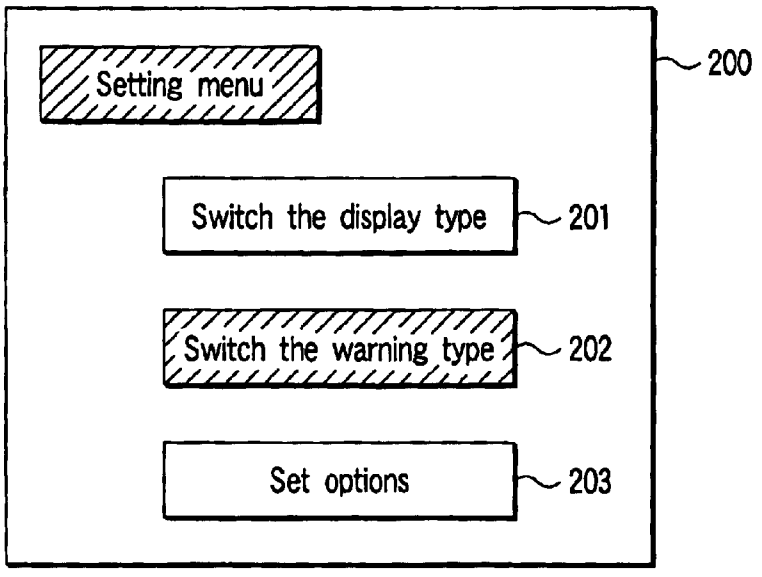

Setting menu
200
Switch the display type
201
Switch the warning type
202
Set options
203

FIG. 14

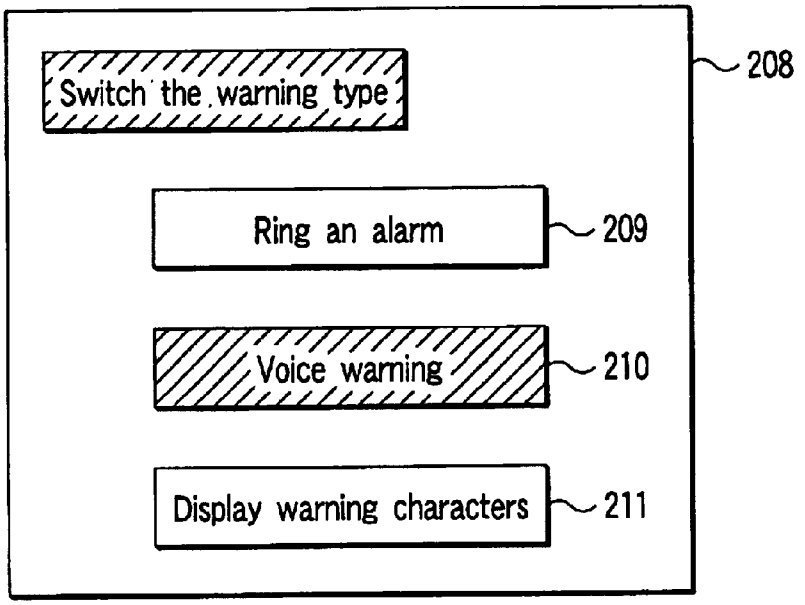

Switch the warning type
208
Ring an alarm
209
Voice warning
210
Display warning characters
211

FIG. 15

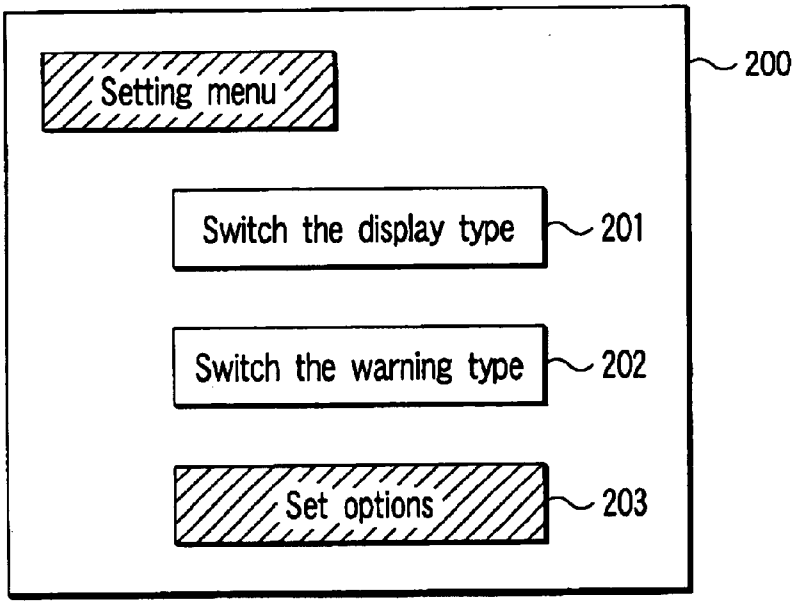

Setting menu
200
Switch the display type
201
Switch the warning type
202
Set options
203

FIG. 16

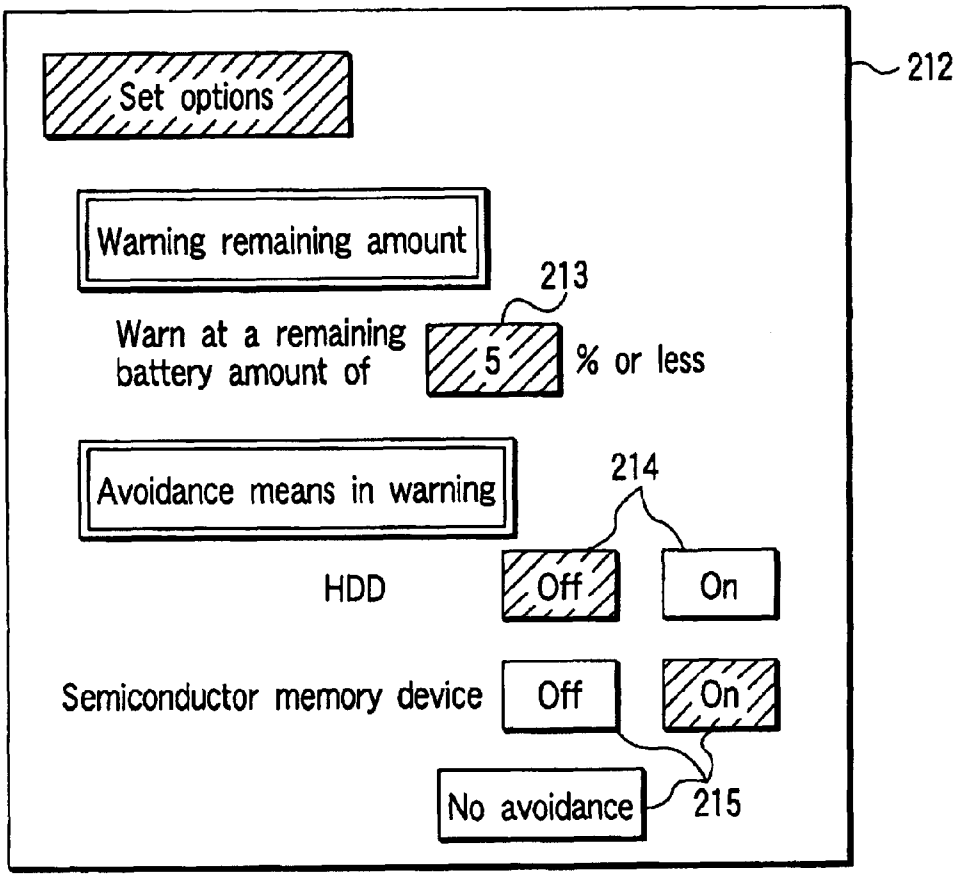

212
Set options
Warning remaining amount
213
Warn at a remaining battery amount of
5
% or less
Avoidance means in warning
214
HDD
Off
On
Semiconductor memory device
Off
On
No avoidance
215

FIG. 17

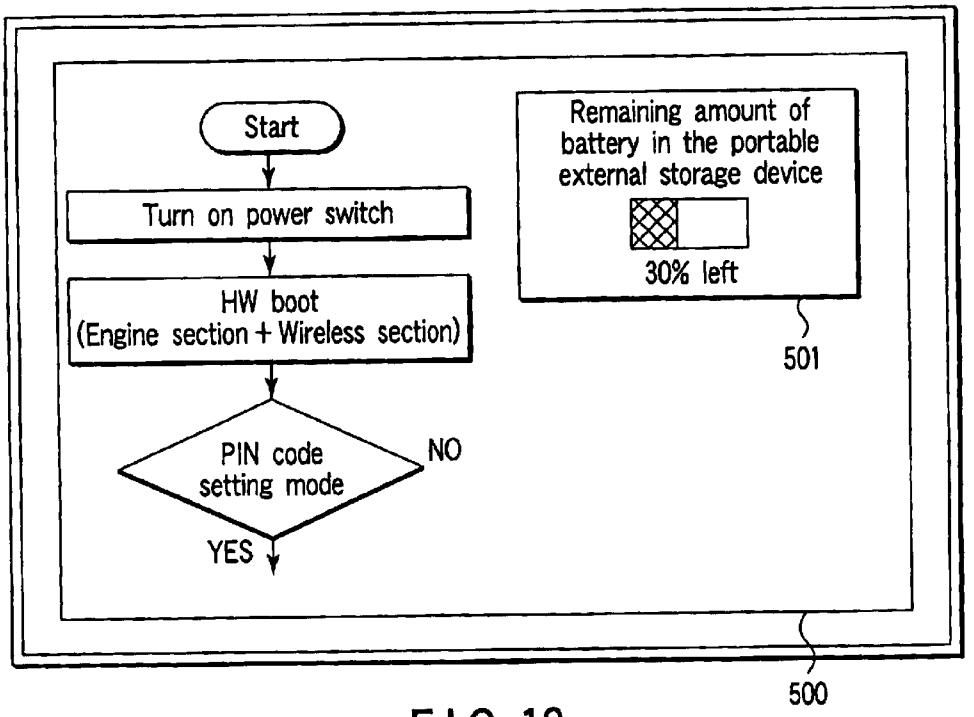

Start
Turn on power switch
HW boot
(Engine section + Wireless section)
PIN code
setting mode
NO
YES
Remaining amount of
battery in the portable
external storage device
30% left
501
500

FIG. 18

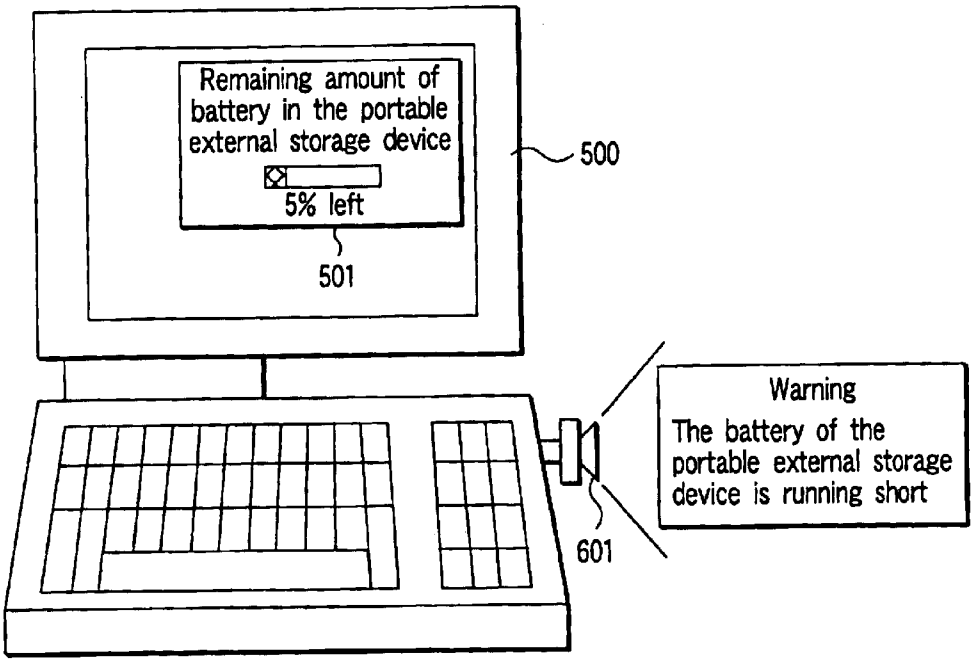

Remaining amount of
battery in the portable
external storage device
5% left
501
500
Warning
The battery of the
portable external storage
device is running short
601

FIG. 19

EXTERNAL STORAGE DEVICE, AND REMAINING BATTERY AMOUNT NOTIFYING METHOD IN THE SAME

CROSS REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims the benefit of priority from the prior Japanese Patent Application No. 2002-22316, filed Jan. 30, 2002, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an external storage device used as the external device of an information processing apparatus.

2. Description of the Related Art

Portable external storage devices having a wireless communication function have recently been developed. In the general use of the portable external storage device, the device is stored in a bag, shirt pocket, or the like. The external storage device accesses a host device such as a personal computer, PDA (Personal Digital Assistant), digital camera, or digital movie by Bluetooth radiowaves.

The remaining amount of battery in the portable external storage device, that is, the energy remaining in the battery, is confirmed on a display mounted on the portable external storage device.

As described above, the portable external storage device is often used in a bag, pocket, or the like. The user cannot quickly, easily confirm information such as the remaining amount of battery.

BRIEF SUMMARY OF THE INVENTION

The present invention has been made in consideration of the above situation, and has as its object to provide a device capable of letting the user know the remaining amount of battery and a warning that the battery is running short even while the device is stored in a bag, pocket, or the like.

To achieve the above object, according to the present invention, there is provided an external storage device comprising a battery which supplies power to a communication section which communicates with an information processing apparatus, detection means for detecting a remaining amount of the battery, and notifying means for notifying the information processing apparatus of information about the remaining amount of the battery detected by the detection means.

Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instrumentalities and combinations particularly pointed out hereinafter.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention, and together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principles of the invention.

FIG. **1** is a view for explaining the use environment of a portable external storage device according to an embodiment of the present invention;

FIG. **2** is a block diagram showing the arrangement of the portable external storage device according to the embodiment of the present invention;

FIG. **3** is a flow chart for explaining the operation of a host device (e.g., PDA or PC) for the portable external storage device;

FIG. **4** is a flow chart for explaining the operation of the host device (e.g., PDA or PC) for the portable external storage device;

FIG. **5** is a flow chart for explaining the operation of the portable external storage device;

FIG. **6** is a flow chart for explaining the operation of the portable external storage device;

FIG. **7** is a flow chart for explaining the operation of the portable external storage device;

FIG. **8** is a view showing a time sequence between the portable external storage device and the host device;

FIG. **9** is a view showing another time sequence between the portable external storage device and the host device;

FIG. **10** is a view showing still another time sequence between the portable external storage device and the host device;

FIG. **11** is a view showing a setting menu window;

FIG. **12** is a view showing a case in which a display type switching button is selected on the setting menu window;

FIG. **13** is a view showing a submenu corresponding to the display type switching button;

FIG. **14** is a view showing a case in which a warning type switching button is selected on the setting menu window;

FIG. **15** is a view showing a submenu corresponding to the warning type switching button;

FIG. **16** is a view showing a case in which an option setting button is selected on the setting menu window;

FIG. **17** is a view showing a submenu corresponding to the option setting button;

FIG. **18** is a view showing an example in which the remaining amount of battery in the portable external storage device is displayed as a pop-up window on the display of the host device; and

FIG. **19** is a view showing a state in which the loudspeaker of the host device outputs a warning by voice.

DETAILED DESCRIPTION OF THE INVENTION

A portable external storage device according to a preferred embodiment of the present invention will be described below with reference to the several views of the accompanying drawing.

FIG. **1** is a view for explaining the use environment of the portable external storage device according to the embodiment of the present invention.

As shown in FIG. **1**, communication partners of a portable external storage device **1** according to the embodiment are information devices such as a personal computer **2**, portable game machine **3**, digital video camera **4**, and PDA (Personal Digital Assistant) **5**. The portable external storage device **1** of the embodiment and the information devices **2** to **5** serving as communication partners incorporate Bluetooth modules, respectively, and exchange data via the Bluetooth modules.

For example, to exchange image data between the digital camera **4** and the personal computer **2**, image data are first exchanged between the digital video camera **4** and the portable external storage device **1** by wireless communication using the Bluetooth modules, and stored in the internal recording medium of the portable storage device. At this time, the digital camera **4** and portable external storage device **1** can be wirelessly connected as far as they are positioned within a wireless communicable distance of about 100 m at maximum by the Bluetooth modules.

The portable external storage device is carried close to a predetermined distance (Bluetooth wireless communicable distance of about 100 m at maximum) from the personal computer **2** which transmits image data. Then, a Bluetooth link is automatically established, and image data is transferred from the portable storage device to the personal computer.

A portable external storage device according to the embodiment of the present invention will be described below. FIG. **2** is a block diagram showing the arrangement of the portable external storage device according to the embodiment of the present invention.

As shown in FIG. **2**, a portable external storage device **1** according to this embodiment comprises an engine section **11**, Bluetooth wireless section **12**, power supply section **13**, setting section **14**, and storage section **15**.

The engine section **11** controls the whole portable external storage device. A CPU **21** which controls the entire storage device is connected to an EEPROM **22** via a bus **26**. The EEPROM **22** records various pieces of setting information of the portable external storage device.

The CPU **21** is connected to a CPU bus/PCI bus bridge **25** via a CPU bus **27**. The CPU bus/PCI bus bridge **25** is connected to a DRAM **23** via a memory bus **28** and to a flash memory **24** via a memory bus **29**.

The DRAM **23** is a work memory for the CPU **21**, whereas the flash memory **24** stores a program executed by the CPU **21**.

The CPU bus/PCI bus bridge **25** is connected to a display controller **31** via a bus **30**, and the display controller **31** is connected to an LCD **33** via a bus **32**. The display controller **31** controls the display of the LCD **33**. The CPU bus/PCI bus bridge **25** functions as an interface bridge between the CPU bus **27** and a PCI bus **41**.

The PCI bus **41** is connected to an ISA bus **43** via a PCI/ISA (Peripheral Component Interconnect/Industry Standard Architecture) bridge **42**. The PCI bus **41** is connected to the Bluetooth wireless section **12** via a USB host controller **46** and to a USB interface **44**. The USB interface **44** is connected to a USB connector **45** for connecting a peripheral device.

The Bluetooth wireless section **12** comprises a baseband LSI **51** which is connected to the USB host controller **46** and controls the Bluetooth wireless function, a flash memory **52** which stores a program executed by the baseband LSI **51**, an antenna **54**, and an RF unit **53** which controls RF signals between the baseband LSI **51** and the antenna **54**.

The PCI bus **41** is connected to the storage section **15**. The storage section **15** comprises an IDE interface controller **61** connected via the PCI bus **41**, and an HDD **63** connected to the IDE interface controller **61** via an IDE interface **62**. The PCI bus **41** is connected to a PCMCIA host controller **91** and to a PC card HDD **93** via the PCMCIA host controller **91**. The PCI bus **41** is further connected to an SD memory controller **111** and to an SD memory card **113** via the SD memory controller **111**.

The PCI bus **41** is connected to the power supply section **13**. The power supply section **13** comprises a power supply controller **71** connected to the PCI bus **41**, and a power supply control circuit **73** connected to the power supply controller **71**. The power supply control circuit **73** is connected to a battery **74** and AC input **75**. Power is supplied from the battery **74** when the portable external storage device is used in a mobile environment, and from the AC input **75** in a battery chargeable/AC drivable environment.

Powers from the battery **74** and AC input **75** are supplied to elements such as the engine section **11**, wireless section **12**, and storage section **15** necessary to operate the portable external storage device.

The ISA bus **43** is connected to the setting section **14**. The setting section **14** comprises an I/O controller **81** connected to the ISA bus **43**, and a button **82** and rotary switch **83** connected to the I/O controller **81**. The button **82** and rotary switch **83** are used for security setting such as input of a Bluetooth PIN code, and activation of the device.

The portable external storage device uses the HDD **63** as a storage medium in the above description, but the storage medium is not limited to this.

The operation of the portable external storage device according to the embodiment of the present invention will be explained.

The portable external storage device according to the embodiment of the present invention causes a host device to let the user know information about the remaining amount of battery in the portable external storage device.

The operation of the host device (e.g., PDA or PC) of the portable external storage device will be described with reference to FIGS. **3** and **4**.

If a remaining battery amount notifying program starts in the host device, the host device displays a setting menu (**S1**). As shown in FIG. **11**, the setting menu displays a display type switching button **201**, warning type switching button **202**, and option setting button **203** on a setting menu window **200**.

The display type switching button **201** is a button for selecting an occasion when the remaining amount of battery is displayed.

The warning type switching button **202** is a button for selecting a warning method.

The option setting button **203** sets the threshold of the remaining amount of battery at which the user is warned of the remaining amount of battery, or an avoidance method in a warning.

The host device checks whether the user enters an input on the setting menu window **200** (**S2**). If YES in **S2**, the host device shifts to the process of **S16**.

In **S16**, the host device checks whether the display type switching button **201** displayed on the setting menu window **200** is selected. If YES in **S16** (FIG. **12**), the host device displays a submenu **204** corresponding to the display type switching button **201** shown in FIG. **13** (**S19**).

The submenu **204** corresponding to the display type switching button **201** displays a remaining battery amount display "normally ON" button **205**, remaining battery amount display "user designation" button **206**, and remaining battery amount display "warning" button **207**.

The remaining battery amount display "normally ON" button **205** is a button for selecting a remaining battery amount display "normally ON" mode in which information about the remaining amount of battery is always transmitted to the host device.

The remaining battery amount display "user designation" button **206** is a button for selecting a remaining battery amount display "user designation" mode in which information about the remaining amount of battery is transmitted to the host device when a user designates remaining battery amount display.

The remaining battery amount display "warning" button **207** is a button for selecting a remaining battery amount display "warning" mode in which information about the remaining amount of battery is transmitted to the host device when warning conditions set by the user are satisfied.

Of the modes (remaining battery amount display "normally ON" mode, remaining battery amount display "user designation" mode, and remaining battery amount display "warning" mode) selected on the submenu corresponding to the display type switching button shown in FIG. **13**, a mode input by the user (**S20**) is saved as setting information (**S21**).

If NO in **S16**, the host device checks whether the warning type switching button **202** is selected (**S17**). If YES in **S17** (FIG. **14**), the host device displays a submenu **208** corresponding to the warning type switching button **202** shown in FIG. **15** (**S19**).

The submenu **208** corresponding to the warning type switching button **202** displays an alarm ringing button **209**, voice warning button **210**, and warning character display button **211**.

The alarm ringing button **209** is a button for selecting a mode in which a warning is generated by ringing an alarm.

The voice warning button **210** is a button for selecting a mode in which a warning is generated by voice.

The warning character display button **211** is a button for selecting a mode in which a warning is generated by characters.

Of the modes (remaining battery amount display "normally ON" mode, remaining battery amount display "user designation" mode, and remaining battery amount display "warning" mode) selected on the submenu corresponding to the warning type switching button shown in FIG. **15**, a mode input by the user (**S20**) is saved as setting information (**S21**).

If NO in **S17**, the host device checks whether the option setting button **203** is selected (**S18**). If YES in **S18** (FIG. **16**), the host device displays a submenu **212** corresponding to the option setting button **203** shown in FIG. **17** (**S19**).

The submenu **212** corresponding to the option setting button **203** displays an item **213** for setting a remaining amount of battery at which a warning is generated, an item **214** for setting the avoidance means for an HDD in a warning, and an item **215** for setting the avoidance means for a semiconductor memory device (e.g., SD memory) in a warning. In FIG. **17**, a warning is generated when the remaining amount of battery decreases to 5% or less. In the warning, the HDD is turned off, and the semiconductor memory device is turned on.

An item input by the user on the submenu **212** corresponding to the option setting button **203** shown in FIG. **17** is saved as setting information (**S21**).

After setting information is saved in **S21**, or if NO in **S18**, the host device checks whether the display of the setting menu ends (**S22**).

If NO in **S22**, the host device returns to the process of **S16**; if YES, to the process of **S4**.

If NO in **S2**, the host device determines that a default value is set (**S3**), and shifts to the process of **S4**. In **S4**, the host device establishes wireless communication with the portable external storage device according to the embodiment of the present invention, and transmits the setting information (**S5**).

The host device checks whether the user generates a remaining battery amount request (**S6**). If YES in **S6**, the host device transmits a remaining battery amount acquisition request to the portable external storage device (**S7**).

If NO in **S6**, or after the host device transmits the remaining battery amount acquisition request in **S7**, the host device checks whether to receive remaining battery amount information from the portable external storage device (**S8**).

If YES in **S8**, the host device loads the received data (**S9**), and displays the remaining amount of battery (**S10**).

The host device checks whether to receive battery warning information from the portable external storage device (**S11**). If YES in **S11**, the host device loads the warning information (**S12**), and executes a warning based on the setting information set by the user (**S13**).

For example, when the voice warning button **210** is selected on the submenu corresponding to the warning type switching button shown in FIG. **15**, a warning is generated by voice. When the warning character display button **211** is selected, a warning message concerning the battery is displayed on the screen of the information processing apparatus.

FIG. **18** shows an example in which the remaining amount of battery in the portable external storage device is displayed as a pop-up window **501** on a display **500** of the host device. FIG. **19** is a view showing a state in which a loudspeaker **601** of the host device outputs a voice warning.

Then, the host device checks whether the program ends (**S14**). If YES in **S14**, the host device transmits an end command to the portable external storage device (**S15**), and stops the program. If NO in **S14**, the host device returns to the process of **S6**.

The operation of the portable external storage device will be explained with reference to FIGS. **5** to **7**.

After the program starts, the portable external storage device checks whether wireless communication starts (**S30**). If YES in **S30**, the portable external storage device receives setting information from the host (**S31**), and saves the received setting information (**S32**).

The portable external storage device checks whether the remaining battery amount display "normally ON" ("always" notifying) mode has been selected on the submenu corresponding to the display type switching button (**S33**).

If YES in **S33**, the portable external storage device checks the remaining amount of battery (**S37**), and determines whether the checked remaining amount of battery is equal to or smaller than a warning remaining amount of battery represented by the saved setting information (**S38**).

If YES in **S38**, i.e., the battery has a sufficient remaining amount, the portable external storage device transmits the checked remaining amount of battery to the host device (**S41**).

If NO in **S38**, i.e., the battery is running short, the portable external storage device transmits warning information to the host device (**S39**). The portable external storage device saves its stored data in an avoidance destination of data, that is, the portable external storage device saves its data in an alternate storage location in order to avoid data loss when the warning is generated, represented by the setting information (**S40**). When the setting information represents no avoidance in a warning, no data avoidance is performed.

The portable external storage device checks whether it has received an end command from the host device (**S42**). If

YES in S42, the portable external storage device stops the program; if NO, returns to the process of S37.

If NO in S33, the portable external storage device checks whether the mode in which the remaining amount of battery is displayed in response to a user designation is selected on the submenu corresponding to the display type switching button (S34).

If YES in S34, the portable external storage device checks whether it has received a remaining battery amount request from the host device (S51).

If YES in S51, the portable external storage device checks the remaining battery amount (S52), and determines whether the checked remaining amount of battery is equal to or smaller than a warning remaining amount of battery represented by the saved setting information (S53).

If YES in S53, i.e., the battery has a sufficient remaining amount, the portable external storage device transmits the checked remaining amount of battery to the host device (S54).

If NO in S53, i.e., the battery is running short, the portable external storage device transmits warning information to the host device (S55). The portable external storage device saves its stored data in an avoidance destination of data represented by the setting information (S56). When the setting information represents no avoidance in a warning, no data avoidance is performed.

Then, the portable external storage device checks whether it has received an end command from the host device (S57). If YES in S57, the portable external storage device stops the program; if NO, returns to the process of S51.

If NO in S34, the portable external storage device checks whether the mode in which warning information is transmitted in response to a warning is selected on the submenu corresponding to the display type switching button (S35).

If YES in S35, the portable external storage device checks the remaining amount of battery (S61), and determines whether the checked remaining amount of battery is equal to or smaller than a warning remaining amount of battery represented by the saved setting information (S62).

If NO in S62, i.e., the battery is running short, the portable external storage device transmits warning information to the host device (S63). The portable external storage device saves its stored data in an avoidance destination of data represented by the setting information (S64). When the setting information represents no avoidance in a warning, no data avoidance is performed.

The portable external storage device checks whether it has received an end command from the host device (S65). If YES in S65, the portable external storage device stops the program; if NO, returns to the process of S61.

FIGS. **8** to **10** are views showing time sequences between the portable external storage device and the host device in the respective modes. FIGS. **8** to **10** are views for supplementally explaining the flow charts shown in FIGS. **3** to **7**.

FIG. **8** is a view showing a sequence when remaining battery amount display is normally ON.

The host device displays a setting menu (**100**), and the user inputs settings on the displayed setting menu (**101**). The host device saves the pieces of input setting information (**102**).

After that, wireless communication (in this case, Bluetooth communication connection) is executed between the host device and the portable external storage device (**103**), and the host device transmits the setting information to the portable external storage device (**104**).

The portable external storage device saves the setting information transmitted from the host device (**105**). The portable external storage device checks the remaining amount of battery, and determines whether the checked remaining amount of battery is equal to or smaller than a remaining amount of battery represented by the setting information at which a warning is generated (**106**).

If the checked remaining amount of battery is larger than the remaining amount of battery represented by the setting information at which a warning is generated, i.e., the battery has a sufficient remaining amount, the portable external storage device transmits remaining battery amount information (**107**).

If the checked remaining amount of battery is equal to or smaller than the remaining amount of battery represented by the setting information at which a warning is generated, i.e., the battery is running short, the portable external storage device transmits battery warning information to the host device (**108**).

Upon reception of the remaining battery amount information or warning information, the host device performs processing such as display of a warning on the display or generation of warning sound on the basis of the setting information (**109**). Finally, the host device transmits an end command to the portable external storage device (**110**), and ends the program.

FIG. **9** is a view for explaining a sequence when the remaining battery amount display "user designation" mode in which information about the remaining amount of battery is transmitted to the host device upon reception of a user designation.

Note that processing up to display of a setting menu on the host device, establishment of wireless communication between the host device and the portable external storage device, and saving of setting information in the portable external storage device is the same as that shown in FIG. **8**, and a description thereof will be omitted.

When the user wants to know the remaining amount of battery, he/she requests the host device to display the remaining amount of battery by, e.g., clicking an icon (**301**). Upon reception of the user request, the host device transmits a remaining battery amount acquisition request to the portable external storage device (**302**).

The portable external storage device checks the remaining amount of battery, and determines whether the checked remaining amount of battery is equal to or smaller than a remaining amount of battery represented by the setting information at which a warning is generated (**303**).

If the checked remaining amount of battery is larger than the remaining amount of battery represented by the setting information at which a warning is generated, i.e., the battery has a sufficient remaining amount, the portable external storage device transmits remaining battery amount information (**304**).

If the checked remaining amount of battery is equal to or smaller than the remaining amount of battery represented by the setting information at which a warning is generated, i.e., the battery is running short, the portable external storage device transmits battery warning information to the host device (**305**).

Upon reception of the remaining battery amount information or warning information, the host device performs processing such as display of a warning on the display or generation of warning sound on the basis of the setting information (**306**). Finally, the host device transmits an end

command to the portable external storage device (**307**), and ends the program.

FIG. **10** is a view for explaining a sequence when the remaining battery amount display "warning" mode in which information about the battery is transmitted to the host device when the battery is running short.

Note that processing up to display of a setting menu on the host device, establishment of wireless communication between the host device and the portable external storage device, and saving of setting information in the portable external storage device is the same as that shown in FIG. **8**, and a description thereof will be omitted.

The portable external storage device checks the remaining amount of battery (**401**). If the remaining amount of battery is equal to or smaller than a remaining amount of battery contained in setting information at which a warning is generated, the portable external storage device transmits battery warning information to the host device (**402**). The host device generates a warning on the basis of the battery warning information from the portable external storage device (**403**), and transmits an end command to the portable external storage device (**404**).

If the remaining amount of battery is larger than the remaining amount of battery at which a warning is generated, the portable external storage device does not transmit any information to the host device, and continuously checks the remaining amount of battery.

Note that the portable external storage device and the information processing apparatus serving as a host device wirelessly communicate with each other in the above-described embodiment, but may communicate by wire.

The present invention is not limited to the above-described embodiment, and can be variously modified without departing from the spirit and scope of the invention in practical use.

The portable external storage device according to the embodiment of the present invention can notify the user of information about the battery via the host device. The user can quickly know information about the battery regardless of the storage location of the portable external storage device.

Additional advantages and modifications will readily occur to those skilled in the art. Therefore, the invention in its broader aspects is not limited to the specific details and representative embodiments shown and described herein. Accordingly, various modifications may be made without departing from the spirit or scope of the general inventive concept as defined by the appended claims and their equivalents.

What is claimed is:

1. A device comprising:

a battery which supplies power to a communication section which communicates with an information processing apparatus;

means for receiving, from the information processing, apparatus, a setting information representing at least one of a notifying method for information about remaining energy of said battery, or level of remaining energy of said battery at which a warning is to be displayed on the information processing apparatus; and

means for storing the received setting information; and

means for detecting a remaining energy of said battery; and

means for transmitting, to the information processing apparatus, information about the remaining energy of said battery on the basis of the received setting information.

2. A device according to claim **1**, wherein said notifying means comprises

means for determining whether the remaining energy of said battery detected by said detection means is not more than the remaining energy of said battery represented by the setting information when the notifying method represented by the setting information is a method of notifying the information processing apparatus of a remaining energy of said battery, and

means for, when said determination means determines that the remaining energy of said battery is not more than the remaining energy of said battery represented by the setting information, notifying the information processing apparatus of warning information representing that the remaining energy of said battery is not more than the remaining energy of said battery represented by the setting information, and when said determination means determines that the remaining energy of said battery is more than the remaining energy of said battery represented by the setting information, notifying the information processing apparatus of the remaining energy of said battery detected by said detection means.

3. A device according to claim **1**, wherein said notifying means comprises

first means for determining whether a user has inputted a remaining battery energy information request, while the notifying method represented by the setting information is a method of notifying the information processing apparatus of a remaining energy of said battery in response to a user designation,

second means for determining whether the remaining energy of said battery detected by said detection means is not more than the remaining energy of said battery represented by the setting information when said first means determines that the user inputs the remaining battery energy information request, and

means for, when said second determination means determines that the remaining energy of said battery is not more than the remaining energy of said battery represented by the setting information, notifying the information processing apparatus of warning information representing that the remaining energy of said battery is not more than the remaining energy of said battery represented by the setting information and when said second means determines that the remaining energy of said battery is more than the remaining energy of said battery represented by the setting information, notifying the information processing apparatus of the remaining energy of said battery detected by said detection means.

4. A device according to claim **1**, wherein said notifying means comprises

means for determining whether the remaining energy of said battery detected by said detection means is not more than the remaining energy of said battery represented by the setting information when the notifying method represented by the setting information is a notifying method for a case in which the remaining energy of said battery is not more than a remaining energy of said battery represented by the setting information at which a warning is generated, and

means for notifying the information processing apparatus of warning information representing that the remaining energy of said battery is not more than the remaining energy of said battery represented by the setting

information, when said determination means determines that the remaining energy of said battery is not more than the remaining energy of said battery represented by the setting information.

5. A device according to claim **1**, in which the setting information includes avoidance destination information representing an avoidance destination of data in the device when a warning is generated, and

which further comprises

means for determining whether the remaining energy of said battery detected by said detection means is not more than the remaining energy of said battery represented by the setting information at which a warning is generated, and

means for storing data stored in the external storage device in an alternate storage location specified by the avoidance destination information when said determination means determines that the remaining energy of said battery detected by said detection means is not more than the remaining energy of said battery represented by the setting information at which a warning is generated.

6. A device according to claim **1**, wherein the information processing apparatus and the device wirelessly communicate with each other.

7. A remaining battery energy notifying method for a device in an information processing apparatus which communicates data with the device, comprising:

transmitting a setting information representing a notifying method for information about a remaining energy of a battery and a level of remaining energy of said battery at which a warning is generated to notify the information processing apparatus to the device, wherein the setting information is transmitted from the information processing apparatus;

receiving, from the device, information about the remaining energy of the battery acquired in the device in response to the setting information ; and

displaying the received information about the remaining energy of the battery in the information processing apparatus.

8. A battery information notifying system which notifies an information processing apparatus serving as a host device of information about a battery of an external device, wherein

the information processing apparatus comprises:

transmission means for transmitting, to the external device, setting information representing a notifying method for information about a remaining energy of a battery of the external device, and a remaining energy of the battery at which a warning is generated,

the external device comprises:

a battery which supplies power to a communication section which communicates with a plurality of information processing apparatuses;

means for detecting a remaining energy of said battery;

means for storing setting information transmitted from the information processing apparatus; and

means for notifying the host device of information about the remaining energy of said battery detected by said detection means, on the basis of the setting information stored in said storage means, and

the information processing apparatus further comprises:

means for receiving the information about the remaining energy of said battery from the external device; and

means for exhibiting the received information about the remaining energy of said battery on the basis of the notifying method for the information about the remaining energy of said battery represented by the setting information.

9. An external storage device comprising:

a battery which supplies power to a communication section which communicates with an information processing apparatus;

means for detecting a remaining energy of said battery;

means for storing setting information representing a notifying method for information about a remaining energy of said battery transmitted from the information process apparatus, and a remaining energy of said battery at which a warning is generated; and

means for notifying the information processing apparatus of information about the remaining energy of said battery detected by said detection means on the basis of the setting information stored in said storage means.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,831,444 B2
DATED : December 14, 2004
INVENTOR(S) : Kobayashi et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 9,
Lines 55-56, change "processing, apparatus," to -- processing apparatus, --.

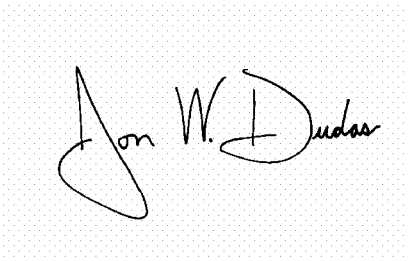
Column 10,
Line 46, change "information and" to -- information, and --.

Column 11,
Line 39, change "information ; and" to -- information; and --.

Column 12,
Line 37, change "process" to -- processing --.

Signed and Sealed this

Nineteenth Day of April, 2005



JON W. DUDAS
Director of the United States Patent and Trademark Office

EXHIBIT 2

US006928166B2

(12) **United States Patent**
Yoshizawa

(10) **Patent No.: US 6,928,166 B2**
(45) **Date of Patent: Aug. 9, 2005**

(54) **RADIO COMMUNICATION DEVICE AND USER AUTHENTICATION METHOD FOR USE THEREWITH**

(75) Inventor: **Junichi Yoshizawa**, Ome (JP)

(73) Assignee: **Kabushiki Kaisha Toshiba**, Kawasaki (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 887 days.

(21) Appl. No.: **09/795,355**

(22) Filed: **Mar. 1, 2001**

(65) **Prior Publication Data**

US 2001/0036273 A1 Nov. 1, 2001

(30) **Foreign Application Priority Data**

Apr. 28, 2000 (JP) 2000-131861

(51) **Int. Cl.**[7] **H04K 1/00**; H04L 9/16
(52) **U.S. Cl.** **380/247**; 380/255; 713/168
(58) **Field of Search** 380/247, 270, 380/255; 713/168, 169, 171, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,442,805	A	8/1995	Sagers et al.	
6,748,195	B1 *	6/2004	Phillips	455/41.2
6,766,160	B1 *	7/2004	Lemilainen et al.	455/411
2002/0132605	A1 *	9/2002	Smeets et al.	455/411
2004/0128509	A1 *	7/2004	Gehrmann	713/171

FOREIGN PATENT DOCUMENTS

EP	WO 97/26769	7/1997	
EP	WO 01/74011 A1	10/2001	
GB	2350971 A *	12/2000	..... G06F/1/00
JP	09-233223	9/1997	
JP	2872996	1/1999	

OTHER PUBLICATIONS

Johannes Elg, "Specification of the Bluetooth System," ver. 1.0 B, pp. 186–199, Nov. 29, 1999.
English abstract of JP 11–275661 published Oct. 8, 1999.

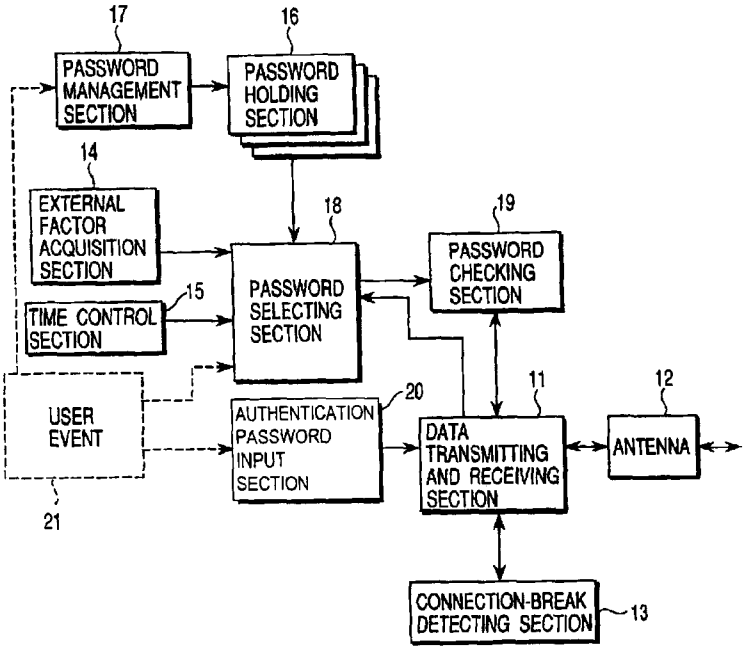
* cited by examiner

Primary Examiner—Matthew Smithers
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

(57) **ABSTRACT**

To allow flexible security level switching according communication situations, a password holding section holds a plurality of device authentication passwords, for example, a temporary password and a private password. The temporary password is valid only under a certain situation and the private password has a high level of confidentiality to increase the device security. A password management section allows the user to add a new password to the password holding section and delete an existing password therefrom. A password selecting section selects the most suitable password for current connection from among passwords in the password holding section according to a user event, information acquired by an external factor acquisition section, and information from a time control section. The selected password is output to a password checking section.

19 Claims, 5 Drawing Sheets



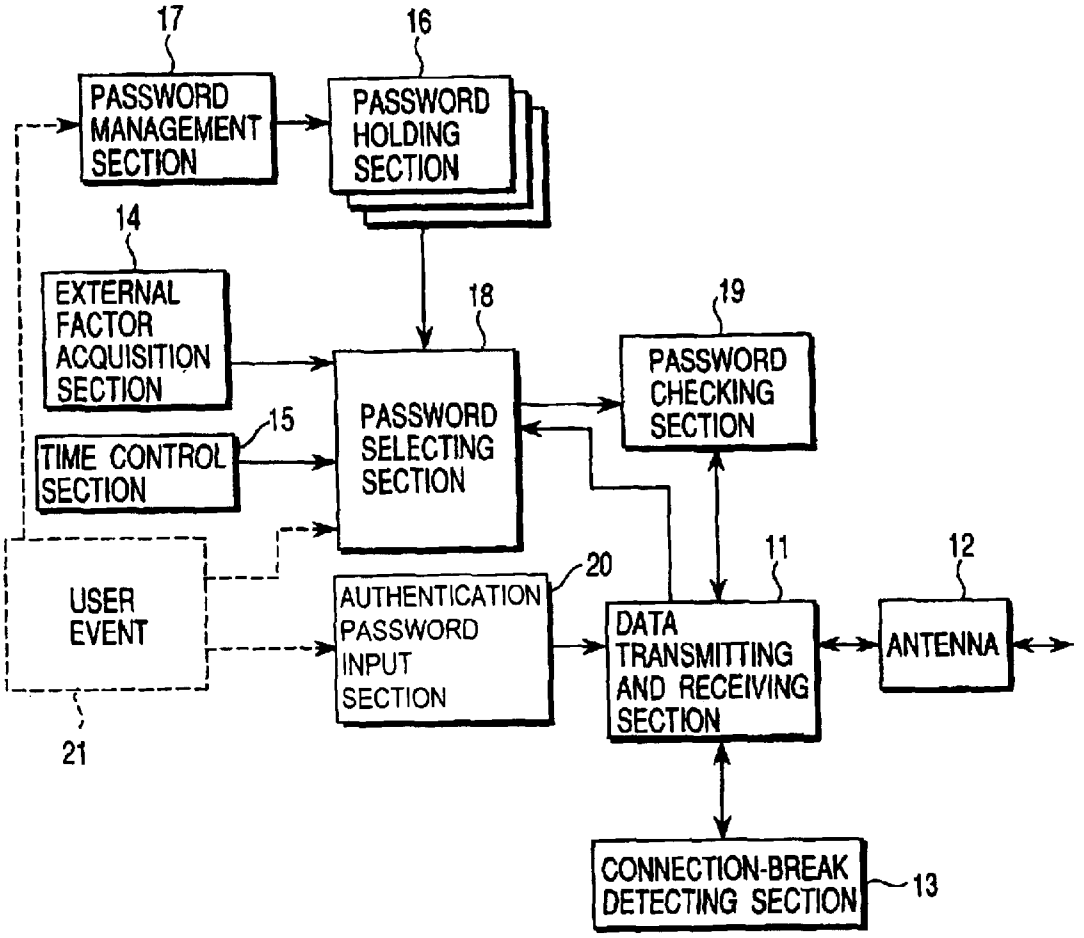

17
16
PASSWORD MANAGEMENT SECTION
PASSWORD HOLDING SECTION
14
EXTERNAL FACTOR ACQUISITION SECTION
18
19
PASSWORD CHECKING SECTION
15
TIME CONTROL SECTION
PASSWORD SELECTING SECTION
USER EVENT
20
AUTHENTICATION PASSWORD INPUT SECTION
11
12
DATA TRANSMITTING AND RECEIVING SECTION
ANTENNA
21
CONNECTION-BREAK DETECTING SECTION
13

FIG. 1

DEVICE A
DEVICE B
CONNECTION REQUEST

FIG. 2

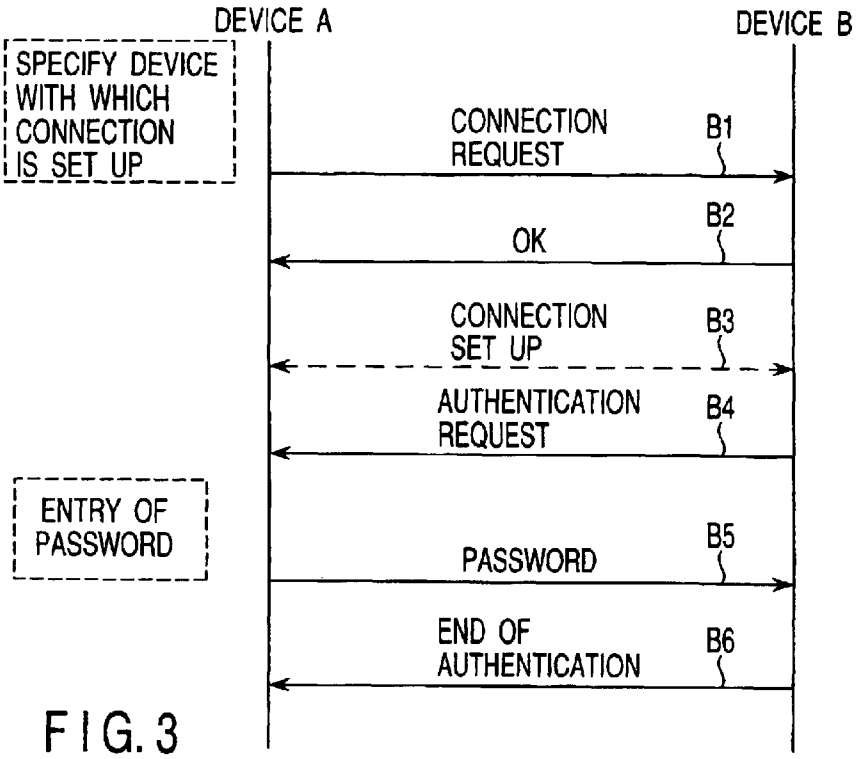

DEVICE A
DEVICE B
SPECIFY DEVICE WITH WHICH CONNECTION IS SET UP
CONNECTION REQUEST
B1
OK
B2
CONNECTION SET UP
B3
AUTHENTICATION REQUEST
B4
ENTRY OF PASSWORD
PASSWORD
B5
END OF AUTHENTICATION
B6

FIG. 3

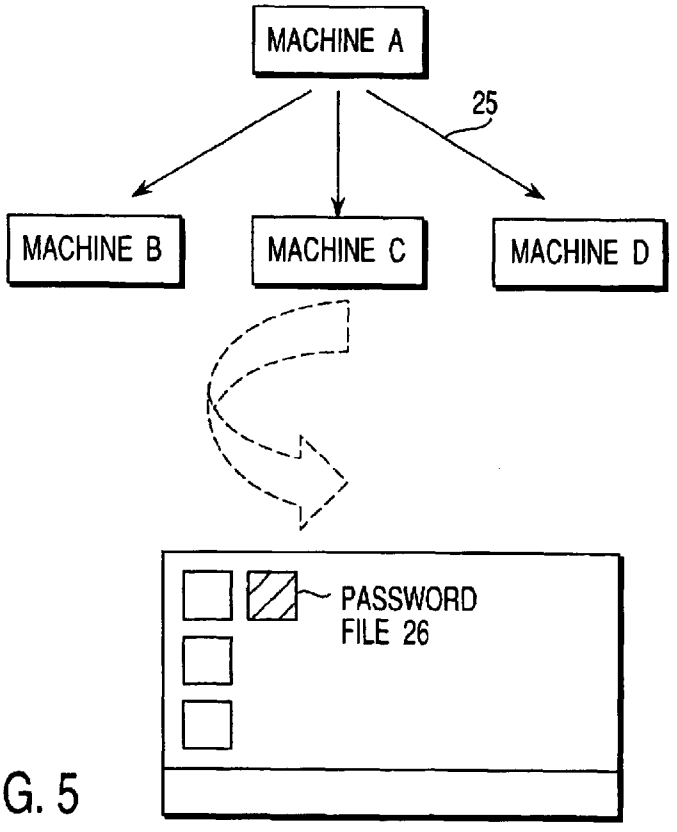

MACHINE A
25
MACHINE B
MACHINE C
MACHINE D
PASSWORD FILE 26

FIG. 5

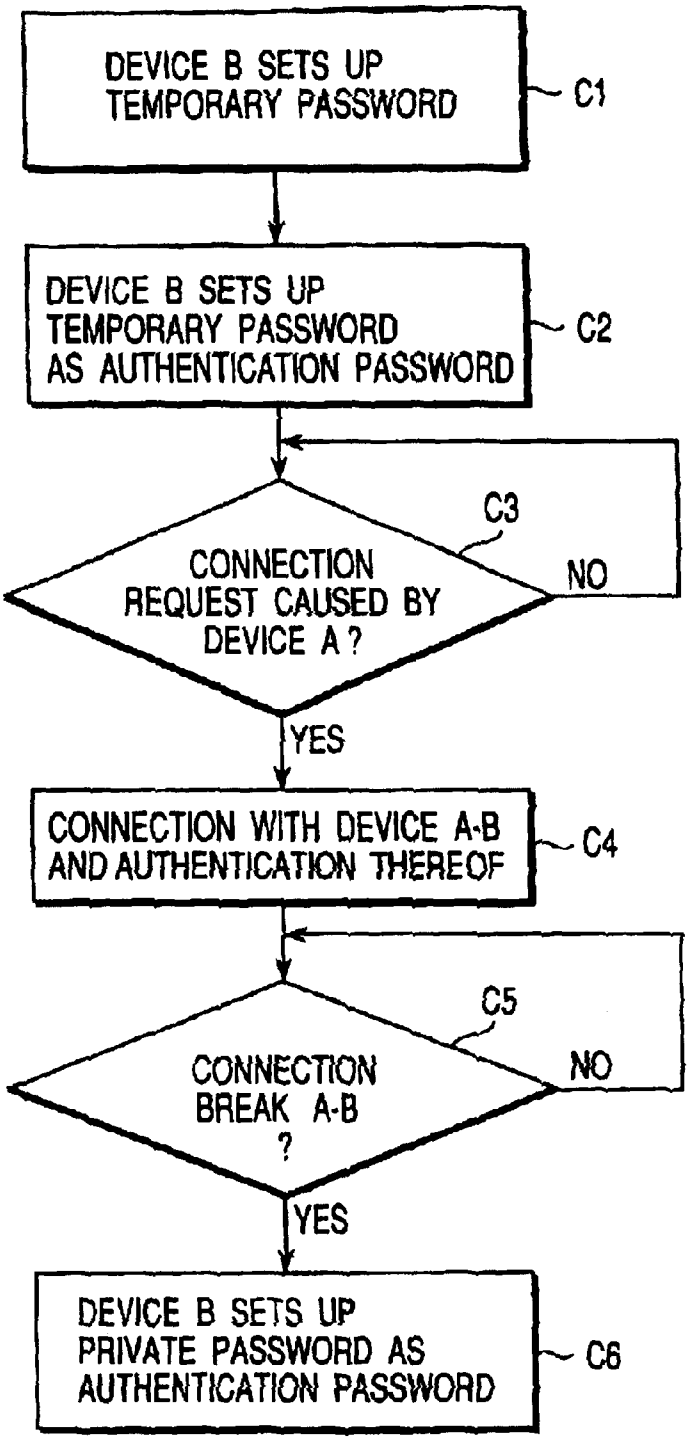

DEVICE B SETS UP TEMPORARY PASSWORD
C1
DEVICE B SETS UP TEMPORARY PASSWORD AS AUTHENTICATION PASSWORD
C2
C3
CONNECTION REQUEST CAUSED BY DEVICE A ?
NO
YES
CONNECTION WITH DEVICE A-B AND AUTHENTICATION THEREOF
C4
C5
CONNECTION BREAK A-B ?
NO
YES
DEVICE B SETS UP PRIVATE PASSWORD AS AUTHENTICATION PASSWORD
C6

FIG. 4

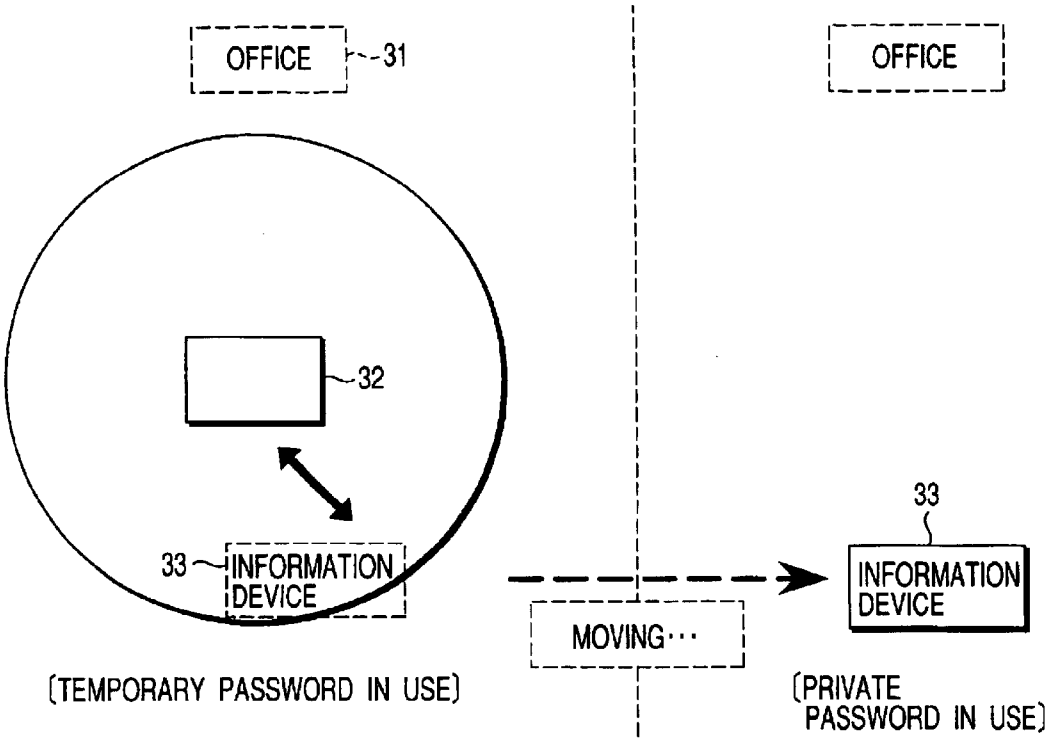

OFFICE
31
OFFICE
32
33
INFORMATION DEVICE
33
INFORMATION DEVICE
MOVING···
(TEMPORARY PASSWORD IN USE)
(PRIVATE PASSWORD IN USE)

FIG. 6

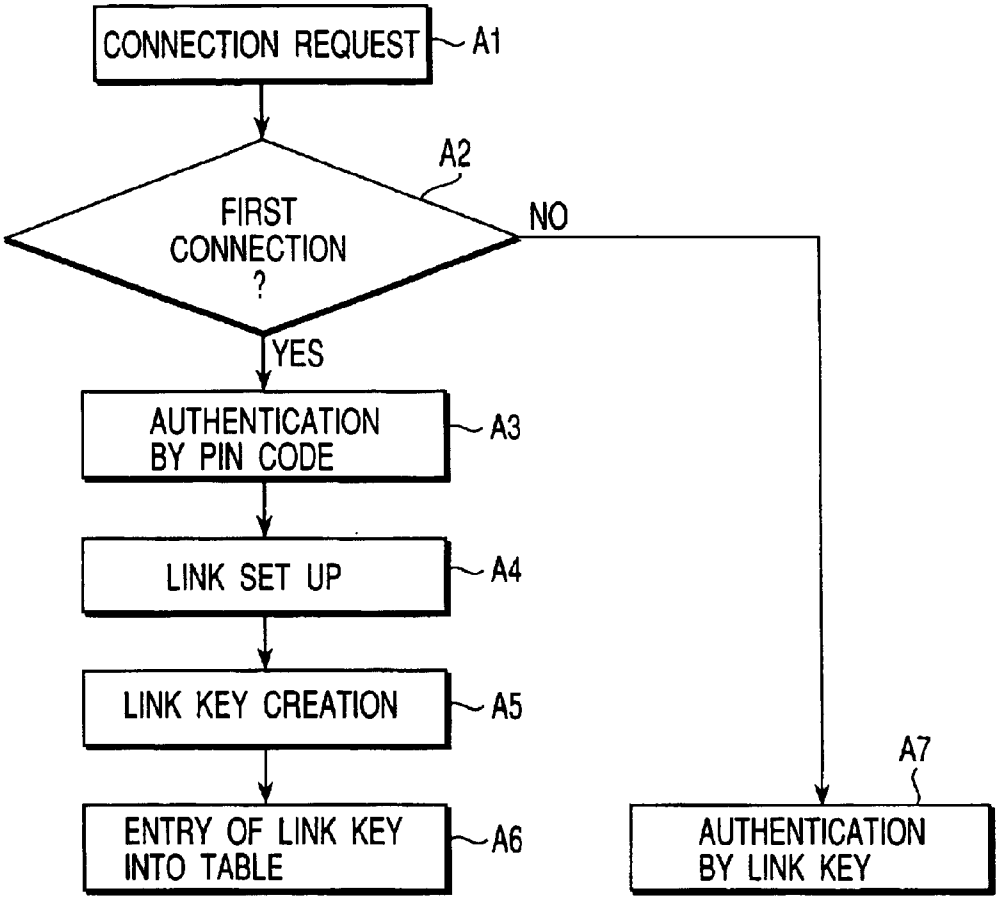


FIG. 7 (PRIOR ART)

UNIQUE ADDRESS (Hex)	LINK KEY
A36B35	******
4B3346	******
.....	.....

FIG. 8 (PRIOR ART)

RADIO COMMUNICATION DEVICE AND USER AUTHENTICATION METHOD FOR USE THEREWITH

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims the benefit of priority from the prior Japanese Patent Application No. 2000-131861, filed Apr. 28, 2000, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to a radio communication device and a user authentication method using user authentication passwords.

In recent years, attention has been paid to radio communication systems adapted for personal areas, such IrDA, Bluetooth, HomeRF, etc. Particularly, Bluetooth and HomeRF have merits of no directivity and high transparence over infrared communication systems, such as IrDA, and are greatly expected to develop and find wide application in the future. The Bluetooth is short-haul radio communication standards and establishes radio communications within 10 m or 100 m using the ISM (Industrial Science Medical) band of 2.4 GHz band. The Bluetooth adopts frequency-hopping spectrum-spreading techniques and allows for connection of up to eight devices through the use of time-division multiplexing techniques.

In addition to allowance for simultaneous connection of multiple devices, the radio communication systems, such as Bluetooth, HomeRF, etc., make a great feature of a relatively long transmission distance of, say, 10 to 100 m in comparison with the infrared communication systems, such as IrDA. This provides an advantage of ease of handling, but on the other hand sufficient attention must be paid to assure system security and confidentiality.

Conventional security systems for radio communication systems include the radio terminal security system as described in Japanese Patent No. 2872996 and the one-time password system as used in the Internet.

These security systems include electronic keys and radio terminals and prohibit successive use of the same key to increase security, thereby providing increased safety against loss and theft of the key.

Next, the user authentication system used in the Bluetooth will be described.

The user authentication system used in the Bluetooth is subject to two: a unique password set up on each device (called a PIN (Personal Identification Number) code) and an encryption key (called link key) created by the password and an ID code unique to the device (information, such as a 48-bit address, assigned by IEEE). This system will be described in brief below with reference to a flowchart shown in FIG. **7**.

Consider now the case where a device A makes access to a device B. The device A makes a request for connection to the device B (step **A1**), whereupon the device B checks the presence or absence of the link key to see if the connection to the device A is set up for the first time (step **A2**). That is, the device B is stored with a list of link keys besides PIN codes. This list is a table of unique addresses of devices connected so far to the device B and corresponding link keys. An example of this table is illustrated in FIG. **8**.

In the situation in which the device A and the device B are connected for the first time, the device A is required to input

the PIN code of the device B. Upon receiving the PIN code from the device A, the device B checks it for validity (step **A3**). If the PIN code is authenticated, then the device B establishes a link (step **A4**) and creates a link key for the device A (step **A5**). The resulting link key is entered into the list together with the unique address of the device A (step **A6**).

If, on the other hand, the device A was sometimes connected to the device B in the past, since the link key has already been entered into the table in the device B, authentication is made through that link key (step **A7**).

The Bluetooth provides authentication using the PIN code unique to each device and the link key based on the PIN code. The PIN code, while being unique, can be altered by the device user into any other string of characters.

The security system disclosed in Japanese Patent No. 2872996, the one-time password system in the Internet and the user authentication system in the Bluetooth can be said to be password management and authentication systems intended to provide only increased security.

The use of the user authentication system in ad hoc network environment causes problems as described below.

As an application of the user authentication system used in the Bluetooth, consider a table conferencing system made up of a plurality of information devices. Each individual device is required to establish a fiduciary relationship based on the above user authentication system with the others.

However, in order for each individual user having his own private PIN code to ensure the security of his own device, it is desirable to adopt a method involving creating a temporary PIN code and changing it to the original private PIN code at the termination of the table conferencing rather than establishing the fiduciary relationship by informing the other users of the private PIN code.

To adopt the user authentication system as described above, therefore, it is required to take the following steps:

S1: Each individual user sets up a temporary PIN code on his own device and informs the other users of that PIN code.

S2: Holds table conferencing.

S3: At the termination of the conferencing, each individual user makes a change from the temporary PIN code to his original private PIN code.

With the above approach, however, not only does it take long to set up the PIN code, but also the security level is considerably lowered in the event that the user forgot to make a change from the PIN code to the original PIN code; for, in such case, the temporary PIN code will come to be used successively.

BRIEF SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a radio communication device and a user authentication method for use therewith which permit the security level to be changed with flexibility according to communication situations without imposing any operating burden on users.

According to one aspect of the present invention, there is provided an authentication processing apparatus of a radio communication which authenticates a device, the apparatus comprising: means for selecting a security level from a plurality of security levels in accordance with a condition of the radio communication;

means for receiving a request for an authentication and authentication information from the device; means for checking whether the received information from the device

is valid or not depending on the selected security level; and means for sending a response of the check result which authenticates or rejects the device thereto.

According to another aspect of the present invention, there is provided a radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising: password holding means for holding at least a first password intended for temporary use and a second password intended for regular use; password selecting means for selecting an appropriate password from the password holding means according to a current communication condition; and password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the another device.

According to still another aspect of the present invention, there is provided a n authentication processing method of a radio communication which authenticates a device, the method comprising the steps of: selecting a security level from a plurality of security levels in accordance with a condition of the radio communication; receiving a request for an authentication from the device; receiving authentication information from the device; checking whether the received information from the device is valid or not depending on the selected security level; and sending a response of the check result which authenticates or rejects the device thereto.

According to still another aspect of the present invention, there is provided a radio communication method communicating with a device, the method comprising the steps of: storing a first password intended for temporary use and a second password intended for regular use; selecting the first password depending on a variable security level; receiving a request for a connection from the device; receiving a password for an authentication from the device; checking whether the received password from the device and the selected first password correspond or not; sending a response of the check result which authenticates or rejects the device thereto; performing a low-security-level communication with the authenticated device based on the connection; and changing over, when the communication is terminated, the security level to higher one than that of the first password and selecting the second password.

Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instrumentalities and combinations particularly pointed out hereinafter.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention, and together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principles of the invention.

FIG. **1** is a block diagram of a radio communication device according to an embodiment of the present invention;

FIG. **2** is a diagram for use in explanation of device-to-device communication in the embodiment;

FIG. **3** illustrates the flow of processing from a request for connection to the completion of authentication in the embodiment;

FIG. **4** is a flowchart for switching between a temporary password and a private password in the embodiment;

FIG. **5** is a diagram for use in explanation of how conferencing passwords are selected in an electronic conferencing system;

FIG. **6** is a diagram for use in explanation of management of passwords of slave stations through ID information of a master station in a radio communication system composed of multiple radio communication devices;

FIG. **7** is a flowchart for user authentication in the Bluetooth system; and

FIG. **8** shows the contents of the table used in the user authentication processing shown in FIG. **7**.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** is a block diagram of a radio communication device according to an embodiment of the present invention, which comprises a data transmitting and receiving section **11**, an antenna **12**, a connection-break detecting section **13**, an external factor acquisition section **14**, a time control section **15**, a password holding section, a password management section **17**, a password selecting section, a password checking section **19**, and an authentication password input section **20**. User events **21** are applied to the password management section **17**, the password selecting section **18**, and the authentication password input section **20**.

The data transmitting and receiving section **11** makes radio communication with other devices through the antenna **12**, performs low-level framing and synchronous processing, and can perform error detection and correction as required.

The connection-break detecting section **13** examines data receiving conditions in the data transmitting and receiving section **11** to detect whether the device with which the connection has been set up lies outside the coverage area and presents the result to the password selecting section **18**. The connection-break detecting section **13** is also configured to allow the user to set arbitrarily parameters, such as timer values, receiving sensitivity, etc., for recognizing connection break, that is, to set optimum values so that the password is not readily switched to another one in the event of bad data receiving conditions. Although, in FIG. **1**, the connection-break detecting section **13** is provided independently, it may be incorporated into the external factor acquisition section **14**.

The external factor acquisition section **14** identifies external factors, for example, the presence or absence of AC power supply, the presence or absence of wireless connection, such as Bluetooth, IrDA, etc., or wired connection, such as USB, IEEE1394, etc., and controls the password selecting section **18** correspondingly.

The time control section **15** controls time information in terms of absolute time or relative time and, at the occurrence of timer runout, notifies the password selecting section **18** of it.

The password holding section **16** is a memory that stores a plurality of passwords for authenticating the device (e.g., two passwords: a temporary password and a private password). The temporary password is one which is valid only during the duration of connection with a certain device and intended for temporary use, whereas the private password is one which ensures high confidentiality to increase the security of the device and is intended for regular use. The password management section **17** is adapted to add new

passwords to the contents of the password holding section **16** or deleting existing passwords therefrom according to events **21** from the user.

The password selecting section **18** selects the most suitable password for current connection from among the passwords stored in the password holding section **16** according to the user events **21**, information acquired by the external factor acquisition section **14**, and information from the time control section **15** and sends it to the password checking section **19**. The password selecting section is configured to be able to establish priority among the user event **21**, the external factor acquisition section **14**, and the time control section **15**.

When operating on an external factor acquired by the external factor acquisition section **14**, the password selecting section **18** carries out a password changing operation dependent on the external factor, as follows:

(a) In the absence of AC power supply, i.e., when the device is battery-powered, the device is recognized as being in the mobile environment and hence the private password is chosen.

(b) When a cable is connected, the device is recognized as being in the indoor environment and as a result the temporary password is chosen.

(c) When no radio carrier signal is received from a server, the device is recognized as having moved from the office to the outside, in which case the private password is chosen.

The password checking section **19** checks the password determined by the password selecting section **18** with an authentication password sent from a person with which the connection has been set up, thus implementing appropriate user authentication. The authentication password input section **20** enters the authentication password into the data transmitting and receiving section **11** according to the user event **21**.

Next, the authentication operation according to the present embodiment will be described.

Suppose now that devices A and B are about to be connected together as shown in FIG. **2**. In this case, the authentication procedure is performed when the device A enters the authentication password for the device B.

As shown in FIG. **3**, first, the user at the device A makes a request for connection. In response to this, the data transmitting and receiving section **11** in the device A issues a request for connection and transmits information from the antenna **12** (step B**1**).

Upon receiving the connection request from the device A, the data transmitting and receiving section **11** in the device B examines the received data and, in the case of no problem, sends a message to establish connection to the device A(step B**2**). After that, the connection is set up between the devices A and B (step B**3**). The connection in this case means the connection in low-level layer (e.g., the situation in which a virtual network address has been set up) and does not necessarily means high application services.

After the connection has been set up, the authentication procedure on the password is carried out. That is, the device B upon setting up the connection issues a request for authentication to the device A and prompts it to enter a password (step B**4**). In response to this, the user at the device A enters the password to the device B from the password input section **20** into the data transmitting and receiving section **11** for transmission to the device B (step B**5**).

Upon receipt of the password, the device B checks it with an authentication password chosen by the password selecting section **18**. If the result indicates that the received password is improper, then the device B sends to the device A a message to the effect that the password is incorrect. If, on the other hand, the received password is correct, then the user authentication procedure comes to an end (step B**6**).

In the user authentication procedure, each individual user generally uses an authentication password having much increased confidentiality, thereby providing increased security for his own device. However, in applications of highly ad hoc nature, such as table conferencing, card exchange, etc., an easy-to-handle environment may be expected to be built up even if the security for devices is lowered temporarily. The procedure for implementing such an environment will be described below.

Consider now the case of card exchange with a complete stranger in a card exchange application installed in personal digital assistants (PDAs). In this case as well, user authentication is performed between the devices A and B.

The user at the device B generally uses a private password having much increased confidentiality as the authentication password so as to increase the security for his own device. However, to inform a stranger of the private password in such a situation as in this example is not desirable from the viewpoint of security. For this reason, the user at the device B sets up such a password (temporary password) as is valid only while the connection with the device A is set up and uses the temporary password for user authentication.

The switching control between the private password and the temporary password (security level control) will be described below with reference to a flowchart illustrated in FIG. **4**.

The user at the device B issues a command which is based on the event **21** to the password selecting section **18** (step C**1**) and then sets up the temporary password as the authentication password (step C**2**). After that, the device B is placed in the wait state until a connection request is generated from the device A (step C**3**). The temporary password is very simple one (e.g., "ABC") as compared with the private password and presented to the user at the device A. In an extreme case, communication could be made between the devices A and B with no password. Making the temporary password simple as described above will make it possible to notify the user at the device A of the temporary password orally. Additionally, the temporary password may be sent to the device A along with electronic mail.

The user at the device A received notification from the device B makes a request to the device for connection and enters the temporary password.

In response to the connection request by the device A, the device B sets up the connection with the device A and then carries out authentication processing on the temporary password. After that, the devices A and B make data communications with each other on the card exchange application.

The device B makes a check for the termination of the card exchange application, i.e., for the break of the connection with the device A (step C**5**). Upon detecting the break of the connection, the device B negates the validity of the temporary password and makes an automatic change from the temporary password to the private password (step C**6**).

One method to automatically make a change from the temporary password to the private password is to associate the lifetime of the temporary password with the lifetime of the communication connection as will be described below.

That is, in FIG. **1**, at the time of a break of the connection set up with the current temporary password the connection

break detecting section **13** notifies the password selecting section **18** that the connection has been broken. The password selecting section then makes a change from the currently selected password to the private password.

The temporary password may be associated with time information using the time control section **15** rather than with the connection. In this case, a timer value for the temporary password can be freely set by the user in the time control section **15**. For example, if there is a two-hour conference, then the temporary password is used for two hours and changed to the private password two hours later.

A password which is to be made valid at present is usually chosen by the user through the graphical user interface (GUI). Alternatively, the password may be chosen by an operation of double clicking a password file. For example, in using an application such as an electronic conferencing system, a method can be utilized by which a password file **26** storing information used for selecting a conferencing password is distributed beforehand from a device A to other devices B, C and D over a communication path such as for electronic mail **25** and conference participants are allowed to choose a conferencing password by merely double clicking the file. In this case, the password selecting section **18** chooses a password held in the password holding section **16** according to the information read from the password file **26**.

The use of the password file **26** allows an appropriate password to be chosen by a simple operation of double clicking that file with a mouse. Also, the use of the password file allows passwords to be set up without their contents becoming known to the conference participants.

The password file **26** may be stored with passwords themselves rather than password select information. In this case, a password selected from the file may be automatically set up as the authentication password.

The password file **26** may be distributed to devices through electronic mail by radio.

Next, in a radio communication system made up of a plurality of radio communication devices each having the above functions, the management of passwords of the slave devices through ID information of the master device will be described.

Switching is made between authentication passwords in order to, for example, lower the security level of an information device when it is inside an office so that anybody can make access to it and enhance the security level when it is outside the office to prevent access by a third party.

Specifically, as shown in FIG. **6**, a server (master device) **32** for managing the security level is installed in office **31** to detect whether an information device (slave device) **33** stays in the range of connection with the server through its connection break detecting section **13**. In the situation where the information device **33** is connected with the server **32**, a temporary password (or no password) is selected. In the situation where the connection with the server is broken, the private password is chosen.

The above configuration causes the server **32** to act as the key to password switching.

Although the embodiment has been described in terms of one-way authentication between the devices A and B, mutual authentication is also possible.

According to the present invention, as described in detail above, a radio communication device adapted to perform a authentication procedure on another device using its unique address is configured to hold at least two separate passwords of a temporary password and a private password and make a choice from the two passwords for the procedure of authenticating the other device according to the current communication situations. Accordingly, depending upon what application is used, an appropriate password can be used for authentication and an easy-to-handle communication environment can be implemented in which a high level of security can be maintained at the time of usual communication and the security level can be lowered at the time of temporary communication.

Moreover, the inventive device is configured to usually choose the private password as authentication password, use the temporary password at the time of occurrence of a request by a user at another device for authentication thereof, and reuse the private password after the connection set up by the authentication procedure using the temporary password has been broken; therefore, there is no need for users to be conscious of a change from the temporary password to the private password.

Furthermore, the inventive device is configured to have external factor acquisition means, choose either of the temporary password and the private password for authentication of another device on the basis of information acquired by the external factor acquisition means; thus, the most suitable password can be automatically chosen according to communication situations.

In addition, the inventive device is configured to acquire position information of the device by external factor acquisition means or connection break detecting means and allow switching between the temporary password and the private password according to the position information; thus, the security level of the device can be changed automatically according to its location.

Additional advantages and modifications will readily occur to those skilled in the art. Therefore, the invention in its broader aspects is not limited to the specific details and representative embodiments shown and described herein. Accordingly, various modifications may be made without departing from the spirit or scope of the general inventive concept as defined by the appended claims and their equivalents.

What is claimed is:

1. An authentication processing apparatus of a radio communication which authenticates a device, the apparatus comprising:

means for acquiring an external factor which is associated with a security level;

means for selecting a security level from a plurality of security levels in accordance with the external factor;

means for receiving a request for an authentication and authentication information from the device;

means for checking whether the received information from the device is valid or not depending on the selected security level; and

means for sending a response of the check result which authenticates or rejects the device thereto.

2. An authentication processing apparatus according to claim **1**, wherein said authentication information includes a PIN (Personal Identification Number) code.

3. An authentication processing apparatus according to claim **2**, further comprising means for storing a link-key comprising said PIN code and a unique ID of said device.

4. An authentication processing apparatus according to claim **1**, further comprising means for detecting a connection-break from the device and changing over said security level in response to the connection-break.

5. A radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising:

password holding means for holding at least a first password intended for temporary use and a second password intended for regular use;

password selecting means for selecting an appropriate password from the password holding means according to a current communication condition; and

password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the other device.

6. The radio communication device according to claim **5**, wherein said password selecting means selects a password according to information from a password file.

7. A radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising:

password holding means for holding at least a first password intended for temporary use and a second password intended for regular use;

password management means for entering a new password into the password holding means and deleting an existing password in the password holding means;

password selecting means for selecting an appropriate password from the password holding means according to current communication situations; and

password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the other device.

8. A radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising:

password holding means for holding at least a first password intended for temporary use and a second password intended for regular use;

password selecting means for selecting an appropriate password from the password holding means according to current communication situations;

password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the other device; and

connection break detecting means for detecting radio communication conditions and, upon detecting a connection break as a result of the device having moved to the outside of a communication service area, notifying the password selecting means of the connection break,

the password selecting means usually choosing the second password as an authentication password, using the first password at the time of occurrence of a request by a user at the other device as the authentication password, and reusing the second password after the connection set up by the authentication procedure using the first password has been broken.

9. The radio communication device according to claim **8**, wherein the connection break detecting means includes means for setting parameters containing timer values and receiving sensitivity for recognizing the connection break.

10. A radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising:

password holding means for holding at least a first password intended for temporary use and a second password intended for regular use;

external factor acquisition means;

password selecting means for selecting an authentication password from the password holding means on the basis of information acquired by the external factor acquisition means; and

password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the other device.

11. A radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising:

password holding means for holding at least a first password intended for temporary use and a second password intended for regular use;

password selecting means for selecting an appropriate password from the password holding means according to current communication situations;

password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the other device; and

time control means for counting time to provide management information on a set time to the password selecting means,

the password selecting means usually choosing the second password as an authentication password, using the first password at the time of occurrence of a request by a user at the other device as the authentication password, and setting the second password as the authentication password at the expiration of the time set by the time management means.

12. A radio communication device having a password unique to it and adapted for authenticating another device by use of the password, comprising:

password holding means for holding at least a first password intended for temporary use and a second password intended for regular use;

password selecting means for selecting an appropriate password from the password holding means according to current communication situations; and

password checking means for checking a password sent from another device with the password selected by the password selecting means to thereby authenticate the other device,

each of the devices acting as slave stations recognizing information unique to a master station, selecting one of the first and second passwords in a state where it can communicate with the master station, and selecting the other password in a state where it cannot communicate with the master station.

13. An authentication processing method of a radio communication which authenticates a device, the method comprising:

selecting a security level from a plurality of security levels in accordance with a condition of the radio communication;

receiving a request for an authentication from the device;

receiving authentication information from the device;

checking whether the received information from the device is valid or not depending on the selected security level; and

sending a response of the check result which authenticates or rejects the device thereto.

14. An authentication processing method according to claim **13**, wherein said authentication information includes a PIN (Personal Identification Number) code.

15. An authentication processing method according to claim **14**, further comprising the step of storing a link-key comprising said PIN code and a unique ID of said device.

16. An authentication processing method according to claim **13**, further comprising the step of acquiring an external factor which is associated with said security level.

17. A radio communication method communicating with a device, the method comprising:

storing a first password intended for temporary use and a second password intended for regular use;

acquiring an external factor which is associated with a variable security level;

selecting the first password depending on a variable security level;

receiving a request for a connection from the device;

receiving a password for an authentication from the device;

checking whether the received password from the device and the selected first password correspond or not;

sending a response of the check result which authenticates or rejects the device thereto;

performing a low-security-level communication with the authenticated device based on the connection; and

changing over, when the communication is terminated, said security level to a higher one than that of said first password and selecting said second password.

18. A radio communication method according to claim **17**, wherein said second password includes a PIN (Personal Identification Number) code.

19. A radio communication method according to claim **18**, further comprising the step of storing a link-key comprising said PIN code and a unique ID of said device.

* * * * *

EXHIBIT 3

US007127210B2

(12) **United States Patent**
Aoyagi

(10) **Patent No.: US 7,127,210 B2**
(45) **Date of Patent: Oct. 24, 2006**

(54) **WIRELESS COMMUNICATION APPARATUS**

(75) Inventor: **Kazunori Aoyagi**, Fussa (JP)

(73) Assignee: **Kabushiki Kaisha Toshiba**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 576 days.

(21) Appl. No.: **10/096,678**

(22) Filed: **Mar. 14, 2002**

(65) **Prior Publication Data**

US 2003/0114107 A1 Jun. 19, 2003

(30) **Foreign Application Priority Data**

Sep. 20, 2001 (JP) 2001-287376

(51) **Int. Cl.**
H04B 7/00 (2006.01)

(52) **U.S. Cl.** **455/41.2**; 455/403; 455/417; 370/259; 370/260; 370/261

(58) **Field of Classification Search** 455/403, 455/450, 410, 41.2, 41.3, 416, 417; 370/259, 370/260, 261, 262, 263, 264, 265, 266, 267, 370/268, 269, 270
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2002/0164953 A1* 11/2002 Curtis 455/41
2003/0054794 A1* 3/2003 Zhang 455/403

FOREIGN PATENT DOCUMENTS

JP 2000-209646 7/2000
JP 2001-189974 7/2001
JP 2000-018082 1/2002

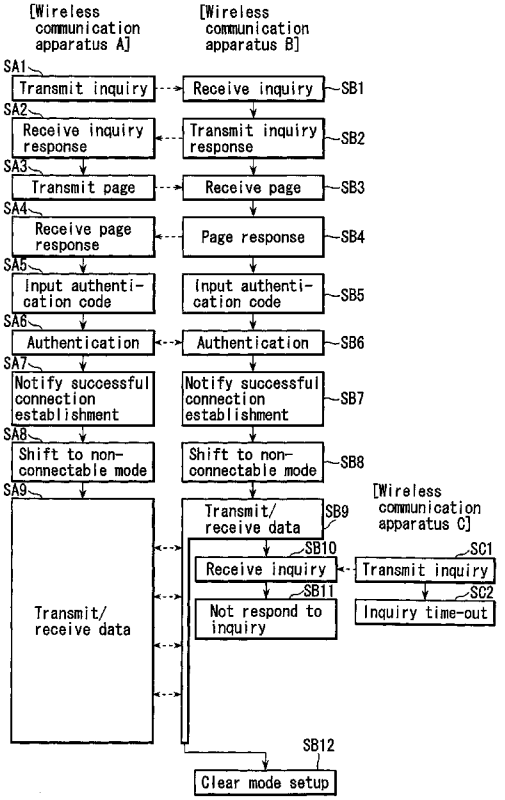
* cited by examiner

Primary Examiner—Matthew D. Anderson
Assistant Examiner—Sanh Phu
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett & Dunner. L.L.P.

(57) **ABSTRACT**

This invention relates to a wireless communication apparatus including a discovery unit which discovers the completion of connection with another wireless communication apparatus, a mode setup unit which sets up a mode which defines processing for a signal for performing communication with the wireless communication apparatus from a wireless communication apparatus except for another wireless communication apparatus, and a shift unit which shifts to the mode set up by the mode setup unit when the discovery unit discovers the completion of connection.

21 Claims, 5 Drawing Sheets



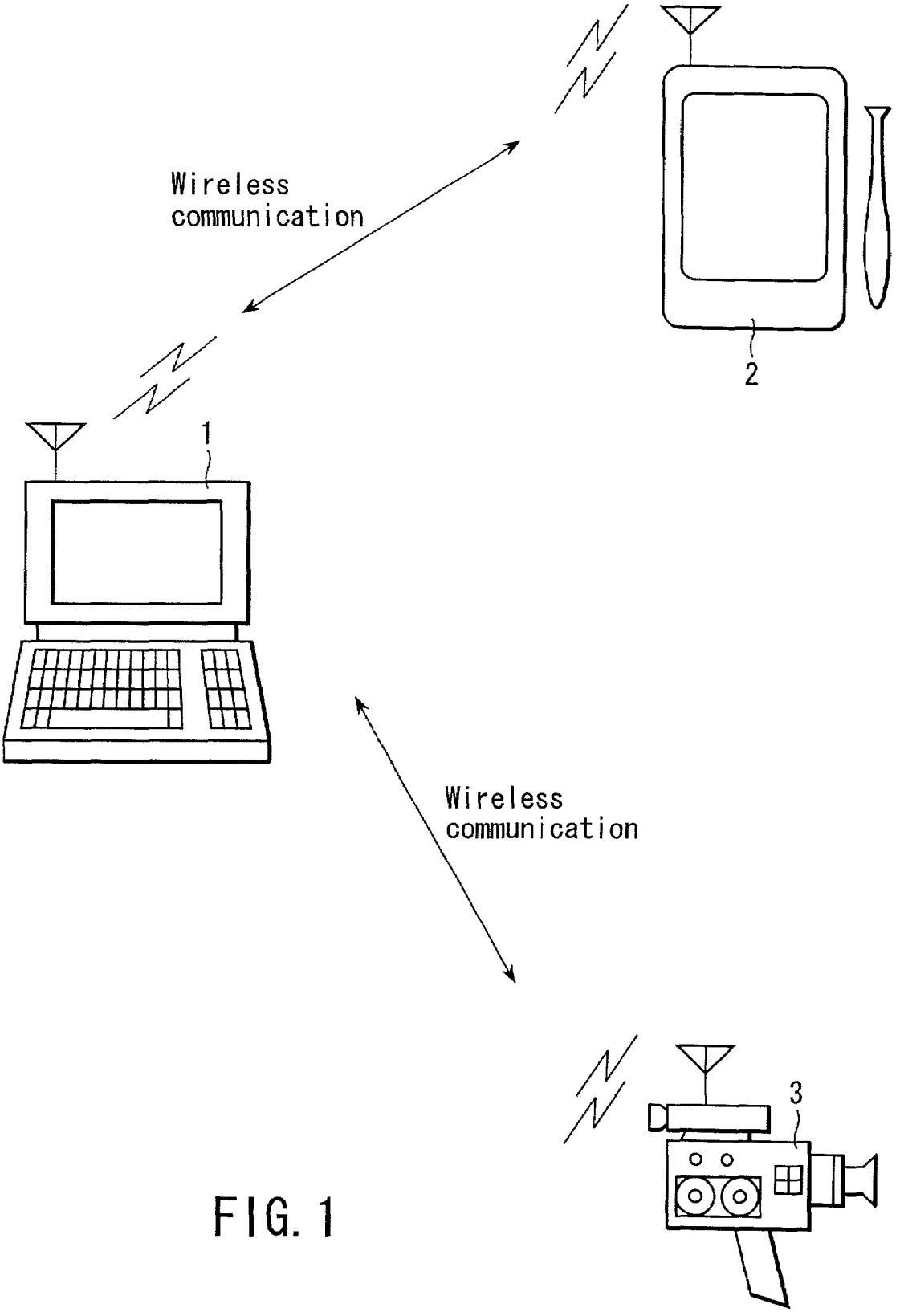


FIG. 1

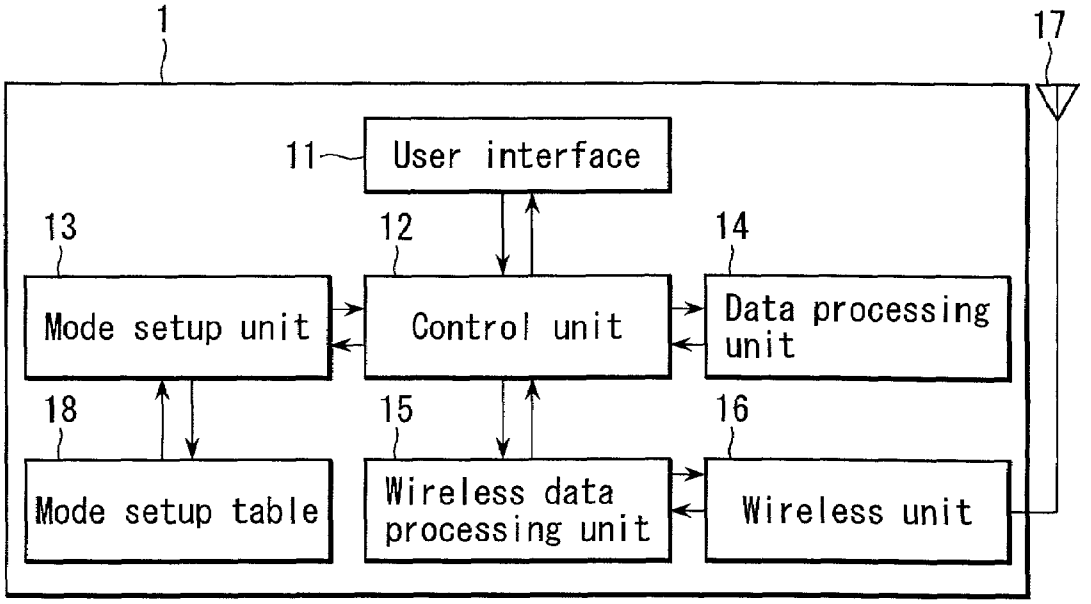


FIG. 2

Unique address	Mode selected upon connection establishment
Unique address A	Non-connectable mode 1
Unique address B	Non-discoverable mode
Unique address C	Non-connectable mode 2
Unique address D	Non-discoverable mode
Unique address E	Non-connectable mode 1
⋮	⋮

FIG. 3

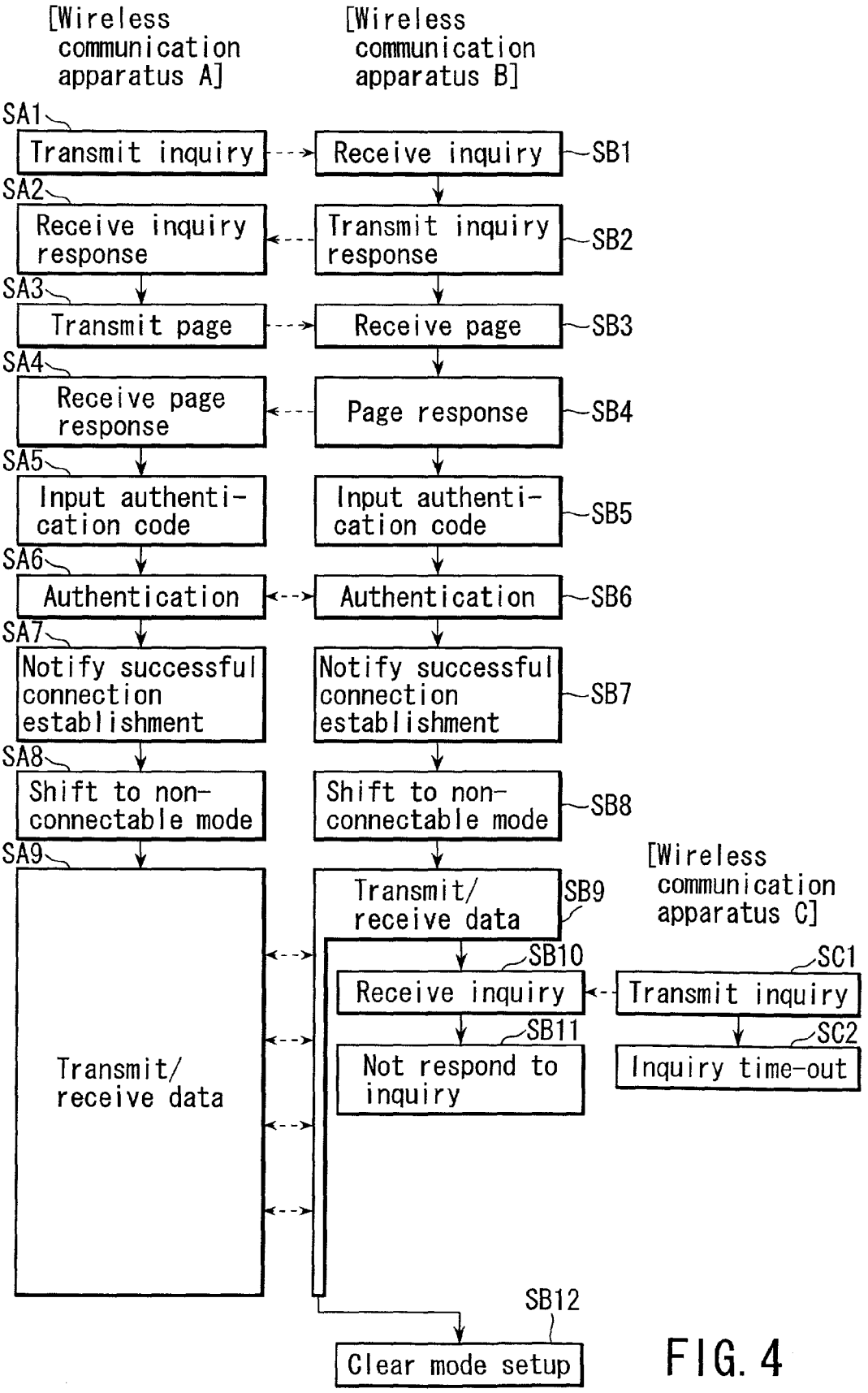

[Wireless communication apparatus A]
[Wireless communication apparatus B]
SA1
Transmit inquiry
Receive inquiry
SB1
SA2
Receive inquiry response
Transmit inquiry response
SB2
SA3
Transmit page
Receive page
SB3
SA4
Receive page response
Page response
SB4
SA5
Input authentication code
Input authentication code
SB5
SA6
Authentication
Authentication
SB6
SA7
Notify successful connection establishment
Notify successful connection establishment
SB7
SA8
Shift to non-connectable mode
Shift to non-connectable mode
SB8
SA9
Transmit/ receive data
Transmit/ receive data
SB9
[Wireless communication apparatus C]
SB10
Receive inquiry
SC1
Transmit inquiry
SB11
Not respond to inquiry
SC2
Inquiry time-out
SB12
Clear mode setup

FIG. 4

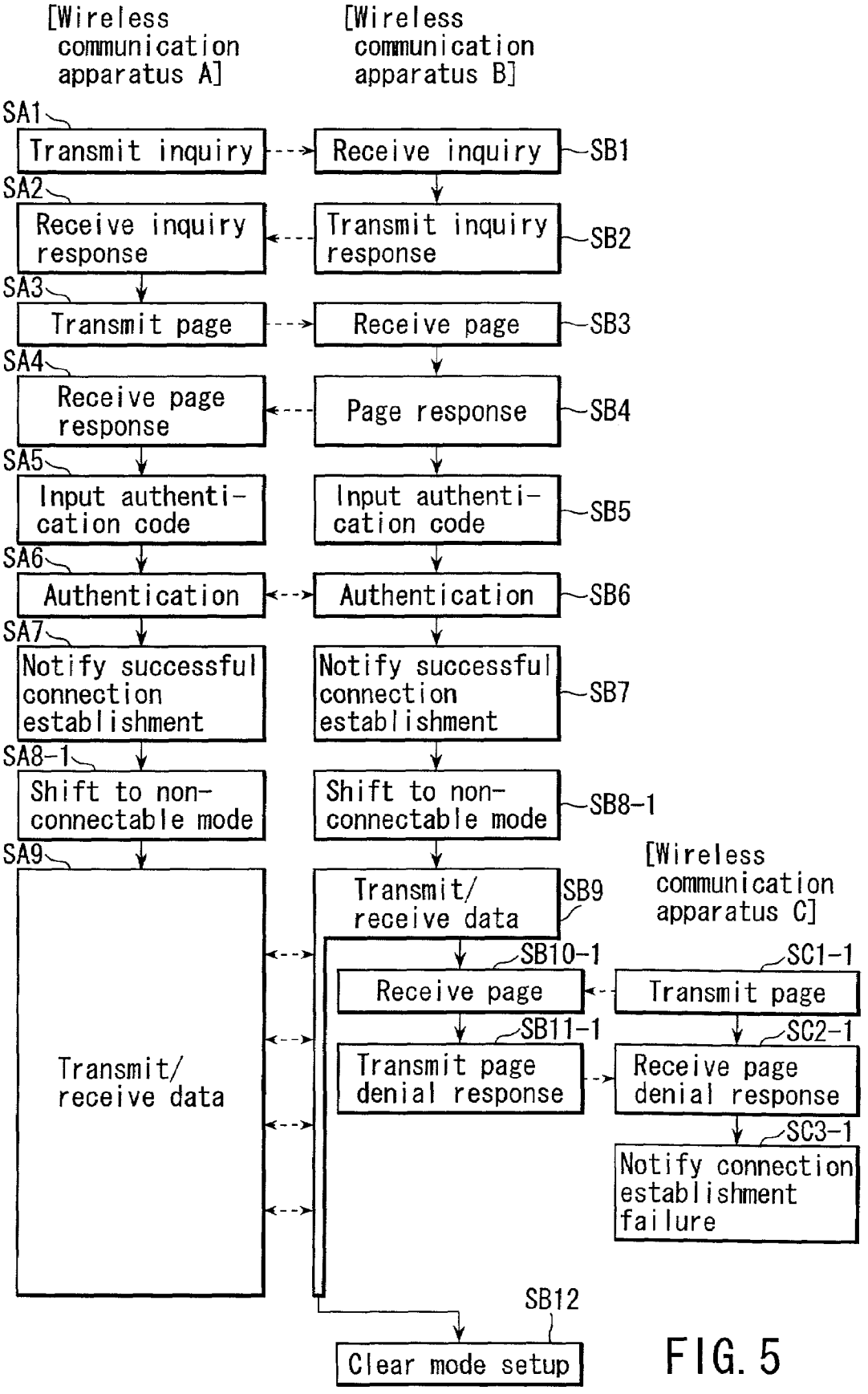

[Wireless communication apparatus A]
[Wireless communication apparatus B]
SA1
Transmit inquiry
Receive inquiry
SB1
SA2
Receive inquiry response
Transmit inquiry response
SB2
SA3
Transmit page
Receive page
SB3
SA4
Receive page response
Page response
SB4
SA5
Input authentication code
Input authentication code
SB5
SA6
Authentication
Authentication
SB6
SA7
Notify successful connection establishment
Notify successful connection establishment
SB7
SA8-1
Shift to non-connectable mode
Shift to non-connectable mode
SB8-1
SA9
Transmit/ receive data
Transmit/ receive data
SB9
[Wireless communication apparatus C]
SB10-1
Receive page
SC1-1
Transmit page
SB11-1
Transmit page denial response
SC2-1
Receive page denial response
SC3-1
Notify connection establishment failure
SB12
Clear mode setup

FIG. 5

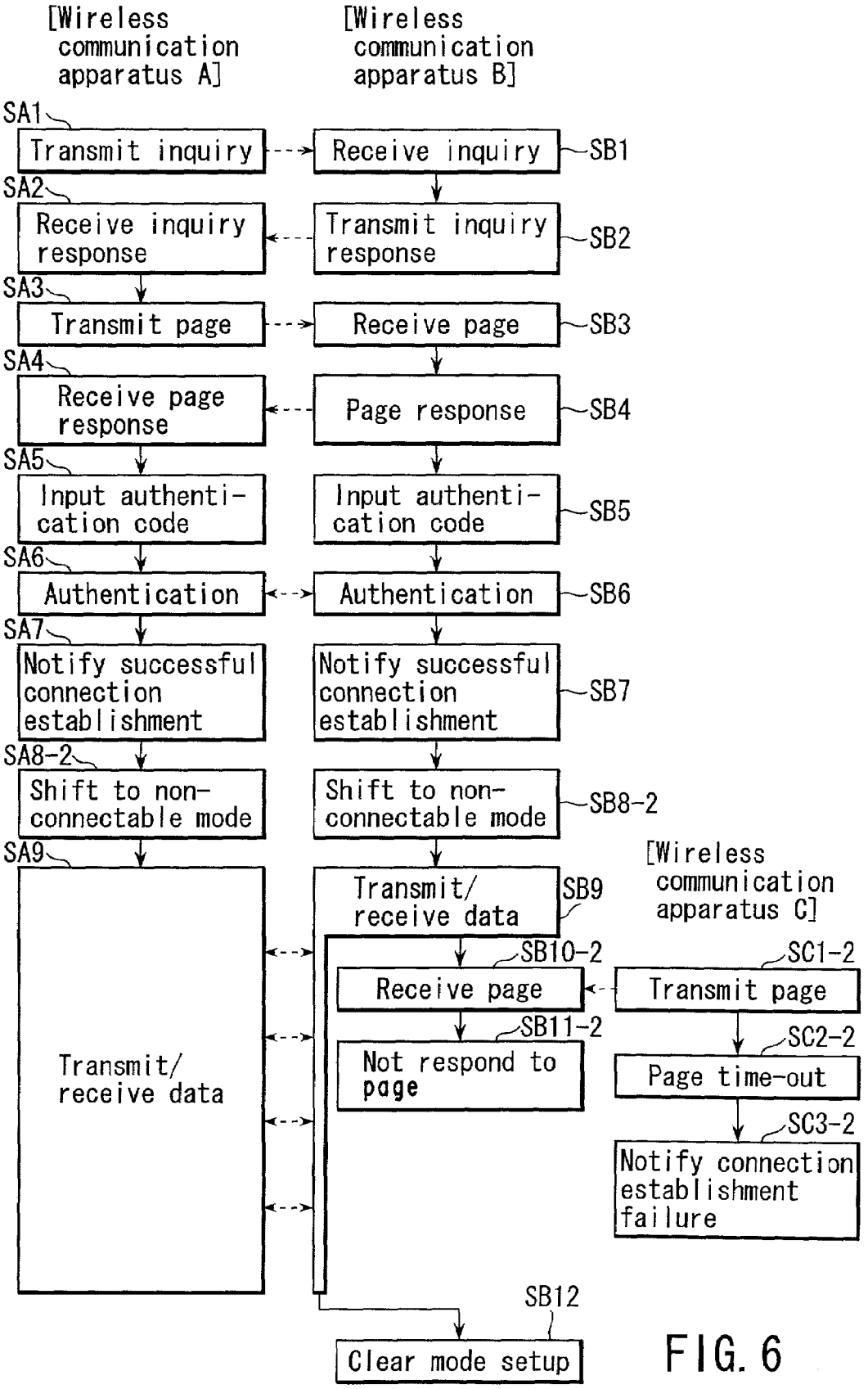

[Wireless communication apparatus A]
[Wireless communication apparatus B]
[Wireless communication apparatus C]
SA1
Transmit inquiry
Receive inquiry
SB1
SA2
Receive inquiry response
Transmit inquiry response
SB2
SA3
Transmit page
Receive page
SB3
SA4
Receive page response
Page response
SB4
SA5
Input authentication code
Input authentication code
SB5
SA6
Authentication
Authentication
SB6
SA7
Notify successful connection establishment
Notify successful connection establishment
SB7
SA8-2
Shift to non-connectable mode
Shift to non-connectable mode
SB8-2
SA9
Transmit/ receive data
Transmit/ receive data
SB9
SB10-2
Receive page
SB11-2
Not respond to page
SC1-2
Transmit page
SC2-2
Page time-out
SC3-2
Notify connection establishment failure
SB12
Clear mode setup

FIG. 6

WIRELESS COMMUNICATION APPARATUS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims the benefit of priority from the prior Japanese Patent Application No. 2001-287376, filed Sep. 20, 2001, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a wireless communication apparatus and, more particularly, to a wireless communication apparatus which, after establishing connection with another wireless communication apparatus, automatically changes setups for discovery or connection with respect to still another wireless communication apparatus except for the connected wireless communication apparatus.

2. Description of the Related Art

The Bluetooth technique capable of achieving short-distance wireless communication between a plurality of wireless communication apparatuses has recently been developed along with the development of the wireless communication technology. An example of techniques adopting the Bluetooth technique is Jpn. Pat. Appln. KOKAI Publication No. 2001-189974.

Regarding the process up to establishing connection between wireless communication apparatuses in Bluetooth which is one of wireless communication schemes, the prior art reads,

"To communicate with another device, a given device makes an inquiry to check whether a device equipped with Bluetooth exists in a range where its radio waves can reach. The device checks an inquiry from another device by inquiry scan, and responds to the inquiry by an inquiry response function. The device can know the 48-bit address of the partner through an inquiry response which transmits an FHS (Frequency Hopping Synchronization) packet. Connection is set between these devices by the address. The paging device which wants to set connection starts a page process by using a specific address. At this time, the paged device periodically performs page scan. Since the normal page period is longer than the page scan period, the paged device can set connection with the paging device Upon recognizing through page scan that it has been paged, the paged device immediately starts a process of setting connection. In a normal state, connection is set."

As described above, when wireless communication apparatuses are to communicate with each other, the first wireless communication apparatus which wants to perform wireless communication sends an inquiry signal to peripheral wireless communication apparatuses. The second wireless communication apparatus which has received the inquiry signal sends back a response to the first wireless communication apparatus. The first wireless communication apparatus receives the response to the inquiry, and discovers the wireless communication apparatus which exists near itself. To request connection, the first wireless communication apparatus sends a page signal to the second wireless communication which has sent back the response. Then, the second wireless communication apparatus receives the page signal, and sends back a page response to the first wireless communication apparatus. Connection between the wireless communication apparatuses is established through this process, and wireless communication is enabled.

Bluetooth assumes that a wireless communication apparatus establishes connections with a plurality of wireless communication apparatuses and communicates with them. Even if a wireless communication apparatus establishes connection with another wireless communication apparatus and does not want to be connected to still another wireless communication apparatus, the wireless communication apparatus performs response processing to an inquiry or page sent from still another wireless communication apparatus. This may interfere with communication with the currently connected wireless communication apparatus.

When authentication is set to be performed in connection, the wireless communication apparatus is prompted to input an authentication code every time it receives a page from another wireless communication apparatus. This forces the user to perform an unwanted operation.

BRIEF SUMMARY OF THE INVENTION

An object of the present invention is to provide a communication apparatus which, after establishing connection with a wireless communication apparatus, controls connection establishment with another wireless communication apparatus.

To achieve the above object, according to a first aspect of the invention, there is provided a communication apparatus comprising means for discovering completion of connection with another wireless communication apparatus, mode setup means for setting up a mode which defines processing for a signal for performing communication with the wireless communication apparatus from a wireless communication apparatus except for the another wireless communication apparatus, and means for shifting to the mode set up by the mode setup means when the discovery means discovers the completion of connection.

According to a second aspect of the invention, there is provided a communication method in a communication apparatus, comprising discovering completion of connection with another wireless communication apparatus and inhibiting connection with a wireless communication apparatus except for the another wireless communication apparatus.

According to the present invention, after a wireless communication apparatus establishes communication with another wireless communication apparatus, it can inhibit communication with still another wireless communication apparatus except for the currently connected wireless communication apparatus. This can prevent interference with communication with the connected wireless communication apparatus.

Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instrumentalities and combinations particularly pointed out hereinafter.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention, and together with the general description given above and the detailed description of the embodiments given below, serve to explain the principles of the invention.

FIG. **1** is a view showing an example of the use environment of a wireless communication apparatus according to an embodiment of the present invention;

FIG. **2** is a functional block diagram showing a notebook type personal computer **1** as a wireless communication apparatus;

FIG. **3** is a table showing a mode setup table representing the relationship between a unique address and a mode selected upon connection establishment;

FIG. **4** is a flow chart for explaining the operation of the notebook type personal computer according to the first embodiment of the present invention;

FIG. **5** is a flow chart for explaining the operation of a wireless communication apparatus according to the second embodiment of the present invention; and

FIG. **6** is a flow chart for explaining the operation of a wireless communication apparatus according to the third embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

First Embodiment

A wireless communication apparatus according to an embodiment of the present invention will be described below with reference to the several views of the accompanying drawing.

FIG. **1** is a view showing an example of the use environment of the wireless communication apparatus according to the embodiment of the present invention. In FIG. **1**, a notebook type personal computer **1**, PDA (Personal Digital Assistant) **2**, and VTR camera **3** have Bluetooth modules, and are in a wireless communicable environment.

FIG. **2** is a functional block diagram showing the notebook type personal computer **1** as a wireless communication apparatus. Although FIG. **2** shows the notebook type personal computer **1**, the PDA **2** and VTR camera **3** as other wireless communication apparatuses also have the same functions.

As shown in FIG. **2**, the notebook type personal computer **1** comprises a user interface **11**, control unit **12**, mode setup unit **13**, data processing unit **14**, wireless data processing unit **15**, wireless unit **16**, and antenna **17**.

The user interface **11** receives an inquiry or paging from the user, and sends the command to the control unit **12**.

The control unit **12** sends the command from the user interface **11** as control data to the wireless data processing unit **15**. The control unit **12** checks whether the received data which is demodulated and output from the wireless data processing unit **15** is control data or general data, and executes processing corresponding to the received data. If the received data is general data, the control unit **12** sends it to the data processing unit **14** which performs data processing.

If the received data is control data, the control unit **12** sends back corresponding control data to the wireless data processing unit **15**, and sends the control information to the user interface **11** and mode setup unit **13**.

The wireless data processing unit **15** modulates the control data and sends it to the wireless unit **16**. The control data is transmitted to another wireless communication apparatus by generating radio waves from the antenna **17**. The wireless data processing unit **15** demodulates received data and sends it to the control unit **12**.

The wireless unit **16** uses the antenna **17** to receive radio waves generated from another wireless communication apparatus, and sends them to the wireless data processing unit **15**.

When the mode setup unit **13** receives control data representing the completion of connection with another wireless communication apparatus, the mode setup unit **13** automatically changes setups for an inquiry or paging from still another wireless communication apparatus.

The setups of the mode are done for a mode setup table **18** representing the relationship between a unique address and a mode selected upon connection establishment, as shown in FIG. **3**.

In FIG. **3**, when connection with a device corresponding to unique address A is established, this means that the mode changes to non-connectable mode **1**. When connection with a device corresponding to unique address B is established, this means that the mode changes to a non-discoverable mode.

The non-connectable mode and non-discoverable mode are defined by the Bluetooth standard. The "non-connectable mode" in which the wireless communication apparatus does not respond to a page signal from another wireless communication apparatus means that the wireless communication apparatus does not change to a page scan state. The non-discoverable mode in which the wireless communication apparatus does not respond to an inquiry signal from another wireless communication apparatus means that the wireless communication apparatus does not change to an inquiry signal response state.

The Bluetooth standard defines two types of non-connectable modes because the wireless communication apparatus either does not respond to a page or sends back a page denial upon reception of a page signal (to be described later).

When received data demodulated by the wireless data processing unit **15** concerns an inquiry or paging from another wireless communication apparatus, the control unit **12** sends a response to the inquiry or paging from the wireless communication apparatus to the wireless data processing unit **14** on the basis of a mode set up by the mode setup unit **13**.

The operation of the notebook type personal computer according to the first embodiment of the present invention will be explained with reference to the flow chart of FIG. **4**. In FIG. **4**, the notebook type personal computer **1** is described as a wireless communication apparatus A; the PDA **2**, as a wireless communication apparatus B; and the VTR camera **3**, as a wireless communication apparatus C.

The user of the wireless communication apparatus A which is to start wireless communication instructs the control unit **12** through the user interface **11** to check wireless communication apparatuses present around the wireless communication apparatus A. The control unit **12** generates inquiry data upon reception of the request through the user interface **11**. The inquiry data is sent to the wireless data processing unit **15** where it is modulated. The modulated inquiry data is sent to the wireless unit **16** and transmitted from the antenna **17** (SA**1**).

The wireless communication apparatus B receives the inquiry transmitted from the wireless communication apparatus A, and outputs the received inquiry from the wireless unit **16** to the wireless data processing unit **15**. The wireless data processing unit **15** demodulates the received inquiry and sends it to the control unit **12** (SB**1**).

The control unit **12** of the wireless communication apparatus B determines that the inquiry has been received. Then, the control unit **12** generates inquiry response data including

the unique address of the wireless communication apparatus B and sends it to the wireless data processing unit **15**. The wireless data processing unit **15** modulates the inquiry response data and sends the modulated inquiry response data to the wireless unit **16**. The inquiry response data is transmitted from the antenna **17** (SB**2**).

The wireless communication apparatus A receives by the antenna **17** the inquiry response transmitted from the wireless communication apparatus B. The received inquiry response is sent from the wireless unit **16** to the wireless data processing unit **15**. The wireless data processing unit **15** modulates the received inquiry response and sends it to the control unit **12**. The control unit **12** determines that the inquiry response has been received (SA**2**), and sends unique address information of the wireless communication apparatus B included in the received inquiry response to the user interface **11**. The user interface **11** displays the unique address information of the wireless communication apparatus B.

The user of the wireless communication apparatus A which wants connection with the wireless communication apparatus B designates the unique address of the wireless communication apparatus B as a destination through the user interface **11**, and sends a paging signal to the control unit **12**. The control unit **12** generates page data to the wireless communication apparatus B and sends it to the wireless data processing unit **15**. The page data modulated by the wireless data processing unit **15** is sent to the wireless unit **16** and transmitted from the antenna **17** (SA**3**).

The wireless communication apparatus B receives by the antenna **17** the page transmitted from the wireless communication apparatus A. The received page is demodulated by the wireless data processing unit **15** and sent to the control unit **12**. The control unit **12** determines that the page has been received (SB**3**). The control unit **12** generates page response data and sends it to the wireless data processing unit **15**. The page response data modulated by the wireless data processing unit **15** is sent to the wireless unit **16** and transmitted from the antenna **17** (SB**4**).

The wireless communication apparatus A receives by the antenna **17** the page response transmitted from the wireless communication apparatus B. The received page response is demodulated by the wireless data processing unit **15** and sent to the control unit **12**. The control unit **12** determines that the page response has been received (SA**4**). If authentication is necessary, the control unit **12** causes the user interface **11** to display an authentication code input request. The user of the wireless communication apparatus A inputs the authentication code (SA**5**). The wireless communication apparatus A exchanges the authentication data with the wireless communication apparatus B and performs authentication (SA**6**).

After the wireless communication apparatus B transmits the page response, it causes the user interface **11** to display an authentication code input request if authentication with the wireless communication apparatus A is necessary. The user of the wireless communication apparatus B inputs the authentication code (SB**5**). The wireless communication apparatus B exchanges the authentication data with the wireless communication apparatus A and performs authentication (SB**6**).

If authentication in steps SA**6** and SB**6** succeeds, the wireless communication apparatuses A and B determine that connection is established, and send connection establishment information to their user interfaces **11**. The user interfaces **11** of the respective wireless communication apparatuses notify the users of the wireless communication apparatuses of connection establishment (SA**7** and SB**7**).

If the control unit **12** determines in step SA**7** in the wireless communication apparatus A or in step SB**7** in the wireless communication apparatus B that connection has been established, the control unit **12** notifies the mode setup unit **13** of connection establishment. In the wireless communication apparatus A, the mode setup unit **13** sends to the control unit **12** an instruction for shifting to the non-discoverable mode, in accordance with a mode setup set in the mode setup table **18** in advance. Similarly in the wireless communication apparatus B, the mode setup unit **13** sends to the control unit **12** an instruction for shifting to the non-discoverable mode. Note that the mode setup tables **18** of the wireless communication apparatuses A and B are so set as to shift the mode to the non-discoverable mode when connection is established between the wireless communication apparatuses A and B. After connection is established between the wireless communication apparatuses A and B, the mode automatically shifts to the non-discoverable mode (SA**8** and SB**8**). After connection establishment, data is exchanged between the wireless communication apparatuses A and B (SA**9** and SB**9**).

If the third wireless communication apparatus C wants connection with the wireless communication apparatus B, the wireless communication apparatus C transmits an inquiry in step SC**1** similarly to step SA**1** of the wireless communication apparatus A.

In step SB**10**, the wireless communication apparatus B receives the inquiry from the wireless communication apparatus C by the same procedure as that in step SB**1**. The wireless communication apparatus B has received the inquiry from the wireless communication apparatus C, but the control unit **12** does not generate any response data to the inquiry because the wireless communication apparatus B has shifted to the non-discoverable mode. In step SB**11**, the wireless communication apparatus B does not transmit any inquiry response.

Since the wireless communication apparatus C cannot receive any inquiry response from the wireless communication apparatus B, it cannot discover the wireless communication apparatus B. In step SC**2**, an inquiry time-out occurs. The wireless communication apparatus C cannot acquire the unique address of the wireless communication apparatus B, and cannot request connection. The wireless communication apparatus C does not interfere with data transmission/reception between the wireless communication apparatuses A and B in steps SA**9** and SB**9**.

After data transmission/reception between the wireless communication apparatuses A and B in steps SA**9** and SB**9** ends, the mode setup, i.e., non-discoverable mode is cleared in the wireless communication apparatus B (SB**12**). The wireless communication apparatus B shifts to a normal mode.

The wireless communication apparatus according to the first embodiment shifts to the non-discoverable mode after connection establishment. This can prevent interference with communication with a connected wireless communication apparatus.

Second Embodiment

The operation of a wireless communication apparatus according to the second embodiment of the present invention will be described with reference to the flow chart of FIG. **5**.

The process up to establishing connection between wireless communication apparatuses A and B, i.e., the process from step SA**1** to step SA**7** and from step SB**1** to step SB**7** is the same as that shown in FIG. **4**.

If a control unit **12** determines in step SA**7** in the wireless communication apparatus A or in step SB**7** in the wireless communication apparatus B that connection has been established, the control unit **12** notifies a mode setup unit **13** of connection establishment. In the wireless communication apparatus A, the mode setup unit **13** sends, to the control unit **12** in accordance with a preset mode setup, an instruction for shifting to the non-connectable mode in which the wireless communication apparatus A sends a denial response to the received page. Also in the wireless communication apparatus B, the mode setup unit **13** sends to the control unit **12** an instruction for shifting to the non-connectable mode in which the wireless communication apparatus B sends a denial response to the received page. Note that mode setup tables **18** of the wireless communication apparatuses A and B are so set as to shift the mode to the non-connectable mode when connection is established between the wireless communication apparatuses A and B. After connection is established between the wireless communication apparatuses A and B, the mode automatically shifts to the non-connectable mode in which the wireless communication apparatus sends a denial response to a received page (SA**8-1** and SB**8-1**).

Assume that a third wireless communication apparatus C wants connection with the wireless communication apparatus B. Further, assume that the wireless communication apparatus C acquires the unique address of the wireless communication apparatus B in advance by sending an inquiry and receiving an inquiry response before the wireless communication apparatus B shifts to the non-discoverable mode.

In step SC**1-1**, the wireless communication apparatus C designates the unique address of the wireless communication apparatus B and transmits a page. In step SB**10-1**, the wireless communication apparatus B receives the page from the wireless communication apparatus C. However, the wireless communication apparatus B has already shifted to the non-connectable mode. Thus, the control unit **12** generates a page denial response data (SB**10-1**) and transmits the page denial response (SB**11-1**).

The wireless communication apparatus C receives the page denial response from the wireless communication apparatus B (SC**2-1**). Since connection establishment fails, the control unit **12** notifies a user interface **11** of the connection establishment failure, and causes the user interface **11** to display the connection establishment failure (SC**3-1**). The wireless communication apparatus C cannot establish connection with the wireless communication apparatus B. The wireless communication apparatus C does not interfere with data transmission/reception between the wireless communication apparatuses A and B in steps SA**9** and SB**9**.

After data transmission/reception between the wireless communication apparatuses A and B in steps SA**9** and SB**9** ends, the mode setup, i.e., non-discoverable mode is cleared in the wireless communication apparatus B (SB**12**). The wireless communication apparatus B shifts to a normal mode.

The wireless communication apparatus according to the second embodiment shifts to the non-connectable mode after connection establishment, and transmits a page denial signal in response to a page signal from another wireless communication apparatus. This can prevent interference with communication with a connected wireless communication apparatus.

Third Embodiment

The operation of a wireless communication apparatus according to the third embodiment of the present invention will be described with reference to the flow chart of FIG. **6**.

The process up to establishing connection between wireless communication apparatuses A and B, i.e., the process from step SA**1** to step SA**7** and from step SB**1** to step SB**8** is the same as that shown in FIG. **4**.

If a control unit **12** determines in step SA**7** in the wireless communication apparatus A or in step SB**7** in the wireless communication apparatus B that connection has been established, the control unit **12** notifies a mode setup unit **13** of connection establishment.

In the wireless communication apparatus A, the mode setup unit **13** sends, to the control unit **12** in accordance with a preset mode setup, an instruction for shifting to the non-connectable mode in which the wireless communication apparatus A does not respond to a received page. Also in the wireless communication apparatus B, the mode setup unit **13** sends to the control unit **12** an instruction for shifting to the non-connectable mode in which the wireless communication apparatus B does not respond to a received page. Note that mode setup tables **18** of the wireless communication apparatuses A and B are so set as to shift the mode to the non-connectable mode when connection is established between the wireless communication apparatuses A and B. After connection is established between the wireless communication apparatuses A and B, the mode automatically shifts to the non-connectable mode in which the wireless communication apparatus does not respond to a received page (SA**8-2** and SB**8-2**).

Assume that a third wireless communication apparatus C wants connection with the wireless communication apparatus B. Further, assume that the wireless communication apparatus C acquires the unique address of the wireless communication apparatus B in advance by sending an inquiry and receiving an inquiry response before the wireless communication apparatus B shifts to the non-discoverable mode.

In step SC**1-2**, the wireless communication apparatus C designates the unique address of the wireless communication apparatus B and transmits a page. In step SB**10-2**, the wireless communication apparatus B receives the page from the wireless communication apparatus C. However, the wireless communication apparatus B has already shifted to the non-connectable mode. Thus, the control unit **12** does not generate any response data to the page, and does not transmit any response to the page (SB**11-1**).

The wireless communication apparatus C does not receive any page response from the wireless communication apparatus B. A time-out occurs (SC**2-2**), and the wireless communication apparatus C fails to establish connection. Since the wireless communication apparatus C fails to establish connection with the wireless communication apparatus B, the control unit **12** notifies a user interface **11** of the connection establishment failure, and causes the user interface **11** to display the connection establishment failure (SC**3-2**). The wireless communication apparatus C cannot establish connection with the wireless communication apparatus B. The wireless communication apparatus C does not

interfere with data transmission/reception between the wireless communication apparatuses A and B in steps SA9 and SB9.

The wireless communication apparatus according to the third embodiment shifts to the non-connectable mode after connection establishment, and does not respond to a page signal from another wireless communication apparatus. This can prevent interference with communication with a connected wireless communication apparatus.

The above embodiments have separately described shift to the non-connectable mode and shift to the non-discoverable mode. However, the wireless communication apparatus may simultaneously shift to the non-connectable mode and non-discoverable mode after connection is established.

In the above embodiments, the third wireless communication apparatus C sends a paging signal to the wireless communication apparatus B which receives a page from the wireless communication apparatus A and responds to the page to establish the first connection with the wireless communication apparatus A. The present invention is also effective when the wireless communication apparatus C sends a paging signal to the wireless communication apparatus A because the wireless communication apparatus A also automatically shifts to the non-discoverable mode or non-connectable mode after the first connection is established.

As described above, the wireless communication apparatus of the embodiments establishes connection with another wireless communication apparatus, and then automatically changes setups for an inquiry or paging with respect to still another wireless communication apparatus. The wireless communication apparatus does not send back any response or sends back an inquiry denial response, thereby denying connection establishment with still another wireless communication apparatus except for the currently connected wireless communication apparatus. This can prevent interference with communication between currently connected wireless communication apparatuses.

The present invention is not limited to the above-described embodiments, and can be variously modified without departing from the spirit and scope of the invention in practical use. The respective embodiments can be combined as properly as possible. In this case, the effects of the combination can be obtained. The embodiments include inventions on various stages, and various inventions can be extracted by an appropriate combination of building components disclosed. For example, when an invention is extracted by omitting several building components from all the building components described in the embodiments, the omission is properly compensated for by a well-known technique in practicing the extracted invention.

As has been described in detail, the present invention can provide a wireless communication apparatus which, after establishing connection with another wireless communication apparatus, denies connection establishment with still another wireless communication apparatus except for the currently connected wireless communication apparatus, and does not interfere with communication between the currently connected wireless communication apparatuses.

Additional advantages and modifications will readily occur to those skilled in the art. Therefore, the invention in its broader aspects is not limited to the specific details and representative embodiments shown and described herein. Accordingly, various modifications may be made without departing from the spirit or scope of the general inventive concept as defined by the appended claims and their equivalents.

What is claimed is:

1. A wireless communication apparatus comprising:

a unit configured to set up a first mode where the wireless communication apparatus is connectable with at least a first wireless communication device and a second wireless communication device and accepts a connection request from the first wireless communication device;

a unit configured to establish a connection with the first wireless communication device;

a unit configured to discover a completion of the connection with the first wireless communication device;

a unit configured to set up a second mode where, in a state where the connection with the first wireless communication device is established, the wireless communication apparatus is inhibited from establishing a connection with the second wireless communication device with respect to a connection request from the second wireless communication device; and

a unit configured to shift from the first mode to the second mode when said discovering unit discovers the completion of the connection.

2. An apparatus according to claim **1**, wherein the second mode includes a non-discoverable mode in which the wireless communication apparatus does not respond to an inquiry signal.

3. An apparatus according to claim **1**, wherein the second mode includes a non-connectable mode in which no connection is performed for paging.

4. An apparatus according to claim **2**, wherein the second mode includes a non-discoverable mode based on a Bluetooth standard.

5. An apparatus according to claim **3**, wherein the second mode includes a non-connectable mode based on a Bluetooth standard.

6. An apparatus according to claim **4**, wherein the non-discoverable mode does not respond to an inquiry.

7. An apparatus according to claim **5**, wherein the non-connectable mode sends a connection denial response to a paging signal.

8. An apparatus according to claim **5**, wherein the non-connectable mode does not respond to a paging signal.

9. An apparatus according to claim **1**, wherein the second mode includes a non-discoverable mode and non-connectable mode based on a Bluetooth standard.

10. An apparatus according to claim **1**, wherein the second mode inhibits connection with another wireless communication apparatus.

11. An apparatus according to claim **1**, wherein the second mode is canceled after end of communication with the first wireless communication device.

12. A communication method in a wireless communication apparatus, comprising:

setting up a first mode where the wireless communication apparatus is connectable with at least a first wireless communication device and a second wireless communication device and accepts a connection request from the first wireless communication device;

establishing a connection with the first wireless communication device;

discovering a completion of the connection with the wireless communication apparatus;

setting up a second mode where, in a state where the connection with the first wireless communication device is established, the wireless communication

apparatus is inhibited from establishing a connection with the second wireless communication device with respect to a connection request from the second wireless communication device; and

shifting from the first mode to the second mode after the completion of the connection.

13. A method according to claim **12**, wherein the second mode includes a non-discoverable mode in which the wireless communication apparatus does not respond to an inquiry signal.

14. A method according to claim **12**, wherein the second mode includes a non-connectable mode in which no connection is performed for paging.

15. A method according to claim **13**, wherein the second mode includes a non-discoverable mode based on a Bluetooth standard.

16. A method according to claim **14**, wherein the second mode includes a non-connectable mode based on a Bluetooth standard.

17. A method according to claim **15**, wherein the wireless communication apparatus does not respond to an inquiry signal from another wireless communication apparatus after shifting to the second mode.

18. A method according to claim **16**, wherein the wireless communication apparatus sends a connection denial response to a paging signal after shifting to the second mode.

19. A method according to claim **16**, wherein the wireless communication apparatus does not respond to a paging signal after shifting to the second mode.

20. A communication apparatus comprising:

a unit configured to establish a connection with a first wireless communication apparatus in a first mode; and

a unit configured to control a connection from a second wireless communication apparatus when the connection with the first wireless communication apparatus is established, wherein the control unit sets up a second mode in which, in a state where the connection with the first wireless communication device is established, the communication apparatus is inhibited from establishing a connection with the second wireless communication apparatus with respect to a connection request from the second wireless communication device.

21. A communication method in a communication apparatus, comprising:

establishing a connection with a first wireless communication apparatus in a first mode; and

controlling a connection from a second wireless communication apparatus when the connection with the first wireless communication apparatus is established, wherein controlling includes setting up a second mode in which, in a state where the connection with the first wireless communication device is established, the communication apparatus is inhibited from establishing a connection with the second wireless communication apparatus with respect to a connection request from the second wireless communication device.

* * * * *

EXHIBIT 4

US007184707B2

(12) **United States Patent**
Tada et al.

(10) **Patent No.: US 7,184,707 B2**
(45) **Date of Patent: Feb. 27, 2007**

(54) **COMMUNICATION DEVICE AND A METHOD FOR CONTROLLING THE COMMUNICATION DEVICE**

(75) Inventors: **Masahiro Tada**, Tokyo (JP); **Ikuo Sako**, Tokyo (JP); **Koichi Yata**, Saitama-ken (JP)

(73) Assignee: **Kabushiki Kaisha Toshiba**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 663 days.

(21) Appl. No.: **10/084,502**

(22) Filed: **Feb. 28, 2002**

(65) **Prior Publication Data**

US 2002/0147003 A1 Oct. 10, 2002

Related U.S. Application Data

(63) Continuation of application No. PCT/JP01/05570, filed on Jun. 28, 2001.

(30) **Foreign Application Priority Data**

Jul. 6, 2000 (JP) 2000-204623

(51) **Int. Cl.**
H04B 7/00 (2006.01)
H04Q 7/20 (2006.01)
H04J 3/16 (2006.01)

(52) **U.S. Cl.** **455/41.3**; 455/455; 455/510; 455/513; 370/466

(58) **Field of Classification Search** 455/41.2, 455/41.3, 450; 358/1.5
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,287,545 A * 2/1994 Kallin 455/510
6,633,757 B1 * 10/2003 Hermann et al. 455/414.1
6,721,787 B1 * 4/2004 Hiscock 709/217
6,807,413 B1 * 10/2004 Honda 455/414.1
6,965,948 B1 * 11/2005 Eneborg et al. 709/250
7,010,323 B2 * 3/2006 Suwa 455/552.1
7,024,183 B2 * 4/2006 Hymel 455/417

(Continued)

FOREIGN PATENT DOCUMENTS

JP 10-322773 12/1998

(Continued)

OTHER PUBLICATIONS

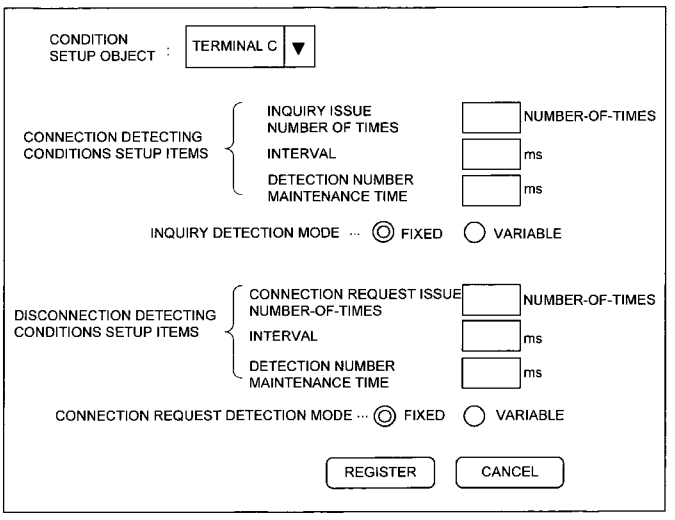
Copy of International Search Report dated Sep. 25, 2001.

Primary Examiner—Fan Tsang
Assistant Examiner—Lisa Hashem
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

(57) **ABSTRACT**

A communication device and a method for controlling a communication device that can load or unload service information at appropriate timings by flexibly designating discriminating conditions of connection or disconnection of a link. A service manager reads out necessary service information, such as service program or driver software, from the information memory area based on discriminating conditions designated in communication controlling information of the communication status. The service manager loads service information to a temporary information memory area in a host device. The service manager also unloads unnecessary service information from the temporary information memory area in the host device. A connection manager then performs communication protocol for communicating between the service information loaded in the temporary information memory area of the host and the service information memory of the device side.

5 Claims, 11 Drawing Sheets



U.S. PATENT DOCUMENTS

2002/0034192	A1*	3/2002	Kim	370/466
2002/0051184	A1*	5/2002	Fritz et al.	358/1.15
2002/0094778	A1*	7/2002	Cannon et al.	455/41
2002/0111138	A1*	8/2002	Park	455/41
2003/0078002	A1*	4/2003	Sanjeev et al.	455/41

FOREIGN PATENT DOCUMENTS

JP	11-164359	6/1999
JP	11225364 A	8/1999
JP	11-355279	12/1999
JP	2000115189 A	4/2000
WO	WO 97/40457	10/1997

* cited by examiner

FIG. 1

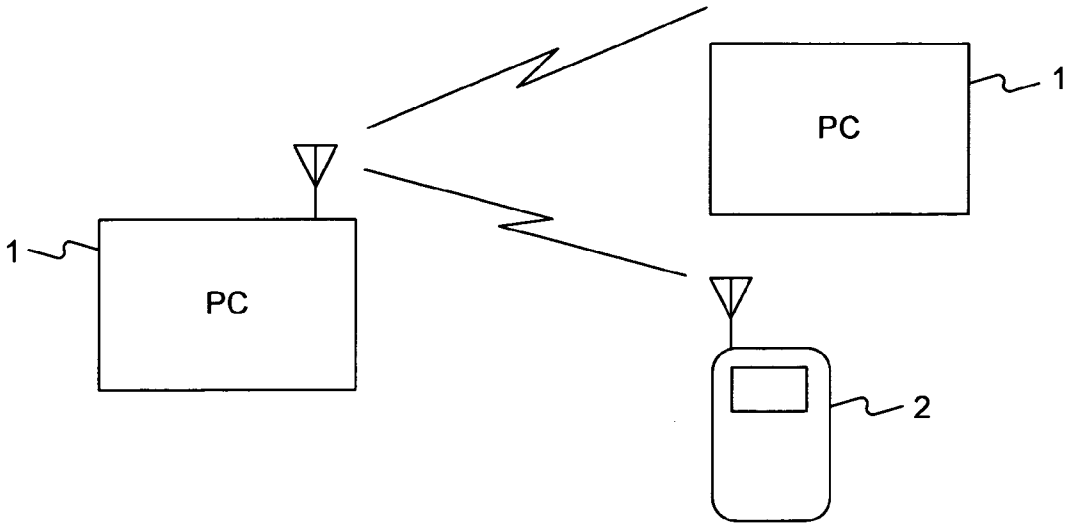

PC
1
1
PC
2
100

FIG. 2

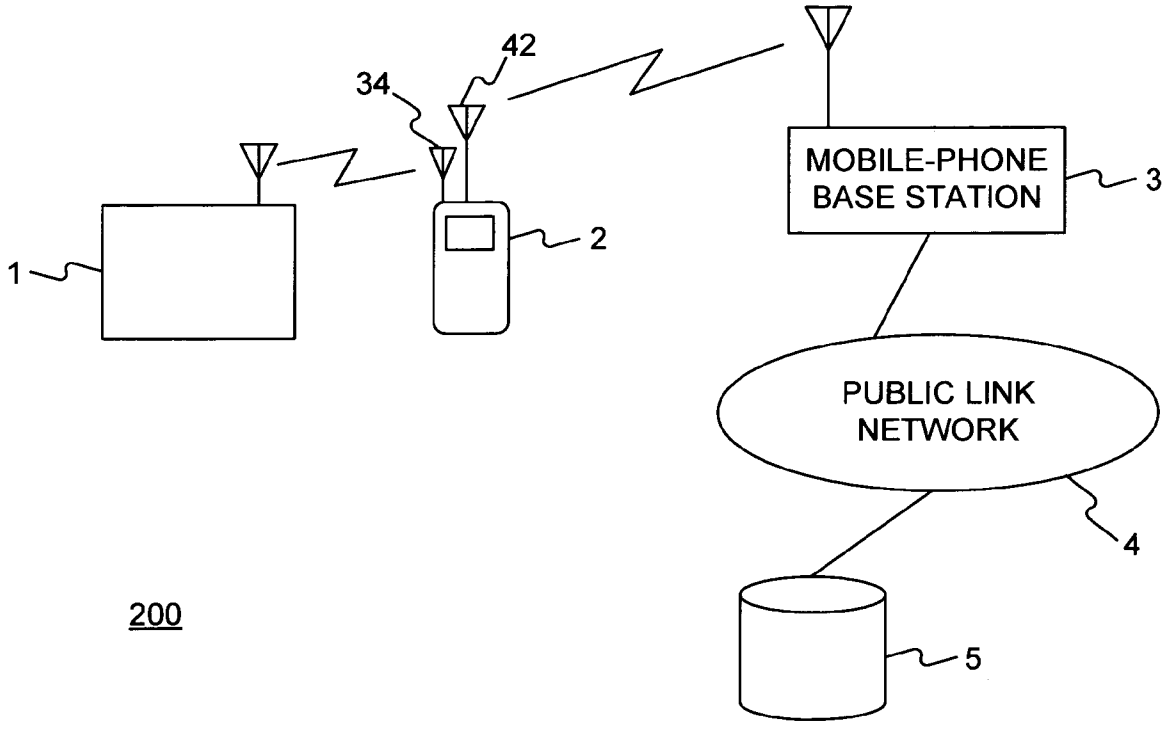

42
34
MOBILE-PHONE BASE STATION
3
1
2
PUBLIC LINK NETWORK
4
200
5

FIG.3

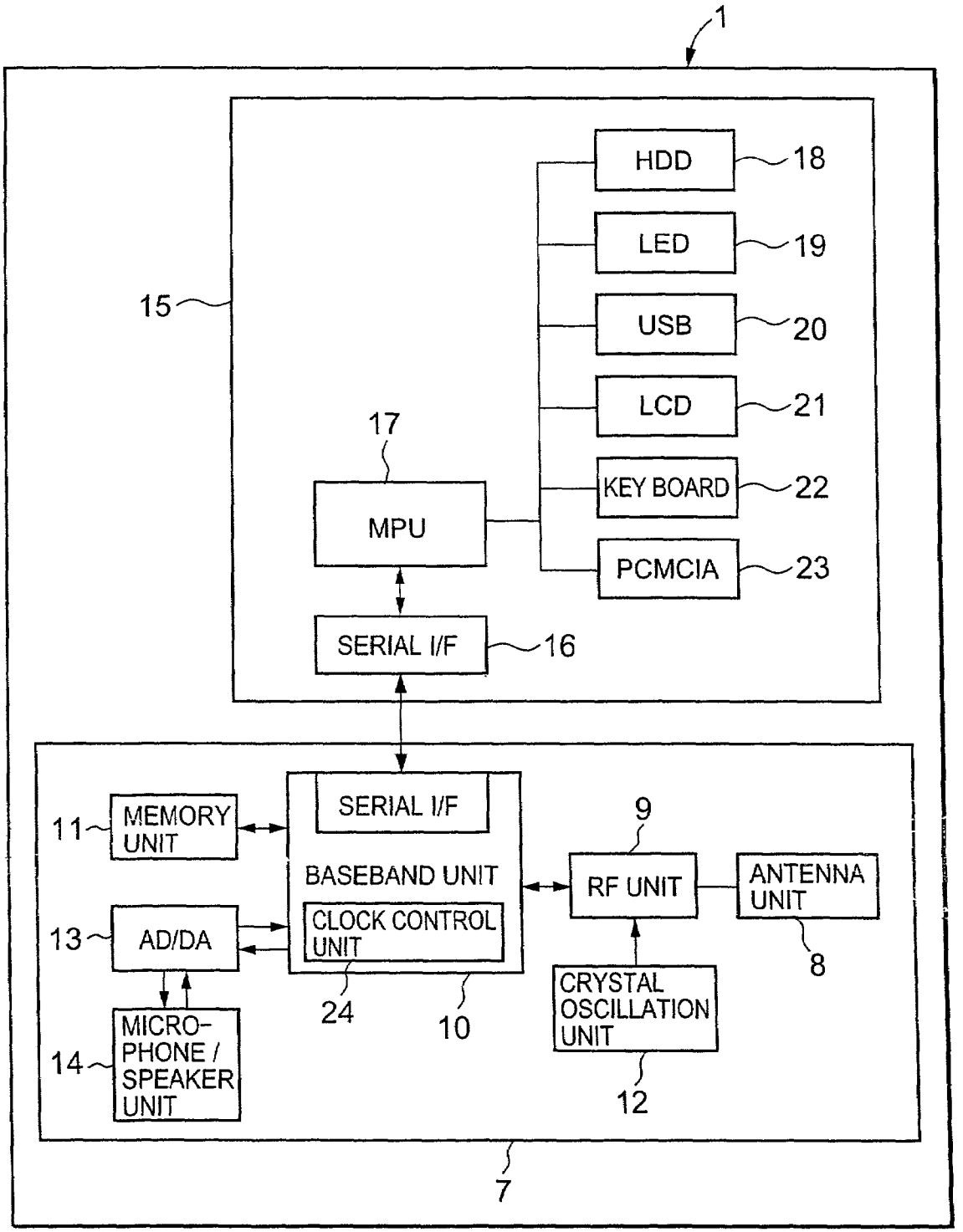

1
HDD
18
LED
19
15
USB
20
LCD
21
17
KEY BOARD
22
MPU
PCMCIA
23
SERIAL I/F
16
SERIAL I/F
9
11
MEMORY UNIT
BASEBAND UNIT
RF UNIT
ANTENNA UNIT
13
AD/DA
CLOCK CONTROL UNIT
8
24
10
CRYSTAL OSCILLATION UNIT
MICRO-PHONE / SPEAKER UNIT
14
12
7

FIG.4

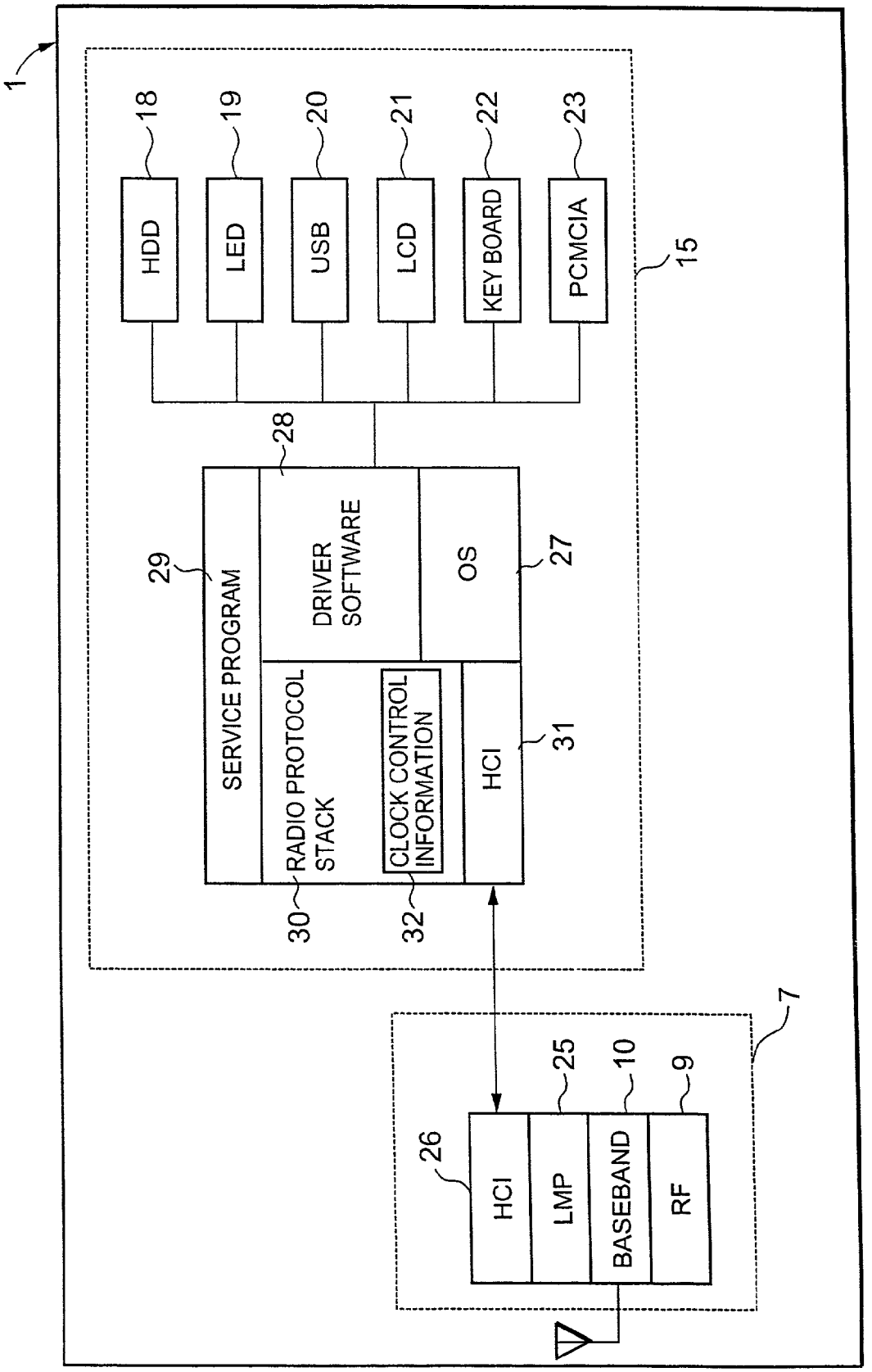

1
18
19
20
21
22
23
HDD
LED
USB
LCD
KEY BOARD
PCMCIA
15
28
29
SERVICE PROGRAM
DRIVER SOFTWARE
OS
27
RADIO PROTOCOL STACK
CLOCK CONTROL INFORMATION
HCI
31
30
32
7
25
10
9
26
HCI
LMP
BASEBAND
RF

FIG. 5

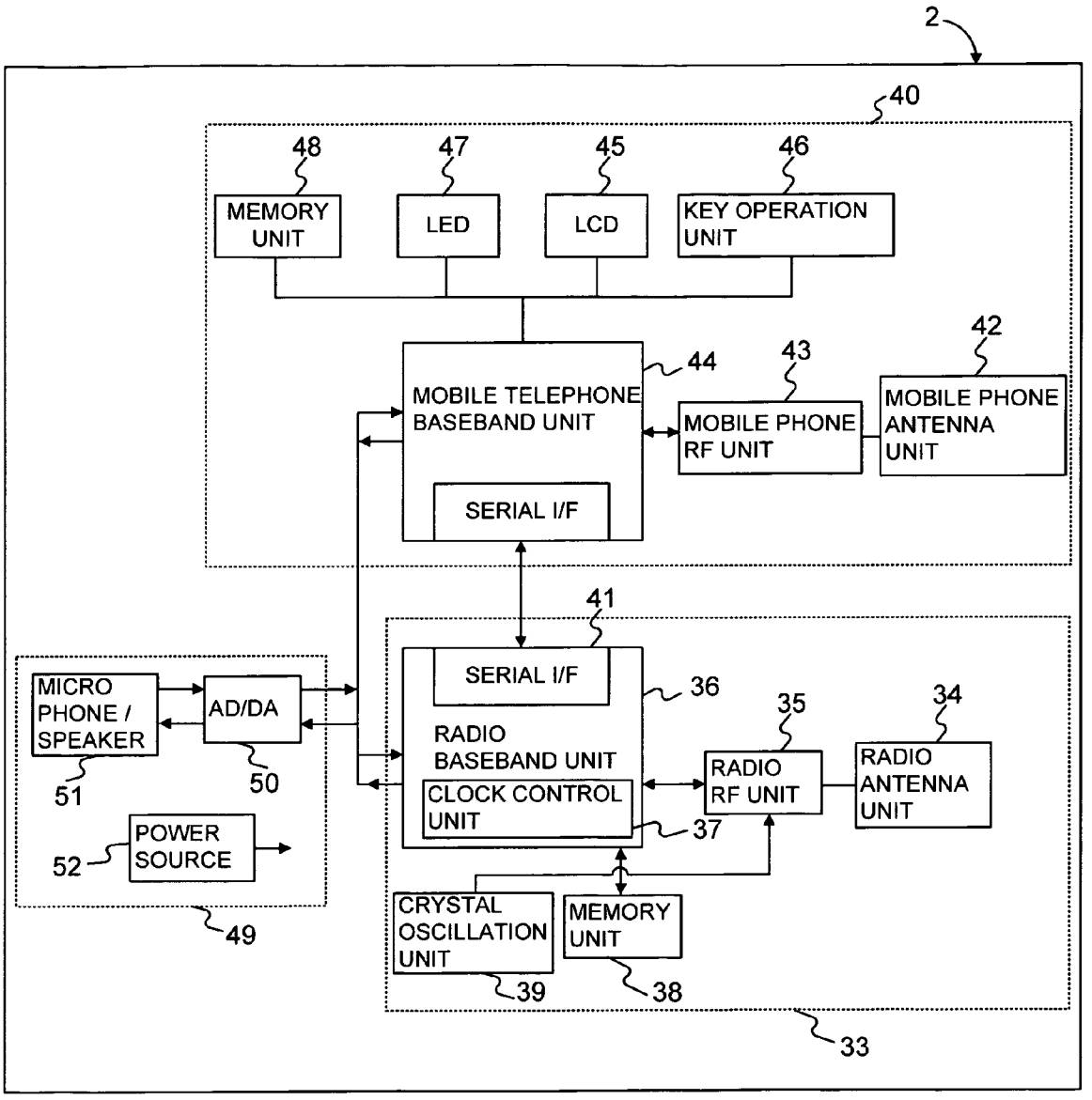

2
40
48
MEMORY UNIT
47
LED
45
LCD
46
KEY OPERATION UNIT
42
44
43
MOBILE TELEPHONE BASEBAND UNIT
MOBILE PHONE RF UNIT
MOBILE PHONE ANTENNA UNIT
SERIAL I/F
41
SERIAL I/F
36
35
34
RADIO BASEBAND UNIT
RADIO RF UNIT
RADIO ANTENNA UNIT
CLOCK CONTROL UNIT
37
MICRO PHONE / SPEAKER
AD/DA
51
50
POWER SOURCE
52
49
CRYSTAL OSCILLATION UNIT
39
MEMORY UNIT
38
33

FIG. 6

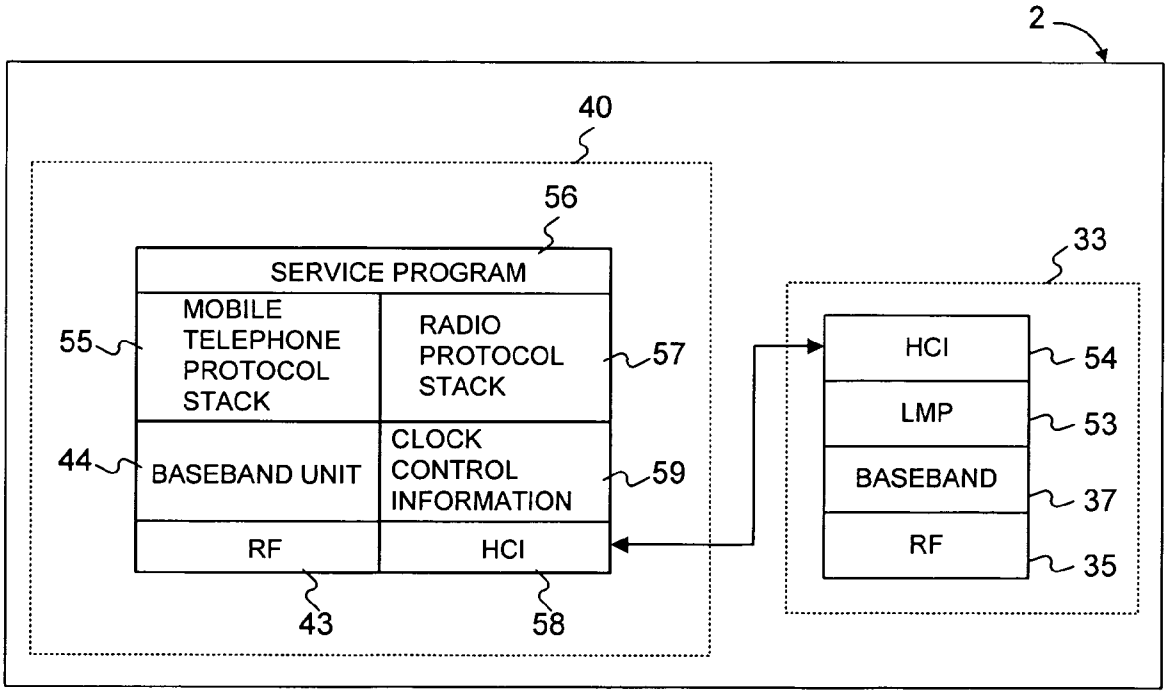

2
40
56
SERVICE PROGRAM
MOBILE TELEPHONE PROTOCOL STACK
RADIO PROTOCOL STACK
55
57
44
BASEBAND UNIT
CLOCK CONTROL INFORMATION
59
RF
HCI
43
58
33
HCI
54
LMP
53
BASEBAND
37
RF
35

FIG.7

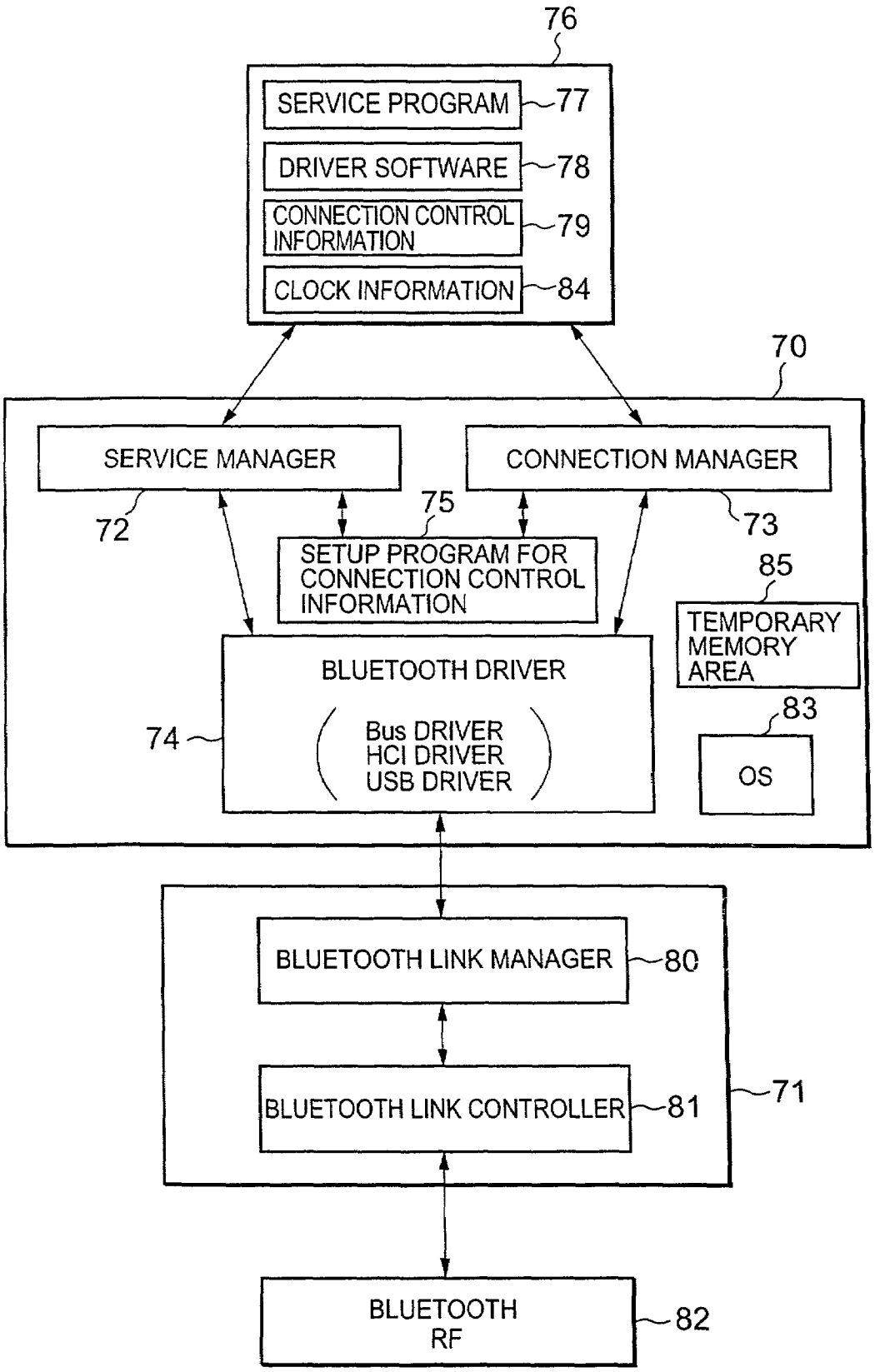

76
SERVICE PROGRAM
77
DRIVER SOFTWARE
78
CONNECTION CONTROL INFORMATION
79
CLOCK INFORMATION
84
70
SERVICE MANAGER
CONNECTION MANAGER
72
75
73
SETUP PROGRAM FOR CONNECTION CONTROL INFORMATION
85
TEMPORARY MEMORY AREA
BLUETOOTH DRIVER
74
Bus DRIVER
HCI DRIVER
USB DRIVER
83
OS
BLUETOOTH LINK MANAGER
80
BLUETOOTH LINK CONTROLLER
81
71
BLUETOOTH RF
82

FIG.8

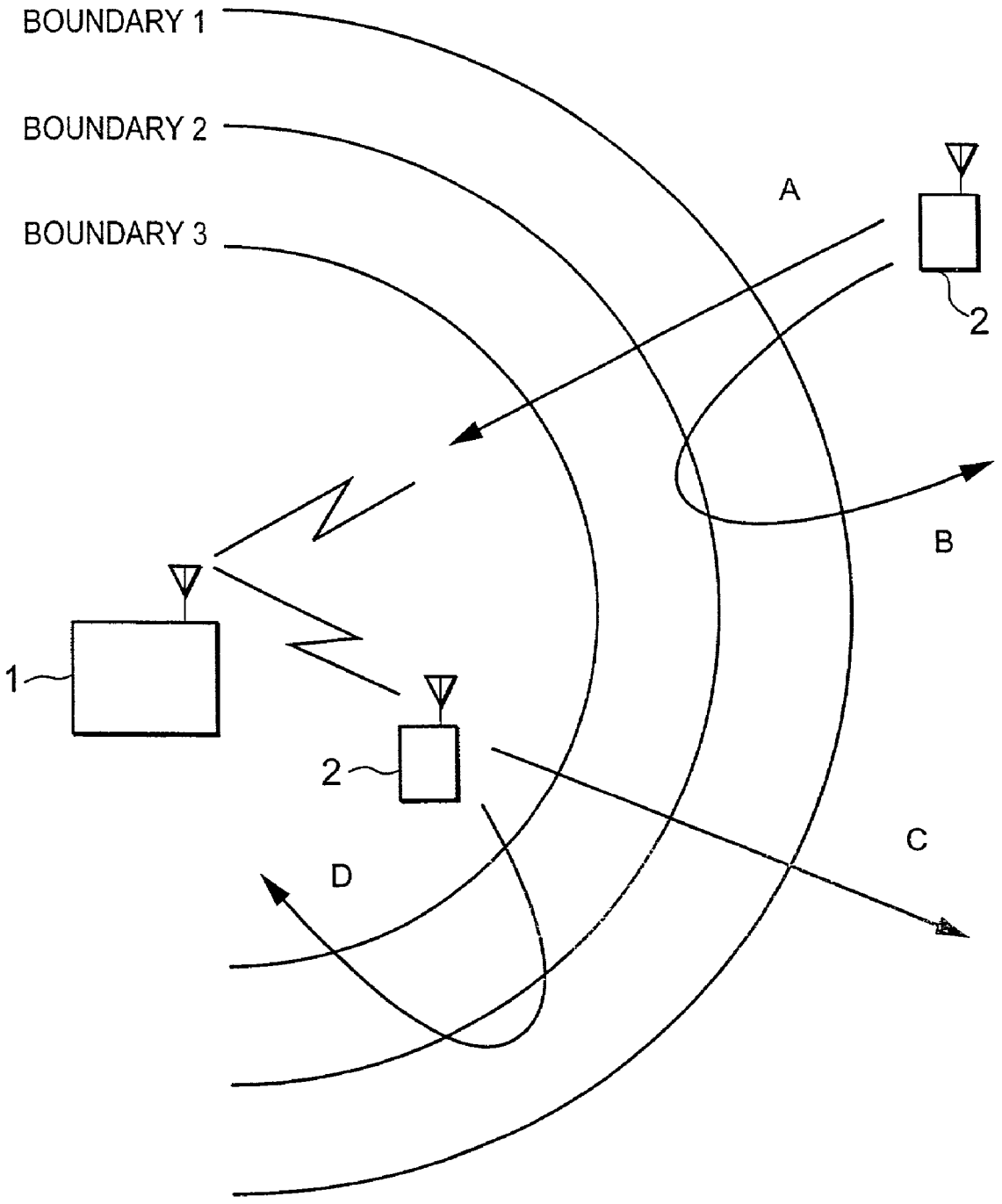


FIG.9

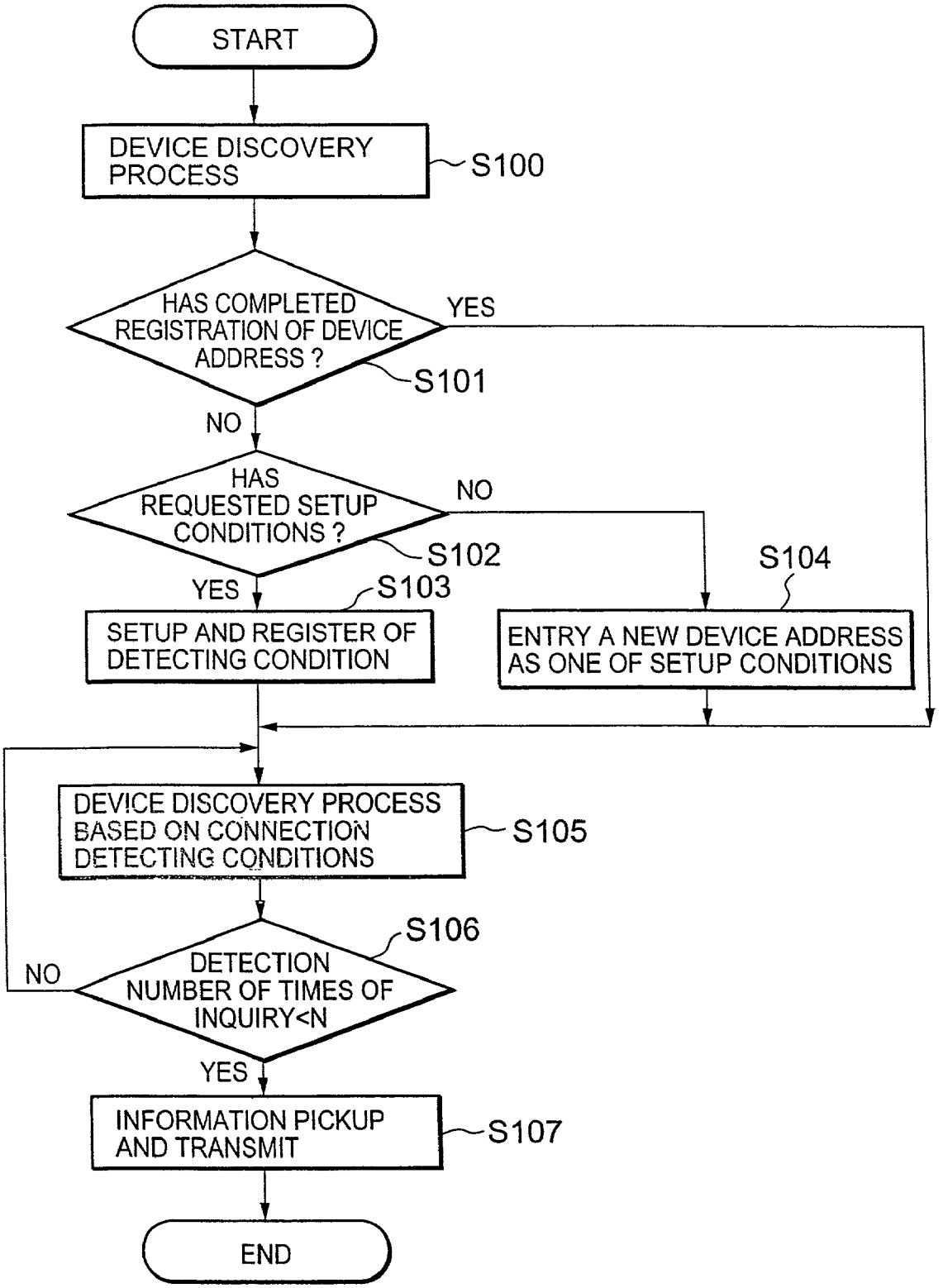

START
DEVICE DISCOVERY PROCESS
S100
HAS COMPLETED REGISTRATION OF DEVICE ADDRESS ?
YES
S101
NO
HAS REQUESTED SETUP CONDITIONS ?
NO
S102
S104
YES
S103
SETUP AND REGISTER OF DETECTING CONDITION
ENTRY A NEW DEVICE ADDRESS AS ONE OF SETUP CONDITIONS
DEVICE DISCOVERY PROCESS BASED ON CONNECTION DETECTING CONDITIONS
S105
S106
NO
DETECTION NUMBER OF TIMES OF INQUIRY<N
YES
INFORMATION PICKUP AND TRANSMIT
S107
END

FIG.10

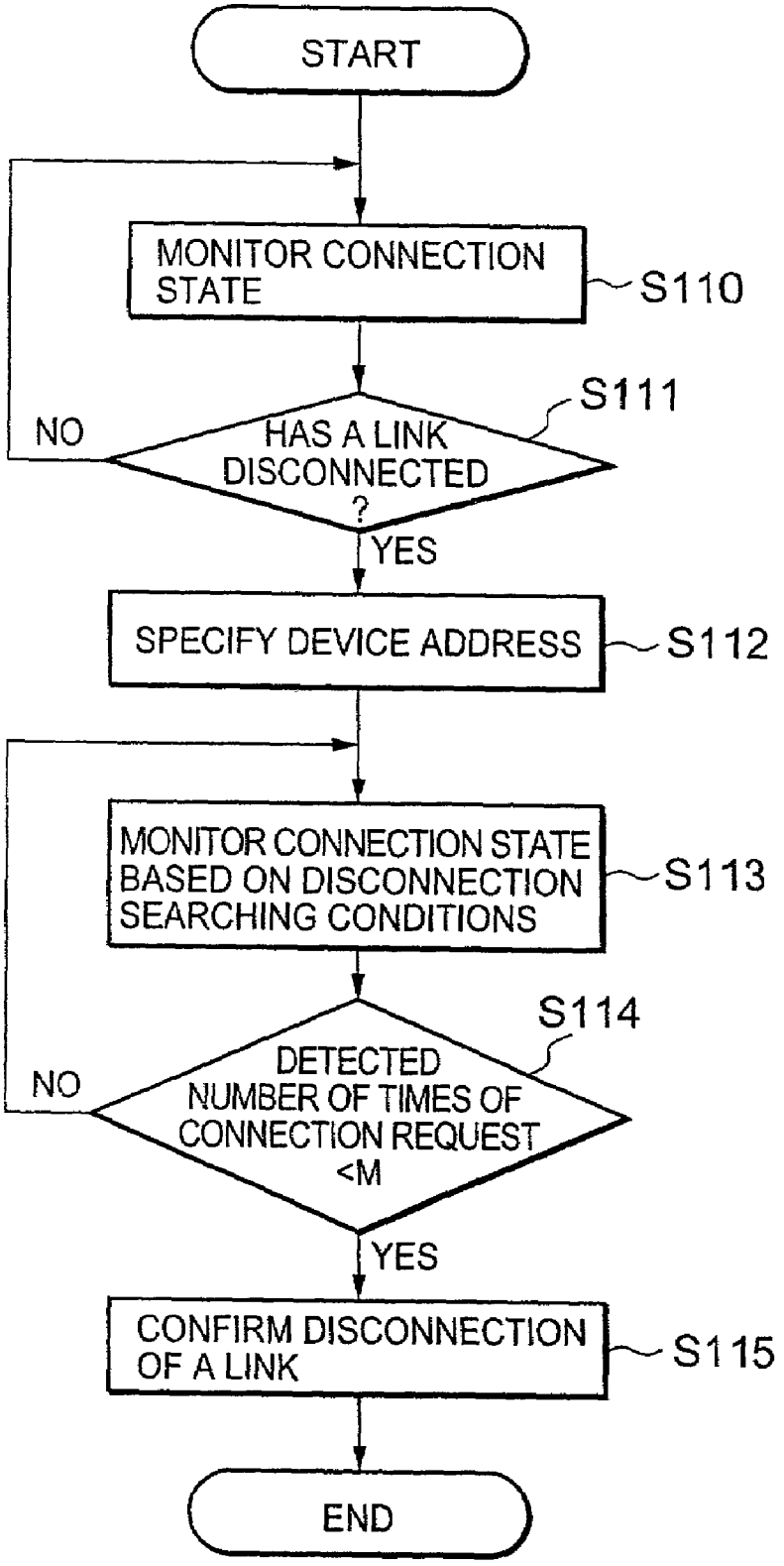
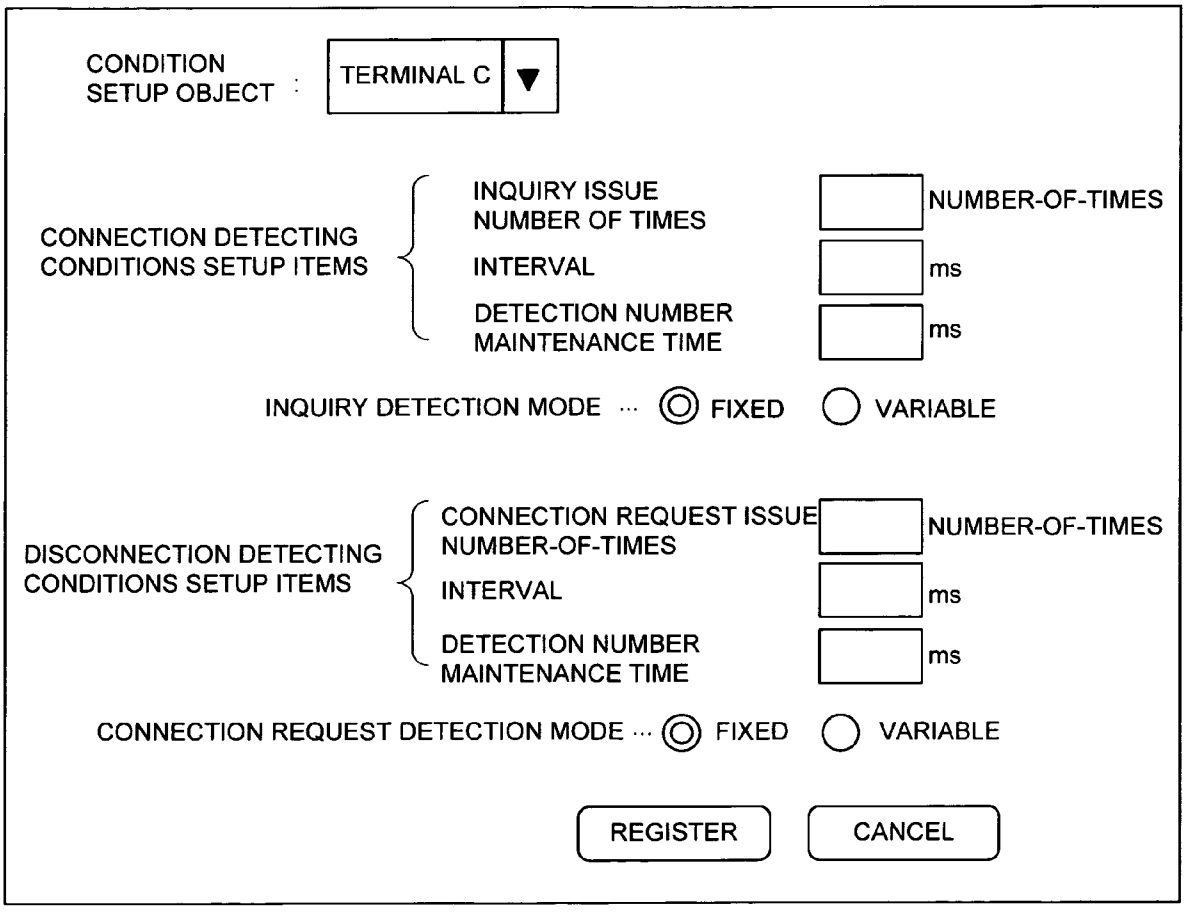

START
MONITOR CONNECTION STATE
S110
S111
NO
HAS A LINK DISCONNECTED ?
YES
SPECIFY DEVICE ADDRESS
S112
MONITOR CONNECTION STATE BASED ON DISCONNECTION SEARCHING CONDITIONS
S113
S114
NO
DETECTED NUMBER OF TIMES OF CONNECTION REQUEST <M
YES
CONFIRM DISCONNECTION OF A LINK
S115
END

FIG. 11

DEVICE ADDRESS	FRIENDLY NAME	CONNECTION JUDGING CONDITIONS			DISCONNECTION JUDGING CONDITIONS			
		ISSUE NUMBER-OF-TIMES OF INQUIRY (n)	INTERVAL (Ti)	DETECTION NUMBER-OF-TIMES MAINTENANCE TIME (Tn)	DETECTION MODE	ISSUE NUMBER-OF-TIMES OF CONNECTION REQUEST (m)	INTERVAL (Tj)	DETECTION NUMBER-OF-TIMES MAINTENANCE TIME (Tm)	DETECTION MODE
A A A A	TERMINAL A								
B B B B	TERMINAL B								
C C C C	TERMINAL C								
X X X X	SETUP DEFAULT								

FIG. 12


CONDITION SETUP OBJECT :
TERMINAL C
CONNECTION DETECTING CONDITIONS SETUP ITEMS
INQUIRY ISSUE NUMBER OF TIMES
NUMBER-OF-TIMES
INTERVAL
ms
DETECTION NUMBER MAINTENANCE TIME
ms
INQUIRY DETECTION MODE ··· FIXED VARIABLE
DISCONNECTION DETECTING CONDITIONS SETUP ITEMS
CONNECTION REQUEST ISSUE NUMBER-OF-TIMES
NUMBER-OF-TIMES
INTERVAL
ms
DETECTION NUMBER MAINTENANCE TIME
ms
CONNECTION REQUEST DETECTION MODE ··· FIXED VARIABLE
REGISTER
CANCEL

COMMUNICATION DEVICE AND A METHOD FOR CONTROLLING THE COMMUNICATION DEVICE

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation of international application number PCT/JP01/05570, filed Jun. 28, 2001, and claims priority to Japanese Patent Application No. 2000-204623, filed Jul. 6, 2000, the contents of which are incorporated herein by reference.

This application claims the benefit of priority of International Application No. PCT/JP01/05370, filed on Jun. 28, 2001.

TECHNICAL FIELD OF THE INVENTION

The present invention relates to a communication device and a method for controlling the communication device, and more particularly to a radio communication device and a method for control thereof.

DESCRIPTION OF RELATED ART

In the case where peripheral devices or extension cards are connected to a personal computer (PC), the PC is loaded with suitable driver software for the respective devices so that it may recognize hardware information for the additional devices. Moreover, the PC may further allocate various resources such as an I/O port, by using plug and play technology. In plug and play technology, the driver software corresponding to the additional devices and other related service programs are loaded or unloaded. The PC determines whether to load or unload the device software and source programs by detecting the device connection to the PC through a direct bus connection or a cable wired connection.

Recently, radio communication techniques have been put to practical use in coupling information devices. Radio communication techniques such as "Bluetooth" or Home RF are being used in coupling, for example, a PC and a Personal Digital Assistance (PDA); or a PC and a mobile telephone.

Bluetooth is a radio communication interface standard that uses an Industrial Scientific Medical (ISM) band of 2.4 GHz as a carrier frequency and provides a band zone of 1 Mbps within a 10 m service area.

Similar to Bluetooth, Home RF is also a radio communication standard for a home application. Home RF uses the same ISM band of 2.4 GHz as a carrier frequency and communicates through a maximum data transmission speed of 1.6 Mbps in a service area covering a distance from 50 m to 100 m.

In the prior art radio communication systems discussed above, a connection or disconnection between a master device and a slave device may frequently occur when the radio state becomes unstable due to the surrounding environment. During each connection or disconnection, a host PC may experience an increase in loads because of the repetitious loading and unloading, for example, of service information such as driver software or service programs. The increased load on the host PC results in a number of problems that hinder performance. Unintended communications generated by a user of the host PC due to the unexpected loading of service information, for example, causes excessive loads on the communication operations of the host PC. Further, unintended unloading of service information by a user may prevent the host PC from communicating service information to the peripheral device.

Japanese patent application publication No. 11-355279, discloses technology that controls data communication in a radio communication system based on a corresponding link status of the radio communication system. The link status is determined by monitoring data communication between two devices of the radio communication system. Based on the number of frames corresponding to decoded managing data, the disclosed technology determines whether the communication environment is an all data transmittable area, an asynchronous transmittable area, or a transmission unable area. Identifying the type of communication environment enables the host PC to determine whether the radio communication system has a link possible status, a link impossible status, or a link possible status for only asynchronous data that are performed during a retransmission process.

A host device in a conventional radio communication system experiences reduced performance in its communication processes because of the repeated loading and unloading of service information, which corresponds to a radio link state of the radio communication system. The technology disclosed in Japanese patent application publication No. 11-355279 may increase the reliability of data communication. However, this technology cannot resolve the problem of reduced communication performance attributed to the unintentional loading or unloading of service information.

To overcome the above and other disadvantages of the prior art, methods and systems consistent with the present invention control a communication device to load or unload service information at appropriate timings by flexibly designating discriminating conditions on a link connection or a link disconnection in order to secure a stable radio communication system.

SUMMARY OF THE INVENTION

An embodiment consistent with the present invention relates to a radio communication device on a network for communicating with a target communication terminal on the network. The radio communication device comprises a memory for storing service information so that perform predetermined functions can be performed over the network with the target communication terminal; a judging module for judging whether predetermined connection conditions with the target communication terminal are satisfied by repeating a target communication terminal discovery process before establishing radio communications with another target communication terminal; and a communication control module for executing the predetermined functions with the target communication terminal by reading service information associated with the target communication terminal from the service information memory when the predetermined connection conditions are satisfied.

Another embodiment consistent with the present invention also relates to a radio communication device on a network for communicating with a target communication terminal on the network. The radio communication device comprises a service information memory for storing service information that corresponds to the target communication terminal so that predetermined functions can be performed with the target communication terminal over the network; a judging module for judging whether predetermined disconnection discriminating conditions are satisfied by repeating a connection process with the target communication terminal before disconnecting radio communication with the target communication terminal; and a communication con-

trol module for invalidating the predetermined functions associated with the service information that corresponds to the target communication terminal and storing the service information in the service information memory mechanism when the predetermined disconnection discriminating conditions are satisfied.

A further embodiment consistent with the present invention relates to a radio communication device in a network for communicating with a target communication terminal in the network. The radio communication device comprises a service information memory for storing service information so that predetermined functions can be performed with the target communication terminal; and a communication control module for communicating with the target communication terminal by using the service information read out from the service information memory based on communication controlling information that defines discriminating conditions for establishing a new connection with the target communication terminal or disconnecting an existing connection with the target communication terminal.

An additional embodiment consistent with the present invention relates to a communication device comprising a radio communication module for exchanging data with a target communication terminal over a network; a service information memory for storing service information so that predetermined functions can be performed with the target communication terminal; a communication control information designating module for designating communication conditions for a newly established radio communication connection with the target communication terminal or for discriminating a disconnection of an existing radio communication connection with the target communication terminal; a memory for storing the designated communication controlling information by the communication control information designating module; and a communication control module for determining whether the radio communication connection with the target communication terminal is in a connection status or a disconnection status based on the communication controlling information stored in the memory, and performing communication through the radio communication module by using service information read from the service information memory in accordance with the determination result.

Yet another embodiment consistent with the present invention relates to a radio communication device in a network that exchanges service information with a target communication terminal in the network for performing predetermined functions. The radio communication device comprises a service memory for storing the service information; a temporary memory for temporarily storing the service information used to establish communications with the target communication terminal; a first module for transferring the service information from the service memory to the temporary memory when a radio communicating connection for the target communication terminal has been established, and for transferring the service information from the temporary memory to the service memory when the radio communication connection with target communication terminal has been disconnected based on communication controlling information used for discriminating between a newly established radio communication connection with the target communication terminal and a disconnection of an existing radio communication connection with the target communication terminal; and a radio communication control mechanism for performing the predetermined functions with the target communication terminal when the service information is stored in temporary memory.

Yet a further embodiment consistent with the present invention relates to a communication device comprising a radio communication module for exchanging data with a target communication terminal through radio; a service memory for storing service information so that predetermined functions can be performed with the target communication terminal; a temporary memory for temporarily storing service information used in an established target communication terminal for communication; a designating module for designating communication controlling information in order to define conditions for discriminating between a newly established radio communication connection with the target communication terminal or a disconnection of an existing radio communication connection with the target communication terminal; a communication controlling information memory for storing the communication controlling information designated by the designating module; a memory for storing the communication controlling information designated by the designating module; a discriminating module for determining whether a status of the radio communication connection with a target communication terminal is a connection status or a disconnection status based on the communication controlling information in the communication controlling information memory, and transferring the service information from the service memory to the temporary memory when the status of the radio communication connection with the target communication terminal is the connection status, and transferring the service information from the temporary memory to the service memory when the status of the radio communication connection with the target communication terminal is the disconnection status; and a radio communication control module for performing the predetermined functions with the target communication terminal when the service information is stored in the temporary memory.

Yet an additional embodiment consistent with the present invention relates to a method for controlling a communication device that exchanges data with a target communication terminal over a radio network. The communication device has a memory for storing various types of data. The method when establishing a new radio communication connection between the communication device and a target communication terminal, comprises judging whether predetermined connection discriminating conditions are satisfied by repeating a target communication terminal discovery process before performing the predetermined functions; and performing the predetermined functions through the radio communication connection by extracting required service information from memory to perform the predetermined functions between the communication device and the target communication terminal, the required service information is stored in the memory by executing the predetermined functions with the target communication when the predetermined connection conditions are satisfied.

Still another embodiment consistent with the present invention relates to a method for controlling a communication device that exchanges data with a target communication terminal over a network. The communication device has a memory for storing various types of data. The method when disconnecting radio communication connection established between the communication device and a target communication terminal, comprises judging whether disconnection conditions are satisfied by repeating a target communication terminal connection process; and invalidating the predetermined functions corresponding to executed service information that is stored in memory so that the predetermined functions between the communication device and the target

communication terminal can be performed when the disconnection discriminating conditions are satisfied.

Still a further embodiment consistent with the present invention relates to a method for controlling a communication device that exchanges data with target communication terminal over a network, the communication device having a memory mechanism for storing various types of data. The method comprises judging whether a radio communication connection between the communication device and a target communication terminal is in a connection status or in a disconnection status, based on communication controlling information that defines conditions for discriminating between a new radio communication connection established between the communication device and a new target communication terminal, or a disconnection of radio communication connection established between the communication device and the target communication terminal, and performing radio communications with the target communication terminal by using service information that executes the predetermined functions between the communication device and the target communication terminal, the service information being stored in memory based on a discrimination result.

Still an additional embodiment consistent with the present invention relates to a method for controlling a communication device that exchanges data with a target communication terminal over a network, the communication device having a memory for storing various types of data. The method comprises storing, in memory, designated communication control information that defines discriminating conditions for discriminating between establishing a new radio communication connection between the communication device and a target communication terminal, or a disconnecting a radio communication connection established between the communication device and the target communication terminal; judging whether the radio communication connection between the communication device and the target communication terminal is in a connection state or a disconnection state based on the designated communication control information; and performing radio communication with the target communication terminal by using service information that executes the predetermined functions between the communication device and the target communication terminal, the service information being stored in memory based on a discrimination result.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating a general structure of a radio-communications system consistent with the present invention.

FIG. **2** is a block diagram illustrating a general structure of a complete radio-communications system consistent with the present invention.

FIG. **3** is a block diagram illustrating a hardware structure of a personal computer used as information processing equipment consistent with the present invention.

FIG. **4** is a block diagram illustrating a software structure of a personal computer consistent with the present invention.

FIG. **5** is a block diagram illustrating a hardware structure of a mobile telephone consistent with the present invention.

FIG. **6** is a block diagram illustrating a software structure of a mobile telephone consistent with the present invention.

FIG. **7** is a block diagram illustrating a structure of a host and a host controller consistent with the present invention.

FIG. **8** is a block diagram illustrating a connection/disconnection state of a radio link consistent with the present invention.

FIG. **9** is a flowchart showing a connection judging process of radio link consistent with the present invention.

FIG. **10** is a flowchart showing a disconnection judging process of a radio link consistent with the present invention.

FIG. **11** illustrates an example of a connection/disconnection setup state of a radio link consistent with the present invention.

FIG. **12** illustrates an example of user interface screen for designating connection/disconnection conditions for a radio link consistent with the present invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

Reference will now be made in detail to exemplary embodiments of the invention, which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

FIG. **1** illustrates a basic structure of a radio-communication network **100** in accordance with an embodiment of the present invention invention. Generally, the radio communication system comprises information process equipment and a mobile apparatus. The information processing equipment may be represented, for example, by a battery driven notebook type personal computer (PC **1**). The mobile apparatus may be represented by a mobile telephone **2**. PC **1** and mobile telephone **2** may communicate information by establishing a local radio link. When a radio link is established between PC **1** and mobile telephone **2**, a user may perform predetermined service programs on radio communication network **100**, such as mailing data or exchanging personal information.

PC **1** may establish a radio link between a plurality of devices on radio communication network **100** at the same time. For example, PC **1** may exploit a multi-point access technique by connecting to mobile telephone **2** and at least one other PC device of network **100**. In the multi-point access technique, even if PC **1** is in a radio link state in which a connection has already been established, PC **1** may enter one of a number of operational modes. Particularly, PC **1** may enter a station discovery mode to search for a new target terminal, a waiting mode for the station discovery, or a waiting mode to demand an established connection to a discovered target terminal on the network. Thus, the multi-access technique enables a new target terminal to dynamically connect to network **100**.

The station discovery mode enables PC **1** to search for a target terminal that is located in a communication range of PC **1**, and collect information required for connection to the target terminal over network **100**. In the station discovery mode PC **1** broadcasts a message that indicates a station discovery. The waiting mode for a station discovery enables PC **1** to detect a station discovery message transmitted from a target terminal for a station search. PC **1** transmits a message in response to the station discovery message of the target node. The waiting mode for demanding establishment of a connection enables PC **1** to detect a demand for connection establishment message transmitted from a target terminal. PC **1** performs a process in response to the demand for connection establishment message of the target terminal.

PC **1** executes one of the operational modes mentioned above to establish a new radio line to a target terminal on network **100**. The station discovery mode, waiting for the

station discovery mode, and waiting for a demand of connection establishment mode allow PC **1** to transfer messages over a control channel of network **100**. However, when transmitting or receiving data, PC **1** uses a radio resource between the control channel and a communication channel. If PC **1** executes a control process while also communicating with a target device, PC **1** temporarily suspends the communication with the target device. PC **1** dynamically controls execution timings and intervals of control procedures based on conditions designated by a user. Particularly, PC **1** executes station discovery mode, waiting for the station discovery mode, and waiting for a demand of connection establishment mode for establishing a new radio link on network **100**. PC **1** further executes the station connection demand mode to disconnect a radio link with a target device on the network.

FIG. **2** shows a general structure of a complete radio-communication network **200** in accordance with an embodiment consistent with the present invention. Radio communications network **200** includes PC **1**, mobile telephone **2**, a mobile phone base station **3**, a public link network **4**, and a server **5**.

PC **1** includes an antenna unit **8** for communicating information with mobile telephone **2** over network **200**. PC **1** further includes an LCD (not shown) for displaying data and a keyboard for inputting data (not shown).

Mobile telephone **2** includes a mobile phone antenna unit **42** for exchanging information with the mobile-phone base station **3** over an 800 MHz radio wave of network **200**. Mobile telephone **2** further includes a radio antenna unit **34** for exchanging information with PC **1** over a 2.45 GHz radio wave. Mobile telephone **2** also includes a LCD (Liquid Crystal Display) for displaying data and a key operation unit for inputting data.

Mobile phone base station **3** represents a predetermined radio area and facilitates communications from a mobile telephone **2** located within the predetermined radio area. Public link network **4** connects mobile phone base station **3** to server **5**.

Mobile telephone **2** performs transmission and reception of sound or data between mobile phone base station **3**. Mobile phone base station **3** constitutes a predetermined radio area, and realizes communication with a portable telephone **2** within the radio area over the 800 MHz radio wave. Mobile phone base station **3** connects to server **5** through a public link network **4**.

PC **1** and the mobile telephone **2** are coupled by a radio wave of a specific frequency band different from the radio wave used for communication in the mobile-phone system. Practically, the Bluetooth system of 2.45 GHz band is used for coupling between the PC **1** and the mobile telephone **2**. The Bluetooth system is a short-distance radio-communications standard for realizing radio communications around 10 m by using an electric wave of 2.45 GHz band.

FIG. **3** is a block diagram illustrating a hardware structure of PC **1** in accordance with an embodiment consistent with the present invention. PC **1** includes a radio module **7** having an antenna unit **8**, a Radio Frequency (RF) unit **9**, a base band unit **10**, a memory unit **11**, a crystal oscillation unit **12**, an AD/DA conversion unit **13**, and a microphone/speaker unit **14**. PC **1** also includes an engine unit **15** having a Mathematical processing unit (MPU) **17**, a hard disc drive (HDD) **18**, a light emitting diode (LED) **19**, a universal serial bus (USB) **20**, a liquid crystal display (LCD) **21**, a keyboard **22**, and a personal computer memory card international association (PCMCIA) interface **23**. Radio module **7** communicates data with mobile telephone **2** over the 2.45 GHz radio wave on network **200**. Engine unit **15** provides an interface to users and other peripheral devices of network **200**.

Antenna unit **8** provides an interface to radio communication network **200** and exchanges information with mobile telephone **2** over a 2.45 GHz radio wave. For illustrative purposes, antenna unit **8** is assumed to receive a signal over radio communication network **200**.

When antenna unit **8** receives a 2.45 GHz radio wave, RF unit **9** is connected to receive the radio wave on its input from antenna unit **8**. RF unit **9** is also connected to receive an input from crystal oscillation unit **12**. RF unit **9** mixes the 2.45 GHz radio wave input from antenna unit **8** and a base frequency signal input from crystal oscillation unit **12** and produces an intermediate frequency signal. RF unit **9** decodes the intermediate frequency signal and generates a digital signal. RF unit **9** outputs the digital signal to an input of baseband unit **10**. Alternatively, when antenna unit **8** transmits a 2.45 GHz radio wave, RF unit **9** is connected to receive an input from baseband unit **10** and an input from crystal oscillation unit **12**. RF unit **9** modulates the signal received from baseband unit **10** with the base band signal received from crystal oscillation unit **12** to generate a 2.45 GHz radio wave. RF unit **9** provides the 2.45 GHz radio wave on its output to antenna **8**.

When antenna unit **8** receives a 2.45 GHz radio wave, baseband unit **10** is connected to receive an input from RF unit **9**. Baseband unit **10** includes a clock control unit **24** and a serial interface **16**. Using clock control unit **24**, baseband unit **10** changes the data sequences of the digital signals received on its input. Baseband unit **10** provides the modified digital signals to MPU **17** on serial interface **16**. Alternatively, when antenna unit **8** transmits a 2.45 GHz radio wave, baseband unit **10** is connected to receive an input signal from MPU **17** over serial interface **16**. Using clock control unit **24**, baseband unit **10** converts the input signal to a form that can be processed by RF unit **9**. Baseband unit **10** provides the converted signal on its output to RF unit **9**.

Memory unit **11** is connected to receive an input signal from baseband unit **10**. Memory unit **11** stores the received input signal. Alternatively, memory unit **11** may also provide the stored information on its output to baseband unit **10**.

Microphone/speaker unit **14** receives or outputs audio information. When receiving audio information, microphone/speaker unit **14** is connected to provide the received audio signal on its output to AD/DA conversion unit **13**. When outputting audio information, microphone/speaker unit **14** is connected to receive an audio signal on its input from AD/DA conversion unit **13**. Microphone/speaker unit **14** then outputs the received audio signal.

MPU **17** includes among other things a central processing unit (CPU), a memory, and a peripheral control circuit. When antenna **8** receives a 2.45 GHz radio wave, MPU **17** is connected to receive an input from baseband unit **10** through serial interface **16** and provide an output to at least one of HDD **18**, LED **19**, USB **20**, LCD **21**, or PCMCIA **23**. Alternatively, when antenna **8** transmits a 2.45 GHz radio wave, MPU **17** is connected to receive an input from one of HDD **18**, USB **20**, LCD **21**, keyboard **22**, or PCMCIA **23**. MPU **17** then provides a signal to baseband unit **10** through serial interface **16**. It should be apparent that MPU **17** may provide an output to at least one of HDD **18**, LED **19**, USB **20**, LCD **21**, or PCMCIA **23** regardless of a communication state of antenna **8**.

When antenna **8** receives a 2.45 GHz radio wave over network **200**, HDD **18** is connected to receive a signal from

MPU **17**. HDD **18** then stores the received signal. Alternatively, when antenna **8** transmits a 2.45 GHz radio wave over network **200**, HDD **18** may provide a signal on its output to MPU **17**.

LED **19** is connected to receive an input from MPU **17**. LED **19** emits a visible colored light based on the input received from MPU **17**. Particularly, LED **19** is used to indicate warnings regarding the operation of PC **1**.

USB **20** is connected to receive an input from MPU **17**. USB **20** connects peripheral devices (not shown) supporting the USB standard to PC **1**. When directed by MPU **17**, USB **20** provides signals on its output to the connected peripheral device. Alternatively, USB **20** is connected to receive an input from a connected peripheral device. USB **20** may provide signals on its input as an output to MPU **17**.

LCD **21** is connected to receive an input signal from MPU **17**. LCD **21** provides the input signal as an output so that information can be displayed to a user.

Keyboard **23** provides an interface between a user and PC **1**. A user may input information onto keyboard **323** by depressing at least one of a plurality of keys (not shown). Keyboard **23** provides the signal generated by the depressed keys on its output to MPU **17**.

PCMCIA **23** is connected to receive an input signal from MPU **17**. PCMCIA **23** provides an interface for mounting a PC card. PCMCIA **23** provides the input signal on its output to the mounted PC card. Alternatively, PCMCIA **23** is connected to receive an input signal from a mounted PC card. PCMCIA **23** provides the input signal on its output to MPU **17**.

FIG. **4** is a block diagram illustrating a software structure of PC **1** in accordance with the present invention. Because hardware components of PC **1** have been previously discussed, only the software components will be described below. PC **1** includes radio module **7** having RF unit **9**, baseband unit **10**, a Link Management Protocol (LMP) unit **25**, and a Host Control Interface (HCI) **26**. PC **1** also includes engine unit **15** having an operating system (OS) **27**, driver software **28**, a service program **29**, a radio protocol stack **30**, an HCI **31**, and clock control information **32**.

LMP **25** is configured to monitor an output of baseband unit **10**. LMP **25** controls a radio link between PC **1** and other radio communication equipment of network **200**, by analyzing information communicated over the 2.45 GHz radio wave. Through the analysis, LMP **25** determines whether a radio link between PC **1** and, for example, mobile telephone **2** exists. LMP **25** is further configured to provide results of this analysis to HCI **26**.

HCI **26** is configured to receive an input from LMP **25**. Alternatively, HCI **26** is also configured to provide an input received from the software components of engine unit **15** to LMP **25**. HCI **26** provides a serial interface between the software components of engine unit **15** and LMP **25**.

OS **27** is configured to provide an environment in which various software processes of engine unit **15** can be executed.

Driver software **28** is configured to control a number of peripheral hardware elements of engine unit **15**, such as HDD **18**, LED **19**, USB **20**, LCD **21**, keyboard **22**, and PCMCIA **23**. Driver software **28** is further configured to control word-processing software, spreadsheet software, electronic mail software, and system software used for recognizing remote-control operations.

Service program **29** is configured to monitor or control specific functions or hardware components associated with engine unit **15**.

Radio protocol stack **30** is configured to control communication over the 2.45 GHz frequency band by storing information received through HCI **31**. Radio protocol stack **30** controls the flow of information between the service program **29** and driver software **28** mounted on engine unit **15** and LMP **25** mounted on radio module **7**. Clock control information **32** is a sub-component of radio protocol stack **30** and is configured to control the timing of all processes input or output from the radio protocol stack **30**.

HCI **31** is configured to receive an input from radio protocol stack **30**. Alternatively, HCI **31** is also configured to provide an input received from the software components of radio module **7** to radio protocol stack **30**. HCI **31** provides a serial interface between the software components of radio module **7**.

FIG. **5** is a block diagram illustrating a hardware structure of mobile telephone **2** in accordance with an embodiment consistent with the present invention.

Mobile telephone **2** includes a radio module unit **33** having a radio antenna unit **34**, an radio RF unit **35**, a radio base band unit **36**, which includes a clock control unit **37** and a serial interface **41**, a memory unit **38**, and a crystal oscillation unit **39**. Mobile telephone **2** further includes a mobile phone engine part **40** having an antenna unit **42**, an RE unit **43**, a baseband unit **44** that includes a serial interface **520**, an LCD **45**, a key operation unit **46**, an LED **47**, and a memory unit **48**. Mobile telephone unit **2** also includes a common unit **49** having an AD/DA conversion unit **50**, a microphone/speaker unit **51**, and a power source **52**. Radio module unit **33** communicates with PC **1** over radio communication network **200** using a 2.45 GHz band radio wave. Mobile phone engine part **40** is connected to radio module unit **33** through a serial interface and serves as an interface to a user or other peripheral devices (not shown). Power unit **49** provides an audio interface and a power source for mobile telephone **2**.

Radio antenna unit **34** is connected to radio communication network **200** through a radio link (not shown). Radio antenna unit **34** transmits and receives a 2.45 GHz radio wave between PC **1** over the radio link. Radio antenna unit **34** provides the received radio wave on its output to radio RF unit **35**.

Radio RF unit **35** is connected to receive an input from radio antenna unit **34**. Radio RF unit **35** is also connected to receive baseband signal input from crystal oscillation unit **39**. Radio RF unit **35** modulates the received radio wave from radio antenna unit **34** with the baseband signal received from crystal oscillation unit **39**, to convert the radio wave into an intermediate frequency signal. Following the conversion, radio RF unit **35** demodulates the intermediate signal to generate a digital signal. Radio RF unit **35** provides the digital signal on its output to radio baseband unit **36**. Alternatively, when mobile telephone **2** desires to transmit a radio wave over radio communication network **200**, radio RF unit **35** receives a digital signal from radio baseband unit **36**. It should be understood that radio RF unit performs the reverse operations as described above, and provides a 2.45 GHz radio wave on its output to radio antenna unit **34**.

Radio baseband unit **36** is connected to receive a digital signal output from radio RF unit **35**. Radio baseband unit **36** is also connected to receive a signal output from memory unit **38**. Furthermore, radio baseband unit **36** is connected to receive an input from power unit **49**. Additionally, radio baseband unit **36** is connected to receive an input from engine unit **40**. Radio baseband unit **36** includes a clock control unit **37** and a serial interface **41**. When sending data through serial interface **41**, radio baseband unit **36** converts

the digital signal received from radio RF unit **35** into a data sequence so that a CPU (not shown) of mobile telephone engine unit **40** may process the data. Clock control unit **37** determines the timing for sending and receiving a data sequence over serial interface **41**. On the other hand, radio baseband unit **36** provides the received digital data on its output to mobile telephone engine unit **40** and power unit **49**. Alternatively, when mobile telephone unit **2** desires to transmit a radio wave over radio communication network **200**, radio baseband unit **36** receives a data sequence from at least one of the power unit **49** or the mobile telephone engine unit **40**. Radio baseband unit **36** performs the reverse of the operations described above, and provides a digital signal on its output to radio RF unit **35**.

The components of mobile telephone engine unit **40** will now be discussed. Mobile phone antenna unit **42** communicates with mobile-phone base station **3**. Mobile phone antenna transmits and receives information over an 800 MHz radio wave. Mobile phone antenna unit **42** provides the received 800 MHz radio wave on its output to mobile phone RF unit **43**.

Mobile phone RF unit **43** is connected to receive the 800 MHz radio wave output from mobile phone antenna unit **42**. Mobile phone antenna unit **43** demodulates the received radio wave to generate a digital signal. Mobile phone RF unit **43** provides the digital signal on its output to mobile telephone baseband unit **44**. Alternatively, when mobile telephone unit **2** desires to transmit information to mobile-phone base station **3**, mobile phone RF unit **43** receives a digital signal output from mobile telephone baseband unit **44**. It should be understood that mobile phone RF unit **43** performs, in reverse order, the operations described above. Mobile phone RF unit **43** provides an 800 MHz radio wave on its output to mobile phone antenna unit **42**.

Mobile telephone baseband unit **44** is connected to receive an input signal from radio module unit **33** and power unit **49**. Mobile telephone baseband unit **44** is also connected to receive an input from key operation unit **46**, LED **47**, and memory unit **48**. Mobile telephone baseband unit **44** controls the flow of information within mobile telephone engine unit **40**. When mobile telephone unit **2** desires to send the information received by mobile telephone baseband unit **44** to mobile phone base station **3**, mobile telephone baseband unit **44** will provide the received signal on its output to mobile phone RF unit **43**. Alternatively, when the received information is targeted to a user, mobile telephone baseband unit **44** may provide the data to at least one of LED **47**, LCD **45**, radio module unit **33** through serial interface **520**, and power unit **49**.

LCD **45** is connected to receive an input from mobile telephone baseband unit **44**. LCD **45** provides the received input signal on its output so that information can be displayed to a user.

Key operation unit **46** provides an interface for a user. Key operation unit **46** converts the user's input into a signal to provide on its output to mobile telephone baseband unit **44**.

LED **47** is connected to receive an input from mobile telephone baseband unit **44**, LCD **45**, key operation unit **46**, and memory unit **48**. LED **319** is used to indicate warnings regarding the operation of mobile telephone unit **2**.

Memory unit **48** is connected to receive an input from mobile telephone baseband unit **44**. Memory unit **48** stores the received input until the mobile telephone baseband unit **44** requests the information.

Turning now to power unit **49**, AD/DA conversion unit **50** is connected to receive an analog signal from microphone/speaker unit **51**. AD/DA conversion unit **50** is also connected to receive a digital signal from radio module unit **33** and mobile telephone engine unit **40**. AD/DA conversion unit **50** converts the received analog signal to a digital signal and provides the digital signal on its output to radio module unit **33** and mobile telephone engine unit **40**. Alternatively, AD/DA conversion unit **50** converts the received digital signal to analog and provides the analog signal on its output to microphone/speaker unit **51**.

Microphone/speaker unit **51** receives or outputs audio information. When receiving analog audio information, microphone/speaker unit **51** is connected to provide the received analog signal on its output to AD/DA conversion unit **50**. When outputting audio information, microphone/speaker unit **51** is connected to receive an analog audio signal on its input from AD/DA conversion unit **50**. Microphone/speaker unit **51** then outputs the received audio signal.

Power source **52** is mounted to provide a source of power for allowing mobile telephone **2** to perform the functions as discussed above.

FIG. **6** shows a block diagram illustrating a software configuration of mobile telephone **2** in accordance with an embodiment of the present invention. Mobile telephone **2** includes radio module **33** having software elements LMP **53** and HCI **54**, and mobile phone engine part **40** having software elements mobile telephone protocol stack **55**, service program **56**, radio protocol stack **57**, and clock control information **59**.

LMP **53** is configured to monitor an output of baseband unit **37**. LMP **53** controls a radio link between mobile telephone **2** and mobile phone base station **3** of radio communication network **200**, by analyzing information communicated over an 800 MHz radio wave. Through the analysis, LMP **53** determines whether a radio link exists between mobile phone **2** and, for example, mobile phone base station **3**. LMP **53** is further configured to provide results of this analysis to HCI **54**.

HCI **54** is configured to receive an input from LMP **53**. Alternatively, HCI **54** is also configured to provide an input received from the software components of mobile engine unit **40** to LMP **53**. HCI **54** provides a serial interface between the software components of engine unit **40** and LMP **53**.

Mobile telephone protocol stack **55** is configured to control communication over the 800 MHz frequency band by storing information received through HCI **54**. Mobile telephone protocol stack **55** controls the flow of information between the service program **56** mounted on engine unit **40** and LMP **53** mounted on radio module **33**. Clock control information **59** is configured to control the timing of all processes input or output from the radio protocol stack **59**.

Service program **56** is configured to monitor or control specific functions or hardware components associated with engine unit **40**.

Radio protocol stack **57** is configured to, control communication over the 2.45 GHz frequency band by storing information received through HCI **54**. Radio protocol stack **57** controls the flow of information between the service program **56** mounted on engine unit **40** and LMP **53** mounted on radio module **33**. Clock control information **59** is configured to control the timing of all processes input or output from the radio protocol stack **59**.

HCI **58** is configured to receive an input from mobile telephone protocol stack **55** and radio protocol stack **57**. Alternatively, HCI **58** is also configured to provide an input received from the software components of radio module **33**

to mobile telephone protocol stack **55** or radio protocol stack **55**. HCI **58** provides a serial interface between the software components of radio module **33** and either of mobile telephone protocol stack **55** and radio protocol stack **57**.

The features of an embodiment consistent with the present invention that enables loading and unloading of service information processes are explained in detail below. In the discussion that follows it is assumed that Bluetooth is used as a radio-communications standard using a 2.45 GHz frequency band.

In the Bluetooth system, data transmission is achieved by a Time-Division Duplex (TDD) packet transmission of 625 microseconds per slot. Bluetooth uses a frequency hopping technique that changes a frequency for each transmitted packet. By using the same frequency hopping sequence, it becomes possible for one master to communicate with a maximum of seven slaves at the same time. A radio communication network configured in such a manner is known as a Piconet. Bluetooth further provides an asynchronous data channel (ACL: Asynchronous Connection Less) and a synchronous voice channel (SCO: Synchronous Connection Oriented) for data communications. The SCO can use up to three channels at once, each channel having a 64 Kbps channel throughput.

In Bluetooth, when a source terminal requests to communicate with a target terminal, but does not know an address of the target terminal, the source terminal performs an Inquiry for collecting information necessary to establish a connection. The Inquiry is also referred to as a station discovery. While performing the Inquiry, the source terminal may collect all device addresses and clock control information on all terminals that respond to the Inquiry. Because of the responses, the source terminal may establish a connection by executing a Page process (demand for connection establishment) based on the information collected from the responding terminals. Further, a remote terminal that is discovered by the source terminal performs an Inquiry Scan (waiting for station discovery) to answer the Inquiry message. Furthermore a remote terminal that is in a waiting state for a demand for connection establishment mode performs a Page Scan (waiting for a demand for connection establishment), to respond to the Page of the source terminal.

FIG. **7** illustrates a plurality of functional elements of PC **1** that enable the Bluetooth system to be mounted in accordance with an embodiment of the present invention. For illustrative purposes, we assume that PC **1** is a host device. PC **1** includes an information memory domain **76** having a service program **77**, driver software **78**, connection control information **79** and clock control information **84**. PC **1** also includes a host **70** having a service manager **72**, a connection manager **73**, a Bluetooth driver **74**, a setup program **75**, an OS **83**, and temporary memory **85**. PC **1** further includes a host controller **71** having a Bluetooth link manager **80** and a Bluetooth link controller **81**, and a Bluetooth RF circuit **82**.

The host **70** and information memory domain **76** permanently reside at host PC **1**. Host **70** and host controller **71** communicate in accordance with the protocol set forth by HCI **26** and **31**. Bluetooth link manager **80** and Bluetooth link controller **81** control operations of the Bluetooth RF circuit **82**. The Bluetooth device (non shown) is connected to PC **1** through USB **20**.

Connection control information **79** defines detection conditions for a link connection state.

Clock control information **84** is used to determine when various operations should be executed.

Service manager **72** accesses information memory domain **76** to read stored service information, for example, service program **77** and driver software **78**. Service manager **72** loads the service information read from service program **77** and driver software **78** to temporary memory **85** of host device **70**. Service manager **72** may unload the service information from temporary memory area **85** as needed.

Connection manager **73** connects the temporary memory area **85** and the service information stored in a target device (not shown) so that service information can be communicated. Communication manager **73** monitors the connection state of a radio link based on communication control information **79**.

FIG. **11** shows a chart illustrating the contents connection control information **79**. Connection control information **79** includes a device address, a friendly name that is arbitrarily defined by a user to identify a device, connection judging conditions, and disconnection judging conditions. Connection judging conditions define conditions for determining whether a host device establishes a radio link with a target device. The connection conditions include a number of times (N) the same device issues Inquiry, an issue interval (Ti) of Inquiry, and a number-of-times maintenance time (Tn=N× Ti) expires before a response is detected, which is based on the Inquiry issue number-of-times (N) and the Inquiry issue interval (Ti). Specifically, service manager **72** loads service information when a response is detected before the predetermined number of times device detection is performed (i.e., after the number-of-times the maintenance time (Tn) ms has expired). If the loading time is shorter than the detected number-of-times the maintenance time (Tn) expires, then the loading process is determined to be unnecessary and is omitted. Host PC **1** determines that there is a low possibility for communication of the service information by establishing a radio link.

The disconnection judging conditions are conditions for determining whether host PC **1** disconnects a radio link with a target device. The disconnection judging conditions include a number-of-times (M) a connection request for recovering the connection is issued after host PC **1** detects a disconnection of a radio link, an issue interval (Tj) of the connection request, and a number-of-times the maintenance time (Tm=M×Tj) expires before a response is detected, which is based on the number-of-times (M) a connection request is made and the connection request issue interval (Tj). Thus, even if host PC **1** disconnects a radio link once, it is possible for host PC **1** to re-establish a connection with the radio link when a response to a connection request is received within a predetermined number of times before the maintenance time expires. PC **1** may, therefore, restrain the number of times service information is loaded because of an unnecessary radio link disconnection.

FIG. **8** explains a connection/disconnection state of a radio link between PC **1** and a mobile telephone **2** on network **200** using Bluetooth technology. In FIG. **8**, a boundary **2** designates a range limit of radio waves transmitted from the PC **1**. A boundary **1** designates an area outside of the range limit of radio waves transmitted by PC **1**. A boundary **3** designates an area inside of the range limit of radio waves transmitted by PC **1**.

In a first example, it is assumed that mobile telephone **2** is initially located in an area outside of boundary **1**.

When the mobile telephone **2** is located in a location outside of the boundary **2**, a radio link between PC **1** and mobile telephone **2** is not established because mobile telephone **2** is unable to answer a device detection (Inquiry) broadcast by PC **1** over radio communication network **200**. Assuming, mobile telephone **2** moves along locus A when mobile telephone **2** crosses boundary **2**, mobile telephone **2**

responds to the device detection (Inquiry). After receiving the response from mobile telephone **2**, PC **1** begins a connection judging process of the radio link. If the PC **1** detects that the responses corresponding to each Inquiry occurs N number of times within a detection maintenance time (Ti) ms, then PC **1** loads service information, and further communicates with mobile telephone **2**.

An analysis of the radio link will now be made assuming that mobile telephone **2** moves along a locus B. As shown in FIG. **8**, when traveling along locus B mobile telephone **2** initially moves toward PC **1**, but reverses direction so that it moves in a direction away from PC **1**. As previously stated, mobile telephone **2** cannot establish a radio link when it is located outside of boundary **2**, because PC **1** cannot receive a response to the device detection (Inquiry). However, PC **1** receives a response to the device detection (Inquiry) from mobile telephone **2** and establishes a radio link, when mobile telephone **2** moves in a direction towards PC **1** and crosses boundary **2**. As a result, PC **1** begins a judging process to determine the connection state of the radio link. However, as shown in locus B, while PC **1** judges the radio link, mobile telephone **2** suddenly changes directions and moves away from PC **1**, until it is located outside of boundary **2**. Because mobile telephone **2** cannot respond to the device detection of PC **1**, when a predetermined number of responses to the device detection have not occurred within a specified time, PC **1** determines that connection conditions do not exist. Therefore, PC **1** does not perform a loading process of service information.

In contrast, under the conventional process, when a mobile telephone **2** moves into a location within boundary **2**, PC **1** begins loading service information. Moreover, when mobile telephone **2** moves to a location outside of boundary **2**, PC **1** immediately unloads service information. As a result, PC **1** performs unnecessary loading and unloading of service information. PC **1** also performs excessive communications with mobile telephone **2**. From the above discussion it is apparent that the conventional process decreases communication performance.

In a second example, it is assumed that mobile telephone **2** is initially located inside of boundary **3**.

Initially, PC **1** establishes a radio link with mobile telephone **2** because mobile telephone **2** is in a location within boundary **2**. Assuming, now that mobile telephone **2** moves along a locus C, in a direction away from PC **1**, when mobile telephone **2** crosses boundary **2**, PC **1** detects a disconnection of the radio link. As a result, PC **1** transmits a connection request to the mobile telephone **2**, indicating that the radio link is disconnected. PC **1** monitors radio communication network **200**, to determine whether N responses are detected within a maintenance time (Tm) ms. However, because mobile telephone **2** is located outside of boundary **2**, PC **1** does not receive N response within the maintenance time. Thus PC **1** disconnects the radio link. At the same time PC **1** disconnects the radio link, service manager **72** of PC **1** unloads the service information. Before disconnection of the radio link, PC **1** and mobile telephone **2** communicated the service information over radio network **200**.

An analysis of the state of the radio link between PC **1** and mobile telephone **2** will now be made assuming that mobile telephone **2** travels in a direction shown by locus D. Initially, because mobile telephone **2** is located within boundary **2**, PC **1** establishes a radio link with mobile telephone **2**. When the mobile telephone **2** moves in a direction away from PC **1** to a location outside of boundary **2**, PC **1** detects a disconnection of the radio link. As a result, PC **1** transmits a connection request to mobile telephone **2**, indicating that the radio link is disconnected. PC **1** monitors radio network **200** for response from mobile telephone **2** to determine whether N responses are detected within a predetermined maintenance time (Tm) ms. If, however, mobile telephone **2** moves in a direction towards PC **1** to a location within boundary **2**, mobile telephone **2** responds to the connection request of PC **1**. Because PC **1** detects a response within the predetermined maintenance time, PC **1** maintains the radio link.

FIGS. **9** and **10** show a flow diagram illustrating the connection judging process and disconnection judging process, respectively, in a manner consistent with the present invention.

During the connection judging process shown in the flow chart of FIG. **9**, service manager **72** of PC **1** sends an HCI command to host controller **71**. Service manager **72** further performs an Inquiry so that a device may be discovered on network **200**. Service manager **72** acquires a device address, clock control information, and service demand information from a target device on network **200** (S**100**). PC **1** then determines whether the detected target device address is registered into connection control information **79** of information memory domain **76** (S**101**). If, PC **1** determines that the detected target device address is not registered in connection control information **79**, then the connection judging process moves to S**102**. On the other hand, if PC **1** determines that the detected device address is registered in connection control information **79**, then the connection judging process moves to S**105**.

At S**102**, because the connection control information corresponding to the detected target device address is not registered, PC **1** asks a user whether connection conditions and disconnection conditions are required to be setup and registered. If a user answers "yes," PC **1** performs an appropriate setup/registration processes (S**103**). If a user answers "no," then PC **1** does not perform the setup process (S**104**) and default connection/disconnection conditions of network **200** are associated with the detected target device and copied into connection control information **79**. This process is performed so that the newly detected target device address is associated with at least standard connection conditions.

The process step performed at S**103**, is explained in further detail in FIG. **12**. FIG. **12** illustrates an example of a condition set-up screen as displayed on LCD **21** of PC **1**. Keyboard **22** enables a user to input the necessary data. A user may optionally input a friendly name of the device as an entry in the condition setup object. A user may indicate connection detecting condition set-up items including a number of times (N) an Inquiry should issue, an issue interval (Ti), and a detection number for the maintenance time (Tn). A user may also indicate disconnection detecting conditions setup items including a number-of-times a connection request should issue request (M), an issue interval (Tj), and a detection number for a maintenance time (Tm).

Furthermore, the condition set-up screen enables a user to indicate an inquiry detection mode, which allows the connection request inquiry detection interval to be fixed or variable. In Bluetooth, a user may also dynamically vary an issue interval of the inquiry or connection request. When a user sets a variable inquiry detection mode, thereby giving priority to the detection number of the maintenance time of detection number-of-times, a host device may connect or disconnect a radio link even when the number of issued inquiries fails to meet the predetermined level. Moreover, a user may give priority to the inquiry detection mode or the connection request detection mode by selecting a fixed state. When a user completes the condition setup, a "Registration"

button may be selected so that an address may be assigned to the previously detected target device. Furthermore, selecting the "Registration" button saves the condition setup information in connection control information **79**. If a user selects a "Cancellation" button, then processing is terminated without saving the contents of the condition set up screen. It is further possible to change the setup items of any devices by selecting a triangle mark in the right column of the condition setup object field. This enables a user to select a detection device from a list of friendly names registered to each respective device in connection control information **79**.

Returning now to FIG. **9**, at S**105** the connection judging conditions based on the detected device address are read from connection control information **79**, and the device discovery process continues based on the read conditions (S**105**). At step S**106**, the host device detects whether the number of times of inquiry is less than N. When the number of times of Inquiry detection is not less than N, the process returns to S**105**. Alternatively, when the number of times of Inquiry detection is less than N, processing progresses to S**107**. At S**107**, the host loads information from service program **77** or driver software **78** in information memory area **76** that corresponds to the service information demanded from the detected device to temporary memory area **85**. As a result, the host device may communicate with the detected device side. By performing the above process, PC **1** prevents the unexpected loading of service information when a mobile telephone **2** enters a communication area of PC **1**. Furthermore, PC **1** avoids an increase in communication loads with mobile telephone **2**.

FIG. **10** shows a flow chart illustration of the disconnection judging process. Connection manager **73** of PC **1** monitors the connection state of a radio link with a mobile telephone **2**, based on a notice from Bluetooth driver **74** (S**110**). Connection manager **73** determines whether the radio link has disconnected (S**111**). When the radio link has disconnected, connection manager returns to S**110** in order to continue monitoring the connection state of the radio link. If radio link disconnection is detected, however, connection manager **73** progresses to S**112**. At S**112**, service manger **72** identifies a device address for the disconnected link (S**112**), and connection manager **73** monitors a radio link connection state by reading out the disconnection judging conditions in connection control information **79** associated with the device address (S**113**). When the number of detected connection requests is less than M, connection manager **73** returns to S**113** in order to continue monitoring the connection state of the radio link. When the number becomes M times, the process progresses to a step S**114**. When the number of detected connection requests is not less than M, connection manager **73** confirms disconnection of the radio link, because no response was received from a target device. Service manager **72** unloads service information from temporary memory area **85**(S**115**). By performing this control, PC **1** avoids unnecessary loading or unloading of operations of the service information, because connection manager **73** maintains a radio link connection if mobile telephone **2** sends a response within a predetermined time period. As shown in FIG. **8**, even if, after the radio link is established, mobile telephone **2** temporarily moves outside of a communication range of the PC **1**, connection manager **73** will maintain a radio link connection if mobile telephone **2** sends a response within a predetermined time period. Thus, PC **1** also avoids an increase of processor loads and can further avoid an increase of radio-communications load with a mobile telephone **2**.

As explained above, embodiments consistent with the present invention enable a user to flexibly setup the connection or disconnection judgment conditions of the radio link state. As a result, it is possible to increase communications processing performance without increasing the processing load of the host device or the communication load due to a target device.

In the above embodiment, the connection condition and disconnection condition of the radio link state was determined based on the number of times of Inquiry and the number of times a connection request are issued within a predetermined time. However, it is also possible to determine a radio link state based on an intensity of a radio wave. For example, in an embodiment of the present invention, a user may setup a power level of the radio wave. In other words, by gradually changing the power level of the radio wave, a user may define the detection range of PC **1** by the boundaries **1**, **2**, and **3**, as shown in FIG. **8**. Here, the radio wave detection range of the standard power level **2** is limited to boundary **2**.

When mobile telephone **2** approaches PC **1** in a direction defined by locus A, if PC **1** performs device detection at each stage from a boundary **1** (power level **1**) to a boundary **3** (power level **3**), PC **1** loads the service information by determining whether mobile telephone **2** desires to establish a radio link connection to PC **1**. On the other hand, when PC **1** does not detect a device between boundary **1** (power level **1**) and boundary **2** (power level **2**), as shown by the direction traveled along locus B, PC **1** does not load the service information by determining that mobile telephone **2** has only temporarily came near to PC **1**.

In another example, when mobile telephone **2** travels in a direction away from PC **1** as shown by locus C, PC **1** determines that the mobile telephone **2** has intentionally separated from PC **1**. As a result, PC **1** disconnects the radio link. Moreover, service manager **72** unloads the service information from temporary memory area **85**. When mobile telephone unit **2** travels in a direction away from PC **1** to a location outside of boundary **2** (locus D), PC **1** determines that the mobile telephone **2** temporarily separated from PC **1**. As a result, PC **1** does not disconnect the radio link.

Although an embodiment has been disclosed that includes the loading/unloading control of service information as it relates to PC **1**, it should be apparent that this process might also be applied to mobile telephone **2**. Moreover, it should be understood that this process is not limited to devices such as PC **1** and mobile telephone **2**. But the loading/unloading control of service information consistent with the present invention may be applied to various other electrical devices having a radio resource that is exclusively used between a communication channel and where a connection is controlled by inserting a communication channel into a control channel for the devices.

As explained above, embodiments consistent with the present invention can prevent unnecessary loading and unloading of service information processes because it is possible to flexibly set up the connection judgment conditions and disconnection judgment conditions of the host device as they relate to the radio link. As a result, communication-processing performance is improved without increasing the processing load of the host device or the communication load of host device with regards to a target device.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered

as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

What is claimed is:

1. A communication device, comprising:

a radio communication module configured to exchange data with a target communication terminal over a network;

a service information memory configured to store service information so that predetermined functions can be performed with the target communication terminal;

a communication control information designating module configured to designate, by a user of the communication device, communication conditions for a newly established radio communication connection with the target communication terminal or for discriminating a disconnection of an existing radio communication connection with the target communication terminal;

a memory configured to store the communication conditions designated by the communication control information designating module; and

a communication control module configured to determine whether the radio communication connection with the target communication terminal is in a connection status or a disconnection status based on the communication controlling information stored in the memory, and performing communication through the radio communication module by using service information read from the service information memory in accordance with the determination result.

2. A communication device, comprising:

a radio communication module configured to exchange data with a target communication terminal through radio;

a service memory configured to store service information so that predetermined functions can be performed with the target communication terminal;

a temporary memory configured to temporarily store service information used in an established target communication terminal for communication;

a designating module configured to designate, through a registration interface, communication controlling information defining conditions for discriminating between a newly established radio communication connection with the target communication terminal or a disconnection of an existing radio communication connection with the target communication terminal;

a communication controlling information memory configured to store the communication controlling information designated by the designating module;

a memory configured to store the communication controlling information designated by the designating module;

a discriminating module configured to determine whether a status of the radio communication connection with a target communication terminal is a connection status or a disconnection status based on the communication controlling information in the communication controlling information memory, to transfer the service information from the service memory to the temporary memory when the status of the radio communication connection with the target communication terminal is the connection status, and to transfer the service information from the temporary memory to the service memory when the status of the radio communication connection with the target communication terminal is the disconnection status; and

a radio communication control module configured to perform the predetermined functions with the target communication terminal when the service information is stored in the temporary memory.

3. The communication device according to claim **1** or claim **2**, wherein:

the communication controlling information includes connection discriminating conditions based on the number of times a detecting command for detecting the target communication terminal issues during a predetermined period and disconnection discriminating conditions based on the number of times a confirming command for confirming the connection to the target communication terminal issues during the predetermined period.

4. The communication device according to claim **1** or claim **2**, wherein:

the communication controlling information includes connection and disconnection discriminating conditions that define a variation status of the radio communication connection for indicating a communication connection or a disconnection to the target communication terminal, the variation status is designated based on a power level of radio waves measured within a predetermined period.

5. A method for controlling a communication device that exchanges data with a target communication terminal over a network, the communication device having a memory for storing various types of data, the method comprising:

designating, by a user of the communication device, communication control information that defines discriminating conditions for discriminating between establishing a new radio communication connection between the communication device and a target communication terminal and disconnecting a radio communication connection established between the communication device and the target communication terminal;

storing, in the memory, the designated communication control information;

judging whether the radio communication connection between the communication device and the target communication terminal is in a connection state or a disconnection state based on the designated communication control information; and

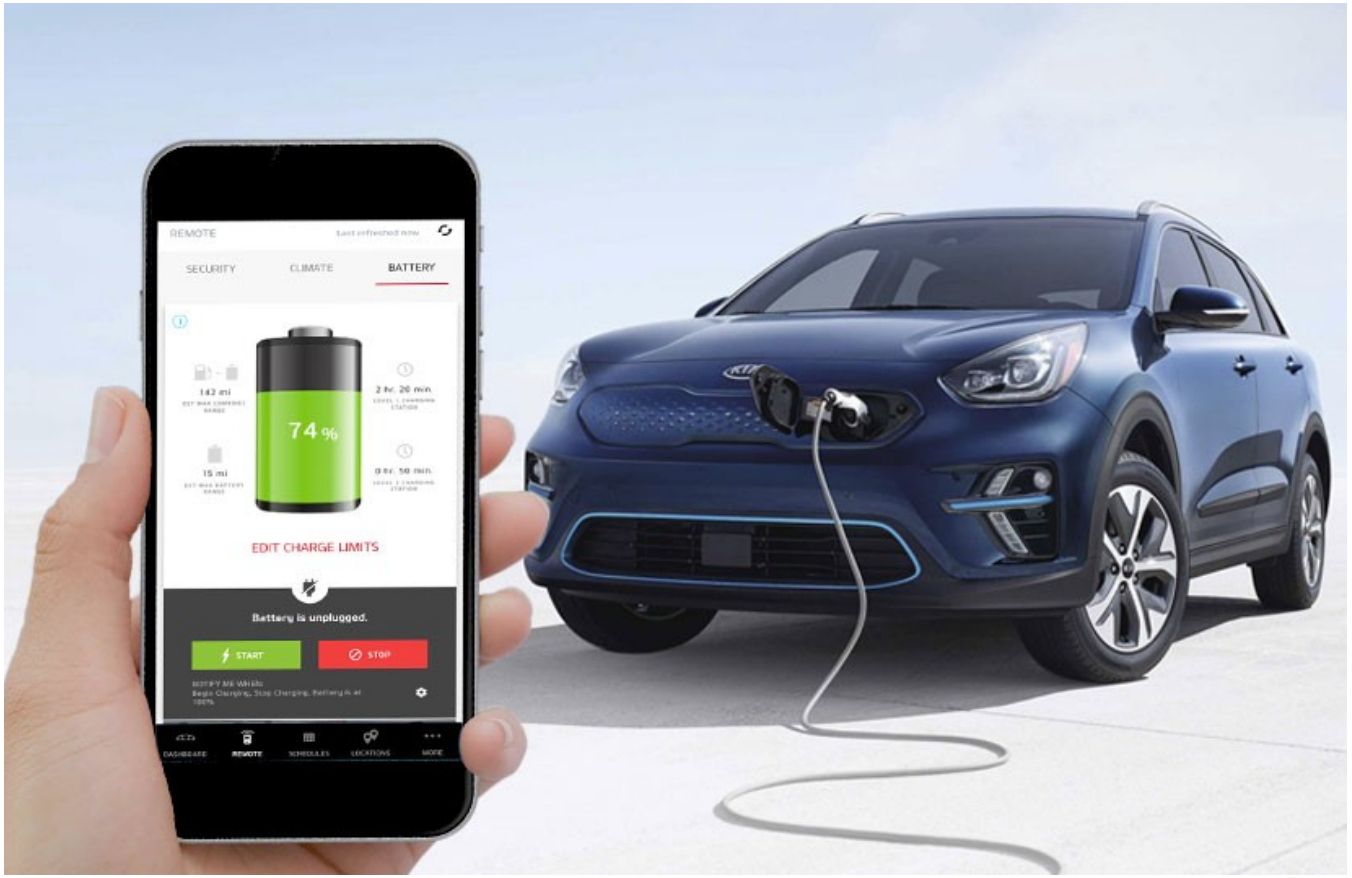
performing radio communication with the target communication terminal by using service information that executes predetermined functions between the communication device and the target communication terminal, the service information being stored in memory based on a discrimination result.

* * * * *

EXHIBIT 5

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

Kia Hybrid/Electric Vehicles (using Kia UVO Smartphone App)



Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

1. A device comprising:

a battery which supplies power to a communication section which communicates with an information processing apparatus;

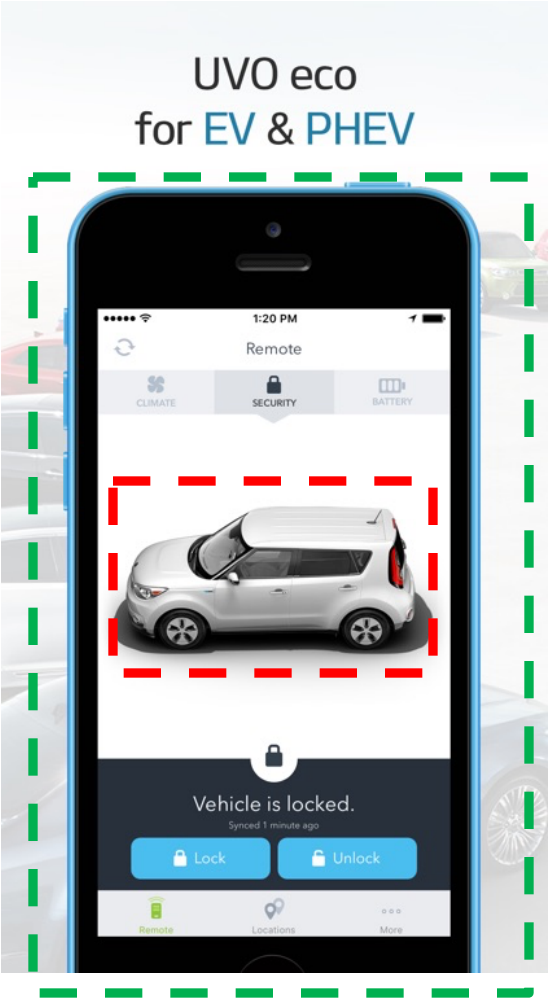
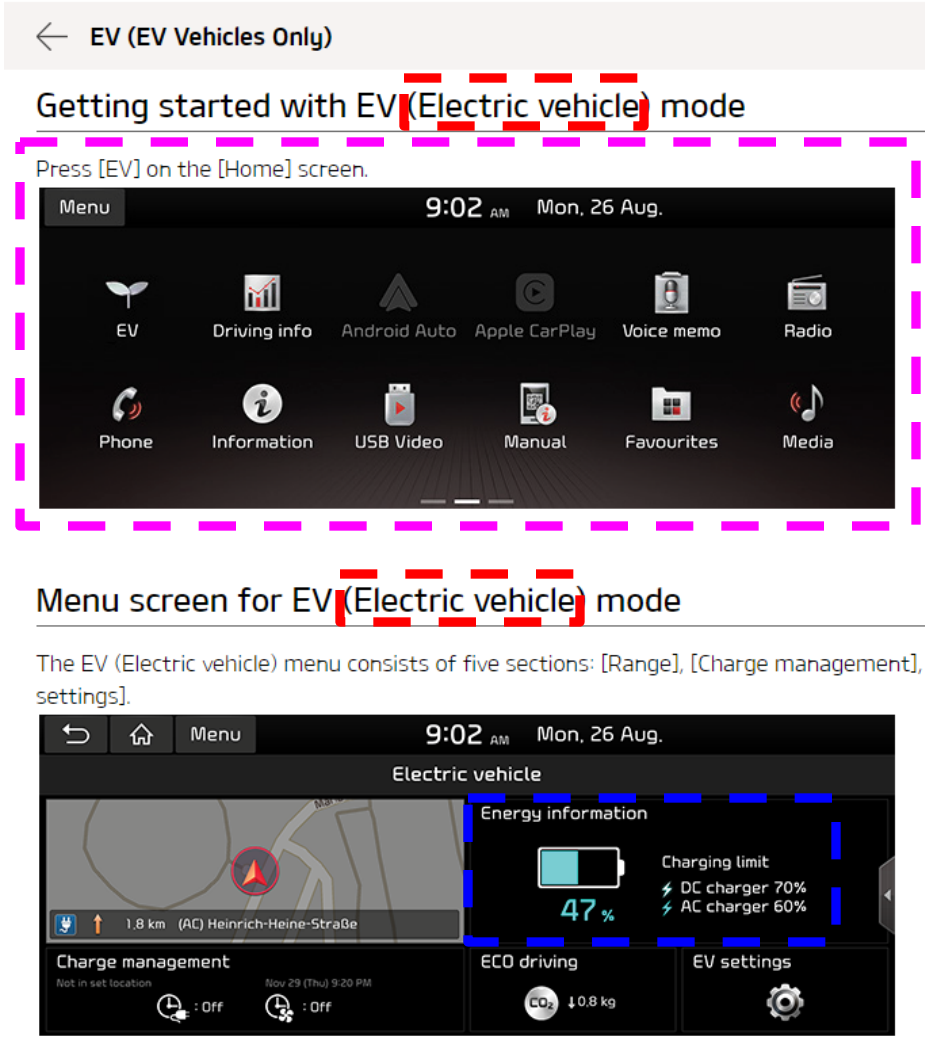
means for receiving, from the information processing, apparatus, a setting information representing at least one of a notifying method for information about remaining energy of said battery, or level of remaining energy of said battery at which a warning is to be displayed on the information processing apparatus; and

means for storing the received setting information; and

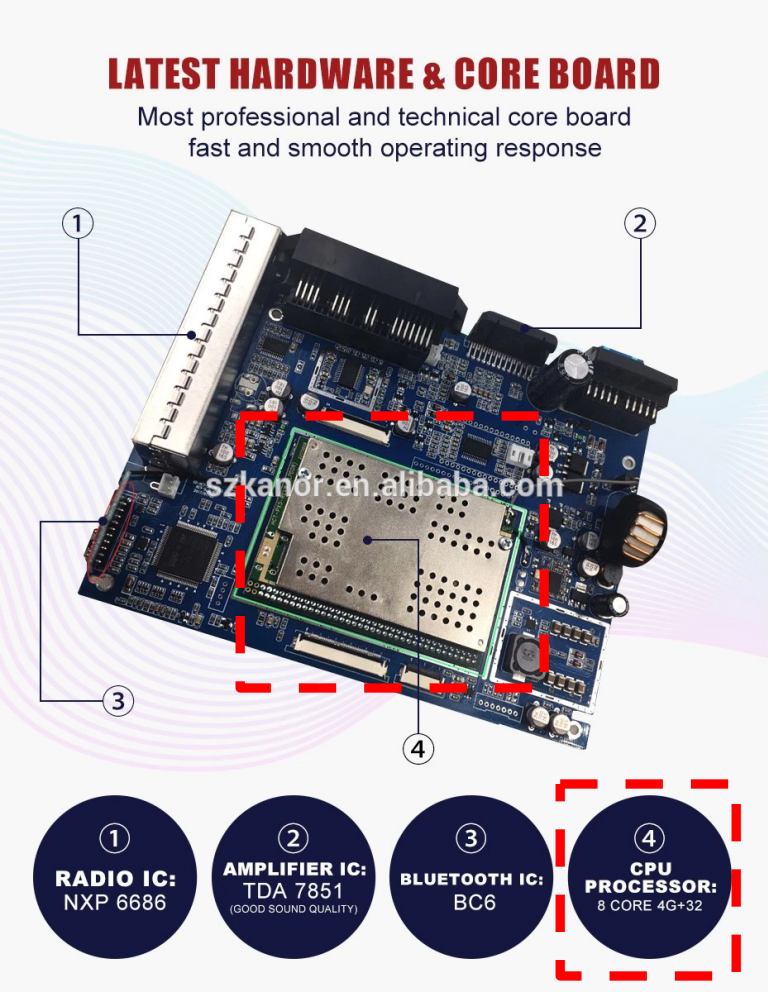
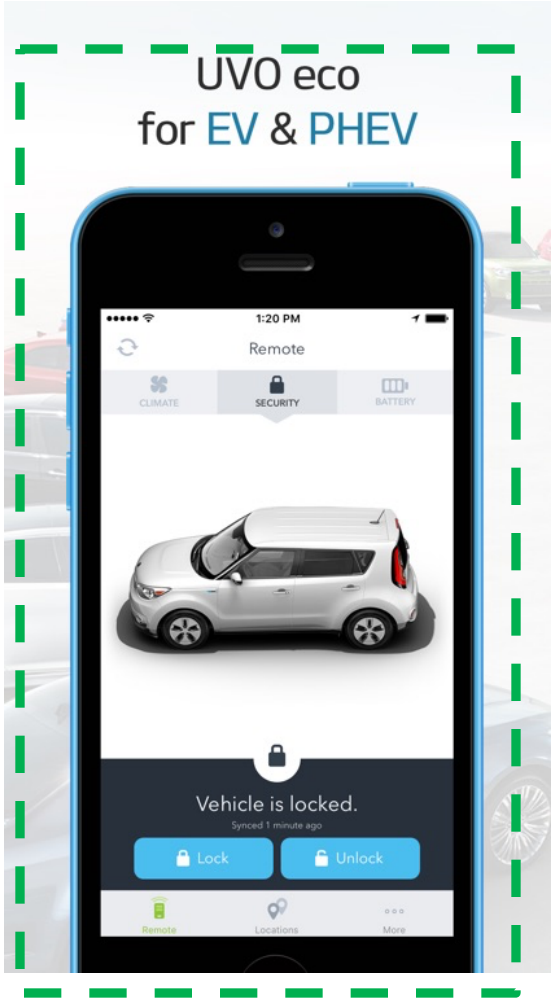
means for detecting a remaining energy of said battery; and

means for transmitting, to the information processing apparatus, information about the remaining energy of said battery on the basis of the received setting information.

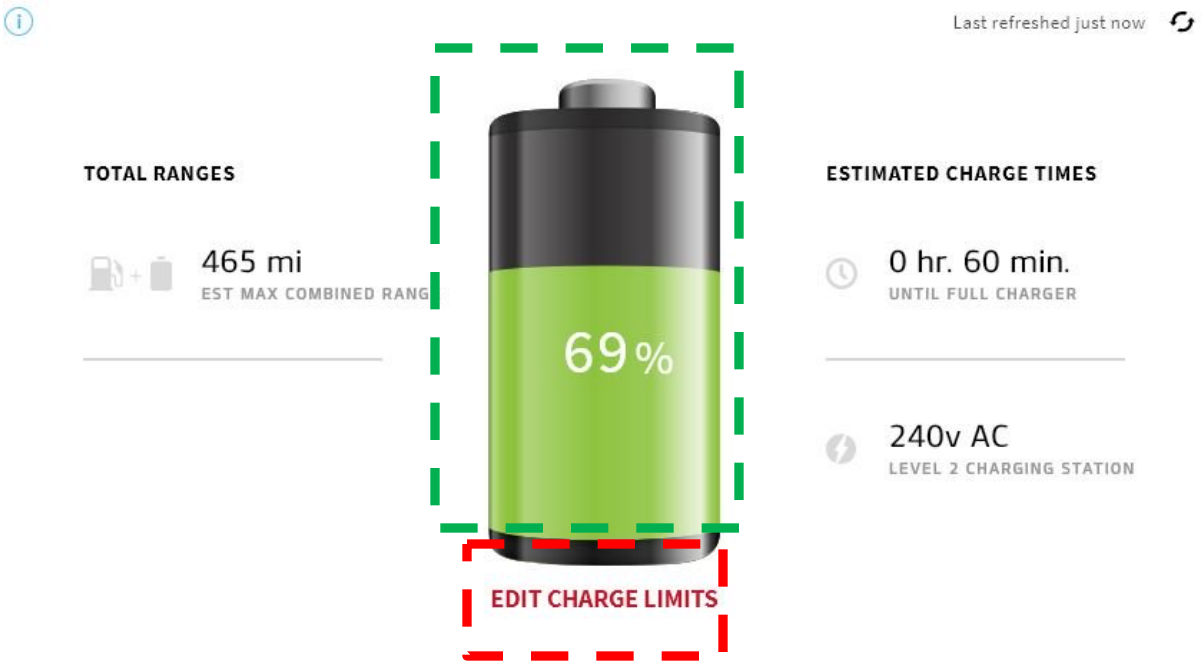
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

Claim 1	
A device comprising: a battery which supplies power to a communication section which communicates with an information processing apparatus;	https://appadvice.com/app/uvo-eco/906128813  http://webmanual.kia.com/STD_GEN5_WIDE/AVNT/AUS/English/evelectricvehicle.html 

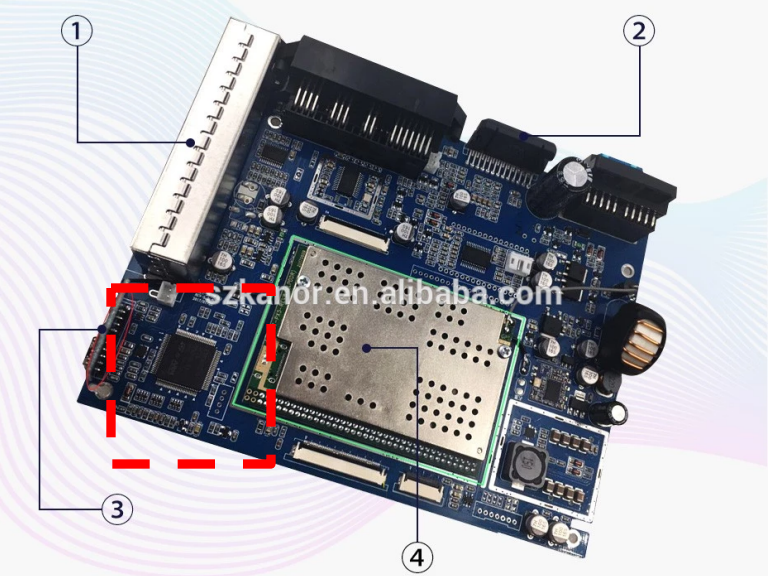
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

Claim 1	
means for receiving, from the information processing apparatus, …	https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html "for Kia Soul"  https://appadvice.com/app/uvo-eco/906128813 

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

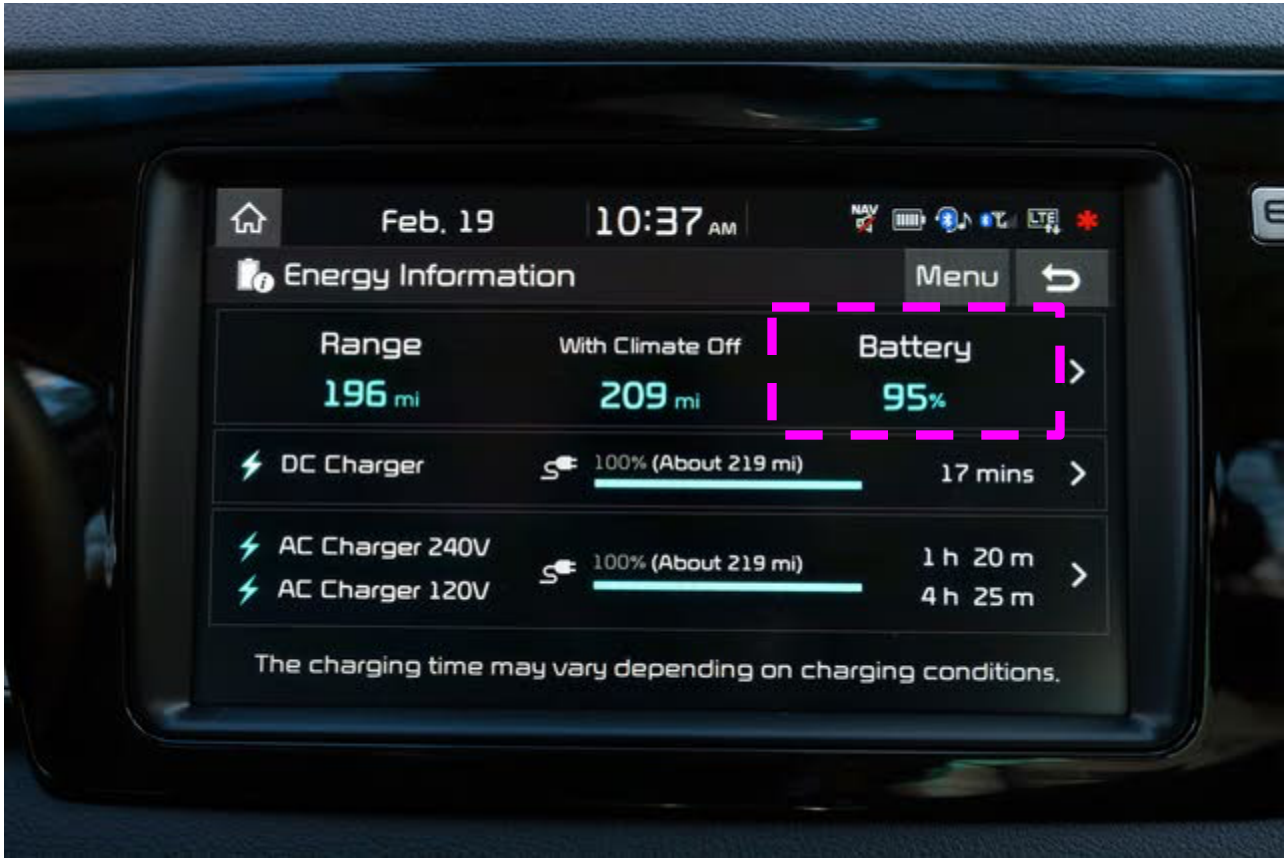
Claim 1	
a setting information representing at least one of a notifying method for information about remaining energy of said battery, or level of remaining energy of said battery at which a warning is to be displayed on the information processing apparatus; and	https://www.kianiroforum.com/threads/uvo-edit-charge-limits.7813/ 

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

Claim 1	
means for storing the received setting information; and	https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html "for Kia Soul"  {e.g. flash memory} Source: https://www.kia.com/us/en/ev-faqsrivers-maximize-efficiency-300377924.html KIA Can I manage my vehicle remotely? Yes! The Kia Access with UVO link app allows you to remotely control your electric vehicle from afar. UVO link seamlessly connects your compatible smartphone to your EV, giving you access to battery status, charging schedules, remote lock/unlock, remote climate control, 24-hour roadside assistance, and much more. Learn more at owners.kia.com.

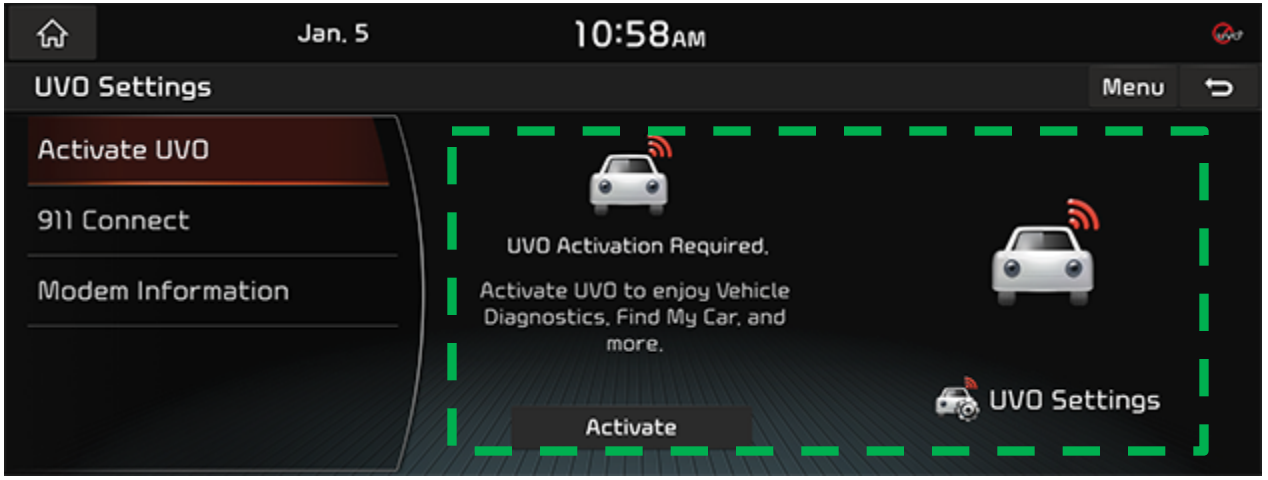
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

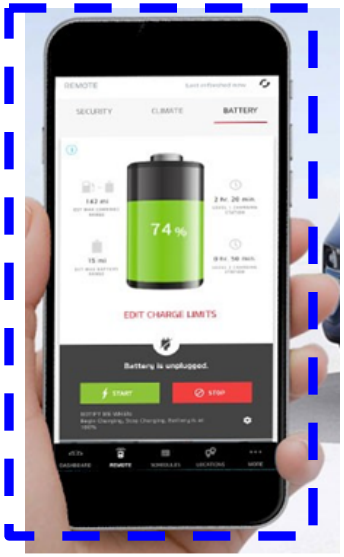
Claim 1	
means for detecting a remaining energy of said battery; and	Source: https://www.cargurus.com/Cars/2019-Kia-Niro-EV-Overview-c28933



Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

Claim 1	
means for transmitting, to the information processing apparatus,	Source: http://webmanual.kia.com/PREM_GEN5/AVNT/RJ/USA/English/system004.html





{UVO provides 4G connectivity For Kia cars}

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,831,444 by Kia

Claim 1	
information about the remaining energy of said battery on the basis of the received setting information.	https://www.kianiroforum.com/threads/uvo-edit-charge-limits.7813/

EXHIBIT 6

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Kia Bluetooth System

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

1. An authentication processing apparatus of a radio communication which authenticates a device, the apparatus comprising:

means for acquiring an external factor which is associated with a security level;

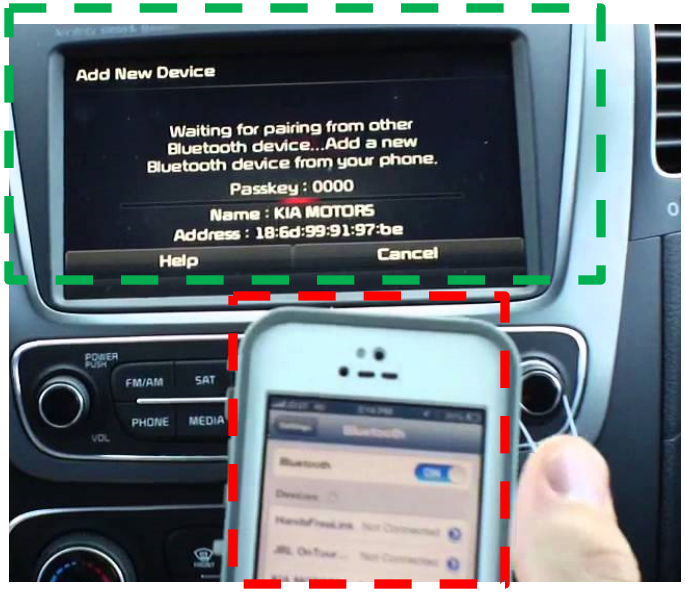
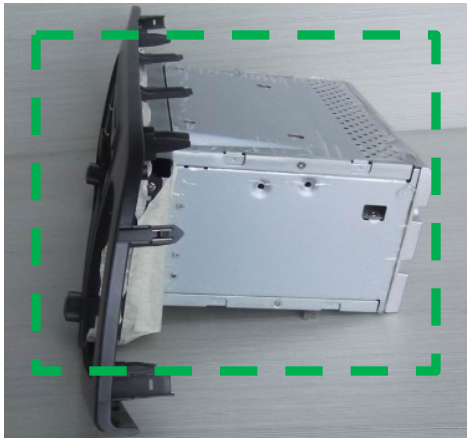
means for selecting a security level from a plurality of security levels in accordance with the external factor;

means for receiving a request for an authentication and authentication information from the device;

means for checking whether the received information from the device is valid or not depending on the selected security level; and

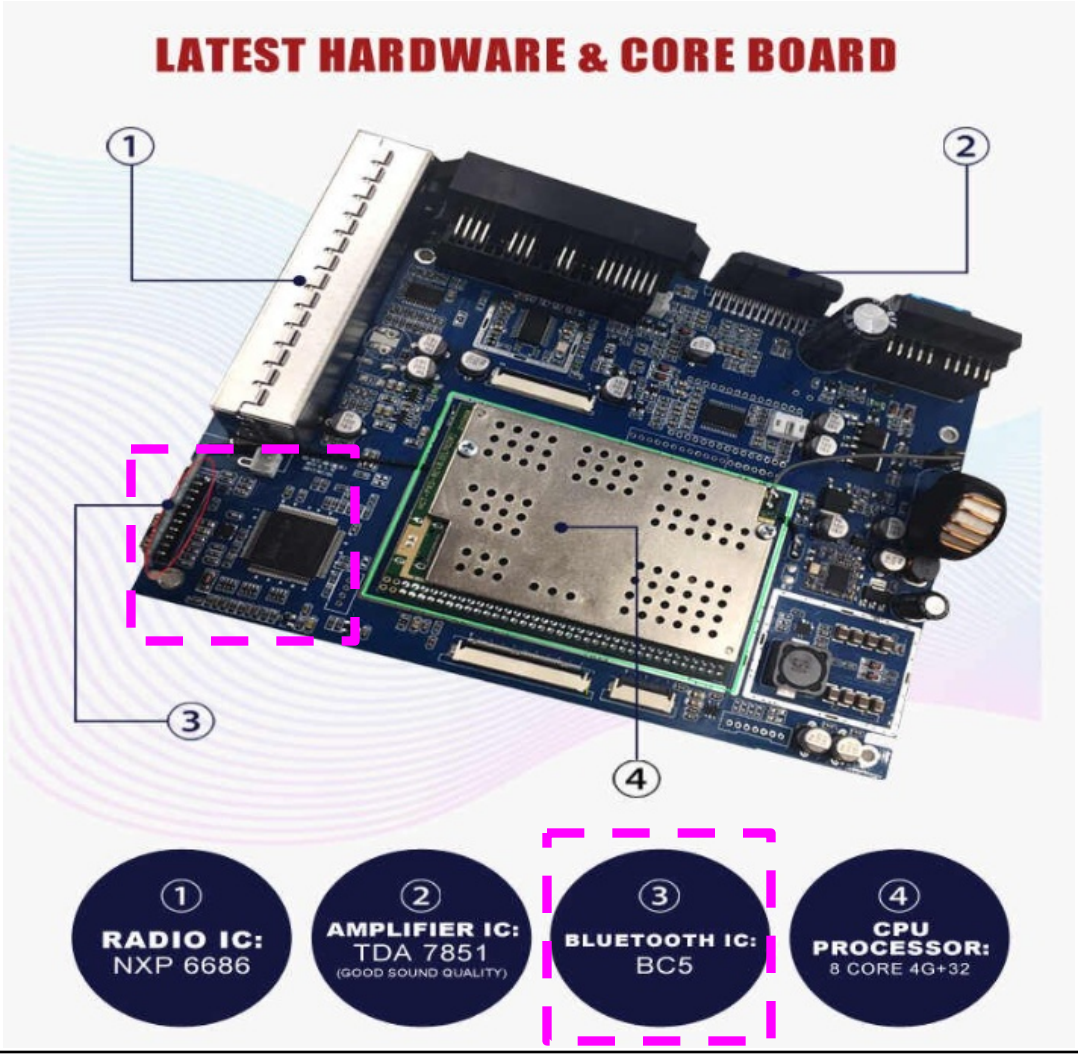
means for sending a response of the check result which authenticates or rejects the device thereto.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Claim 1	
1. An authentication processing apparatus of a radio communication which authenticates a device, the apparatus comprising:	 Source: https://www.youtube.com/watch?v=UcYrwSs3jgw 2014 KIA Sorento iPhone Bluetooth pairing  https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html ***Bluetooth*® Wireless Technology** Frequency Range: 2402 ~ 2480 MHz; Supported Bluetooth® Specification: 3.0 Supported Profile: Handsfree(1.6), A2DP(1.2), AVRCP(1.4), PBAP(1.0) Output: 0.125 mW Number of Channels: 79 channels Source: Kia "CAR MULTIMEDIA SYSTEM USER'S MANUAL – Soul Eco/Electric" page 198

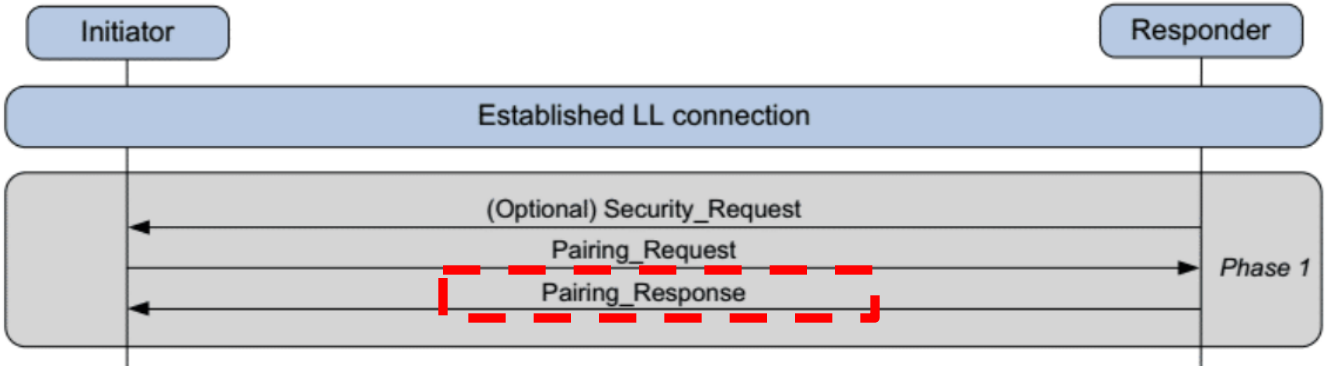
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Claim 1	
means for acquiring an external factor which is associated with a security level;	https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html Kia Picanto Morning 2014 2015 2016



Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Claim 1	
means for acquiring an external factor which is associated with a security level;	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/



Today, we will look at Phase 1: Pairing Feature Exchange. Pairing is the exchange of security features that include things like Input/Output (IO) capabilities, requirements for Man-In-The-Middle protection, etc. The exchange of pairing information between two devices is done through the Pairing Request and Pairing Response packet. The contents of these two messages is shown below in Table 1 Pairing Request/Response.

Field	Code	IO	OOB	AuthReq (1 Byte)					Maximum	Initiator	Responder
Sub-define	(1 Byte)	Cap (1 Byte)	DF (1 Byte)	BF	MITM	SC	KP	Reserved	Encryption Key Size (1 Byte)	Key Distribution (1 Byte)	Key Distribution (1 Byte)
Bits*	8	8	8	2	1	1	1	3	8	8	8

Table 1 Pairing Request/Response

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Claim 1	
means for selecting a security level from a plurality of security levels in accordance with the external factor;	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/

BF, "Bonding_Flags"

Bonding is the exchange of long-term keys after pairing occurs, and storing those keys for later use — it is the creation of permanent security between devices. Pairing is the mechanism that allows bonding to occur.

Bonding_Flags b_1b_0	Bonding Type
00	No Bonding
01	Bonding
10	Reserved
11	Reserved

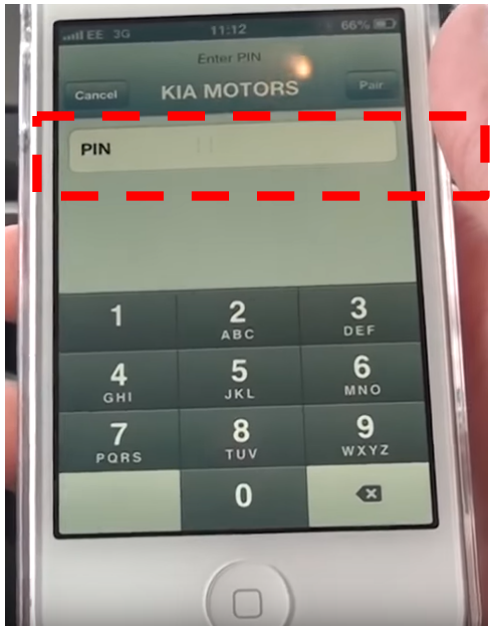
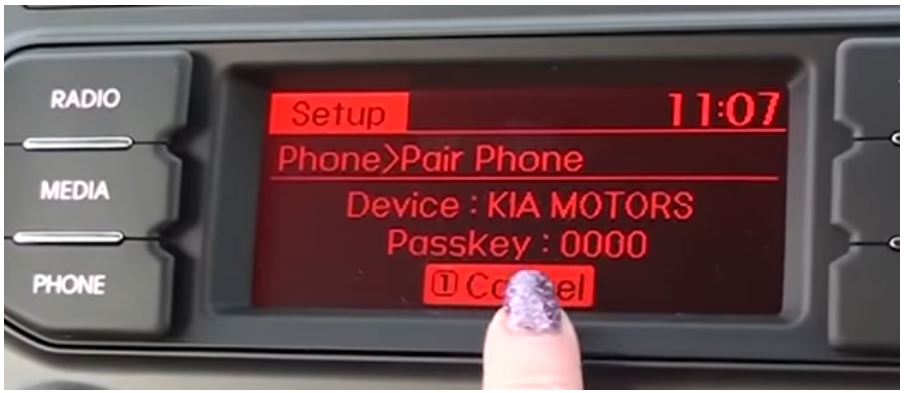
"MITM"

MITM is short for "Man-In-The-Middle." This field is a 1-bit flag that is set to one if the device is requesting MITM protection. This blog focuses on the procedure for the pairing feature exchange—if you are interested in MITM, please refer to the Bluetooth Core Specification v4.2, Vol1, Part A, 5.2.3.

"SC"

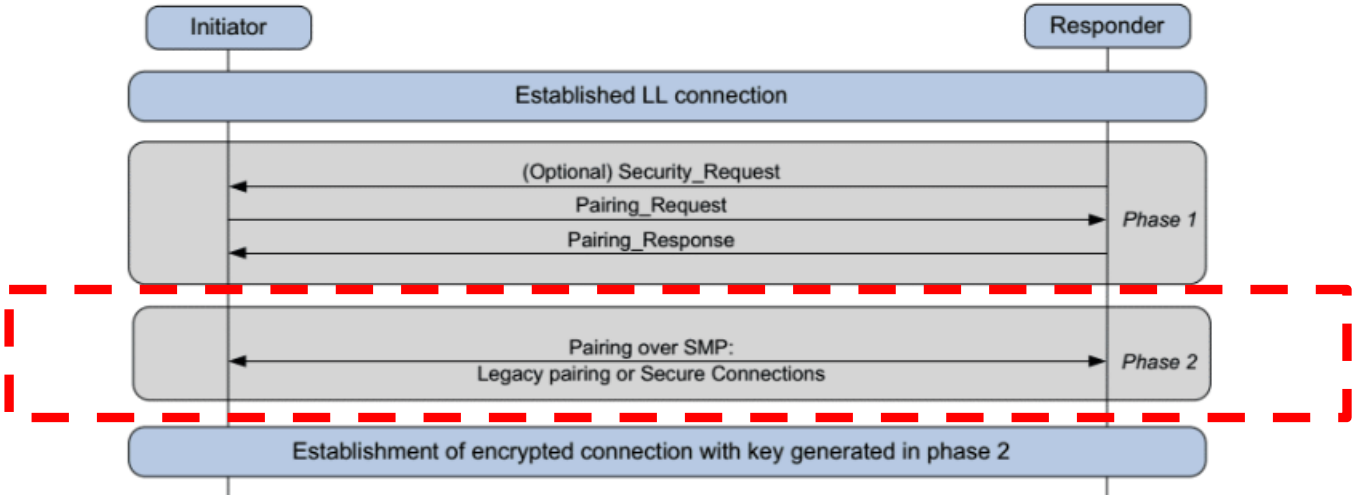
The SC field is a 1-bit flag that is set to one to request LE Secure Connection pairing. The possible resulting pairing mechanisms are if both devices support LE Secure Connections, use LE Secure Connections and otherwise use LE legacy pairing. So this flag is an indicator to determine Phase 2 pairing method.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Claim 1	
means for receiving a request for an authentication and authentication information from the device;	 https://www.youtube.com/watch?v=L8K4uQGo4eg How to Pair your phone to you KIA via Bluetooth  **Adding a device to Bluetooth in a Kia** Connecting your smartphone to Kia's Bluetooth system is actually relatively simple. You'll just have to follow a few steps, and you'll be all set to start making and answering calls, wirelessly streaming music and more all while your eyes stay on the road and hands stay on the wheel. 1. Turn Bluetooth on on your smartphone 2. Depending on what type of phone you have, you may also need to select "Discover," "Search," or "Find Connection" 3. Press the "Setup" button on your Kia's radio unit, and select "Phone" 4. Select "Pair" 5. If it asks you to say the name of your phone, do so and afterwards say "Yes" 6. On your radio unit, you'll see the name of your car and a passkey. Enter the passkey into your phone after selecting the name of your vehicle 7. Pairing is complete! https://www.mattcastruccikia.com/blog/how-to-connect-smartphone-kias-bluetooth-system/

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

Claim 1	
means for checking whether the received information from the device is valid or not depending on the selected security level; and	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/



When the exchange of pairing feature starts, the initiator and responder will exchange their pairing feature information with each other through pairing request and response. With the information, the initiator and responder can determine the I/O capabilities with each other, which pairing mechanism—legacy pairing or secure connection—should be used, and select the pairing method—**Just Work**, **Passkey Entry**, **Numeric Comparison** or **Out of Band**—to use in Phase2. We will explore the details in Part 2: Pairing Method and Key Generation.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 6,928,166 by Kia

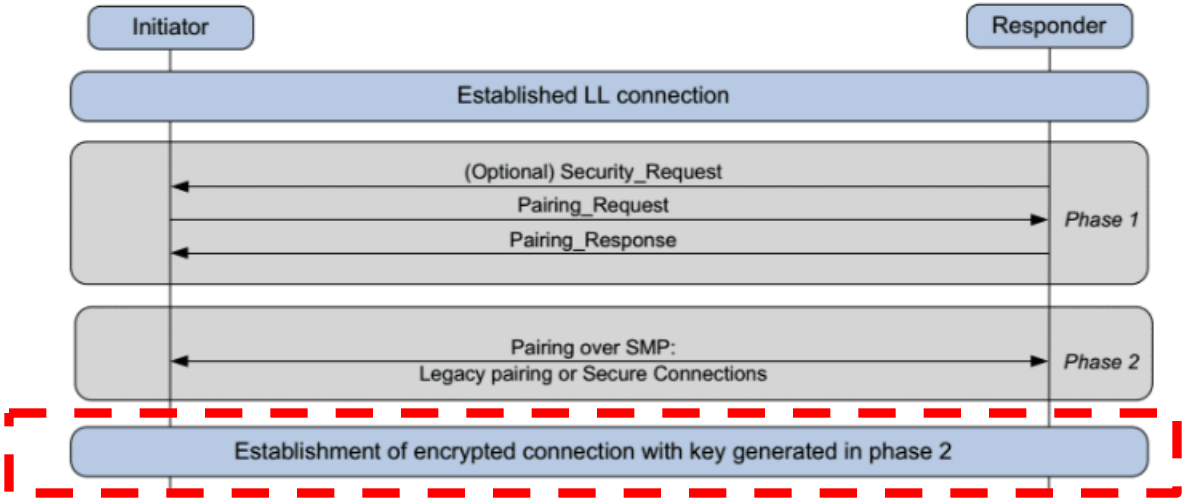
Claim 1	
means for sending a response of the check result which authenticates or rejects the device thereto.	Source: https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/ 

EXHIBIT 7

Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Kia Bluetooth System

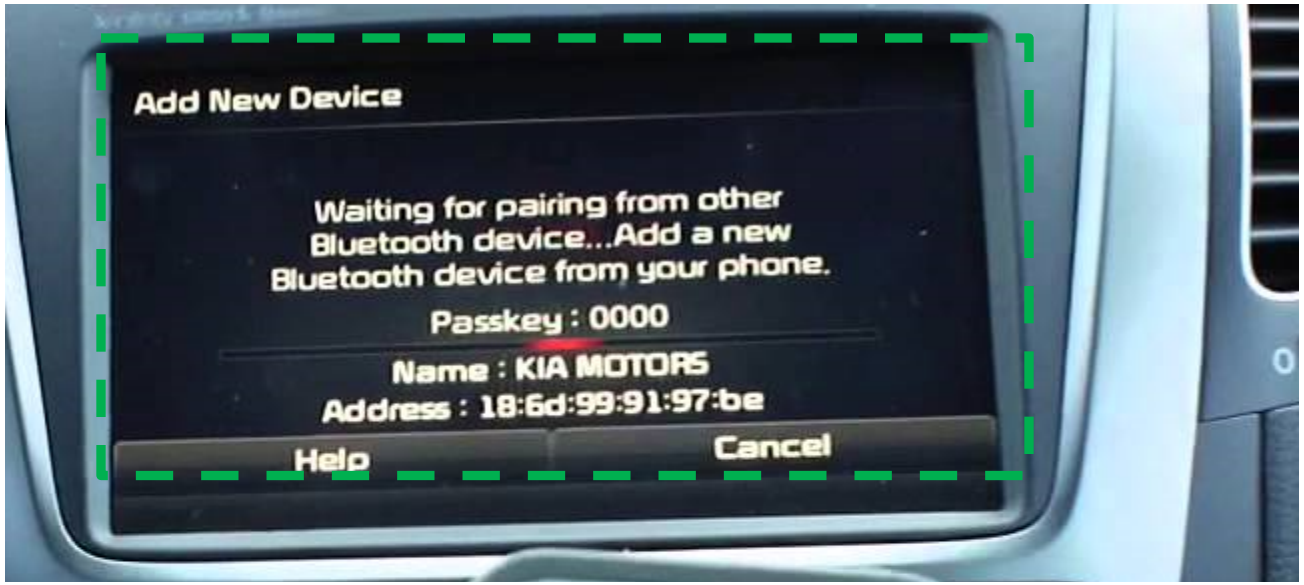
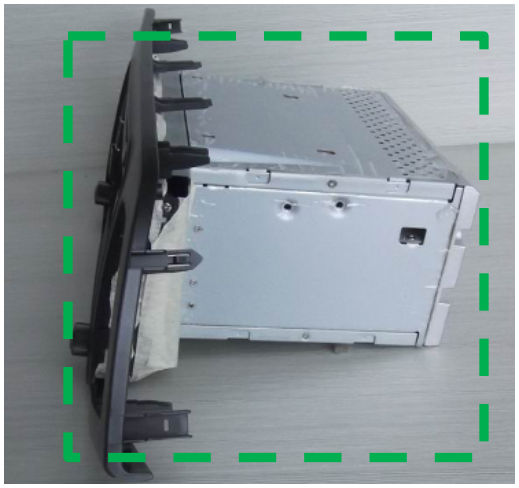
Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

20. A communication apparatus comprising:

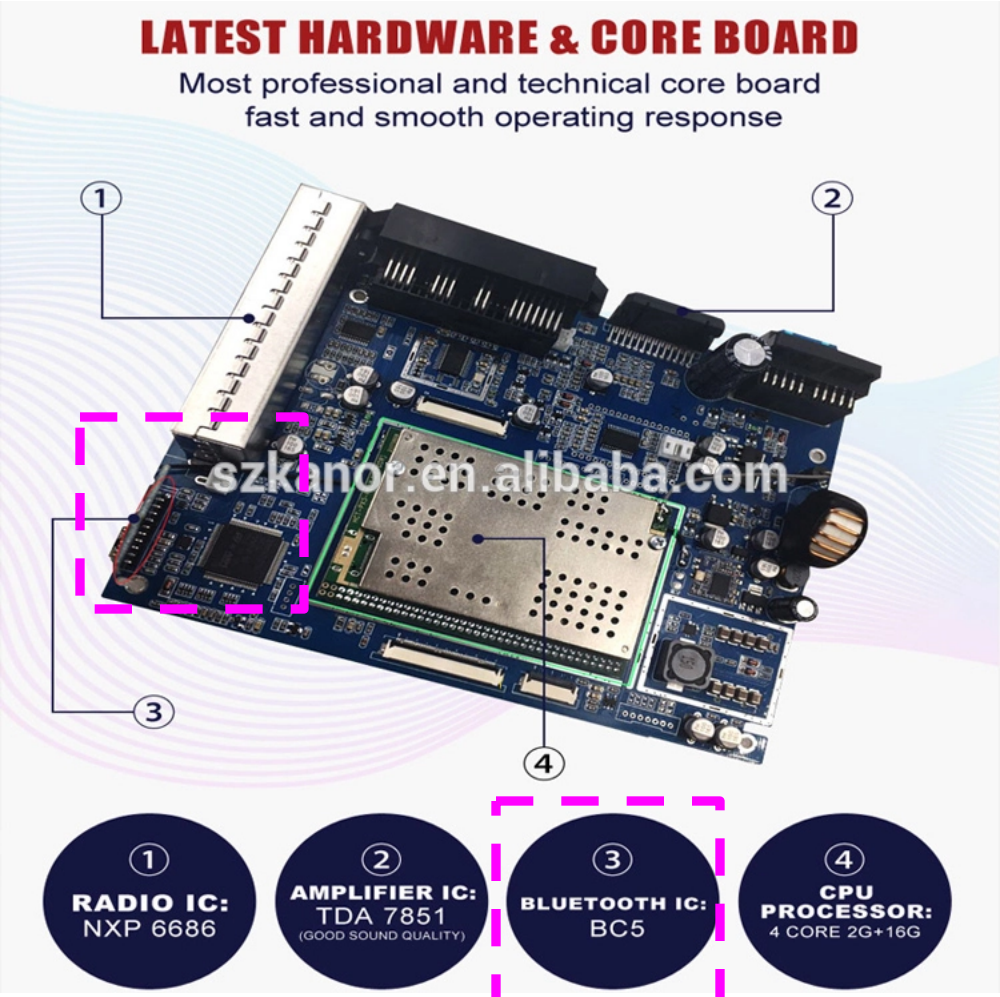
a unit configured to establish a connection with a first wireless communication apparatus in a first mode; and

a unit configured to control a connection from a second wireless communication apparatus when the connection with the first wireless communication apparatus is established, wherein the control unit sets up a second mode in which, in a state where the connection with the first wireless communication device is established, the communication apparatus is inhibited from establishing a connection with the second wireless communication apparatus with respect to a connection request from the second wireless communication device.

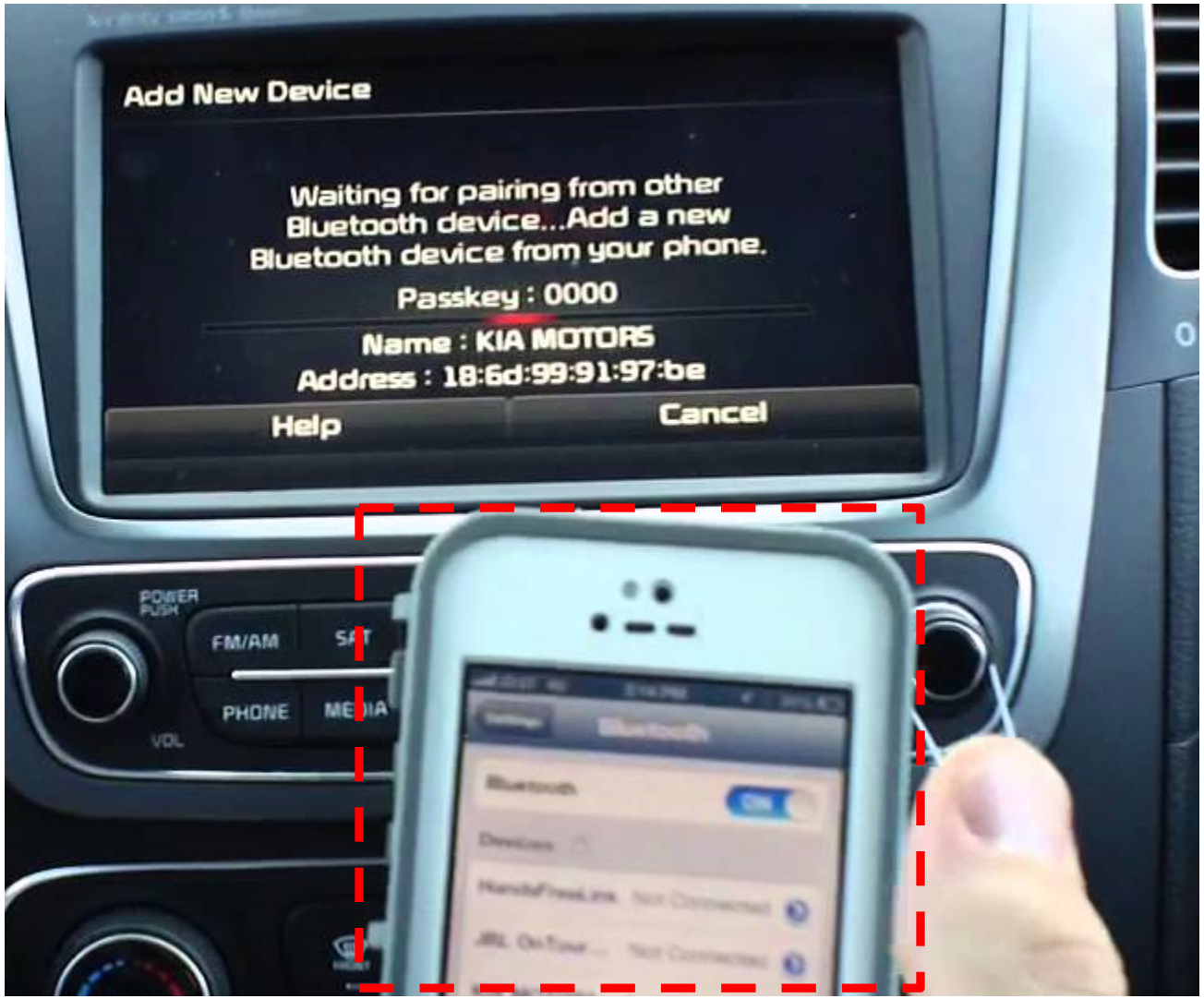
Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
20. A communication device, comprising:	Source: https://www.youtube.com/watch?v=UcYrwSs3jgw 2014 KIA Sorento iPhone Bluetooth pairing   https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html

Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
a unit configured to establish a connection with a first wireless communication apparatus in a first mode; and	https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html 

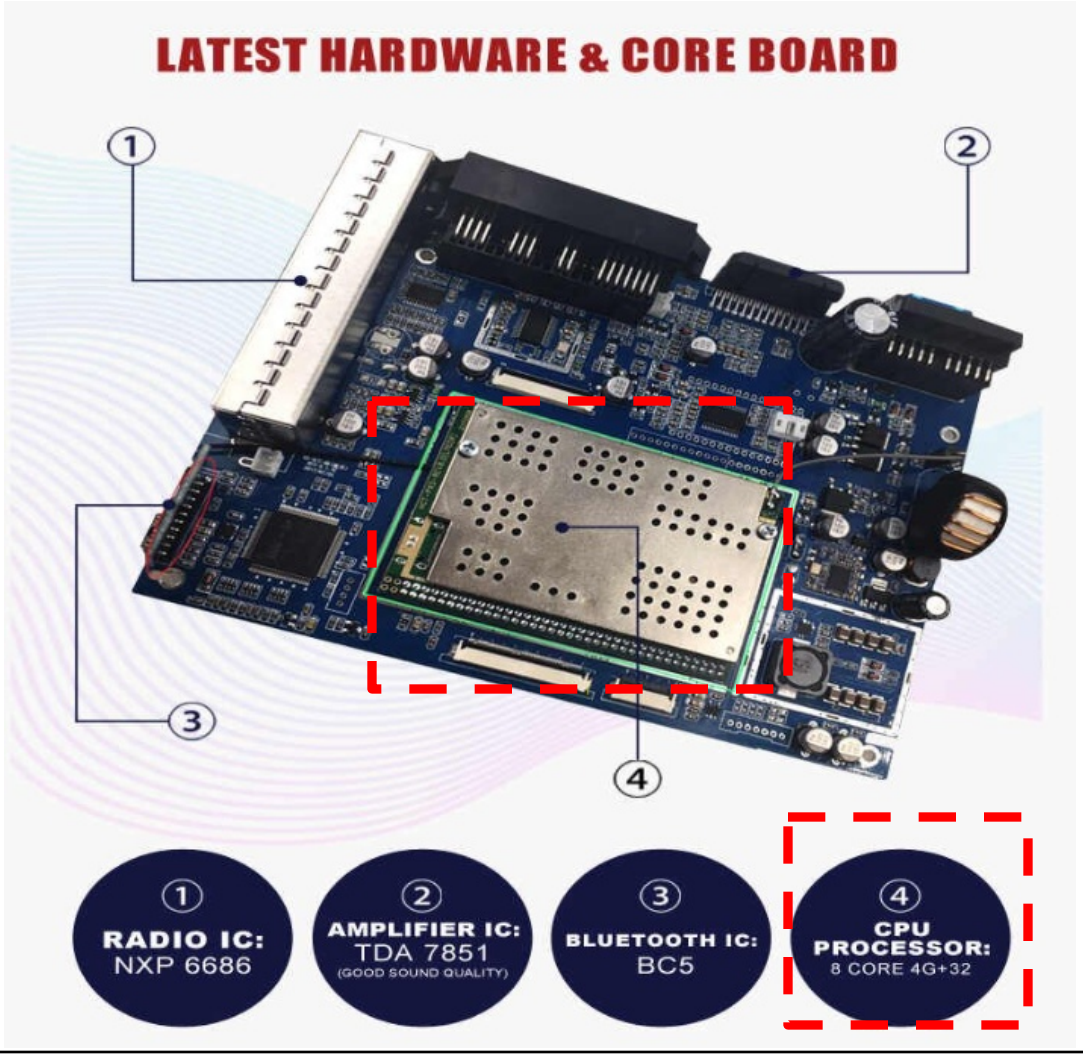
Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
a unit configured to establish a connection with a first wireless communication apparatus in a first mode; and	Source: https://www.youtube.com/watch?v=UcYrwSs3jgw 2014 KIA Sorento iPhone Bluetooth pairing 

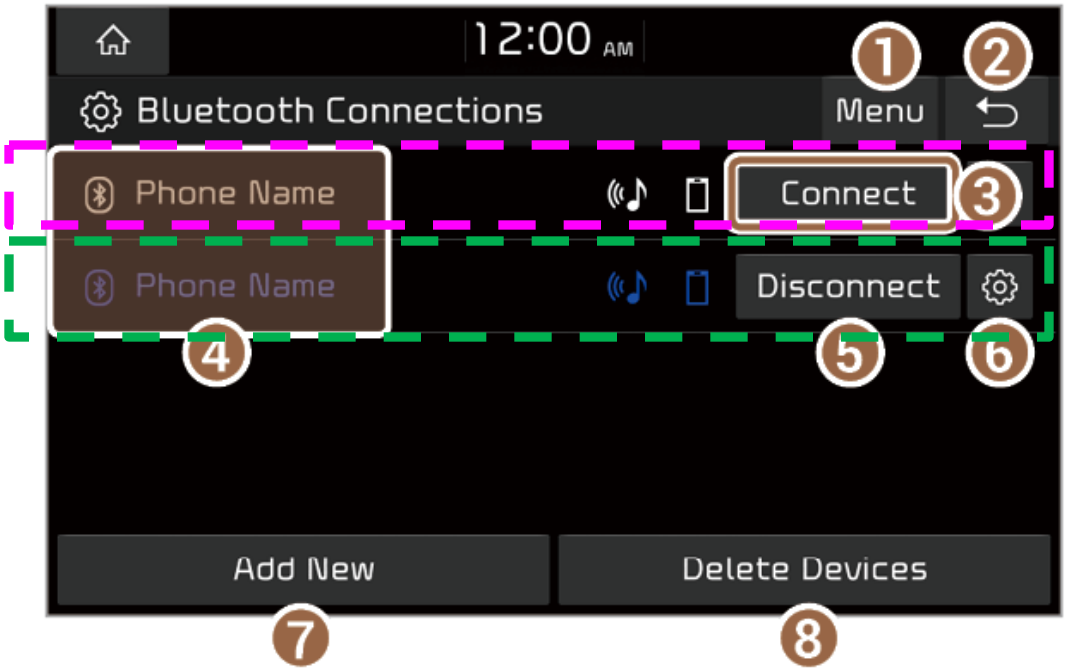
Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
a unit configured to establish a connection with a first wireless communication apparatus in a first mode; and	http://www.kceed.com/changing_priority-431.html **What is Priority?** It is possible to pair up to five Bluetooth® Wireless Technology devices with the car audio system. The "Change Priority" feature is used to set the connection priority of paired phones. However, the most recently connected phone will always be set as the highest priority. Press the SETUP key - Select [Phone] - Select [Paired Phone List] {Note: first phone listed is first priority and in "first mode"}

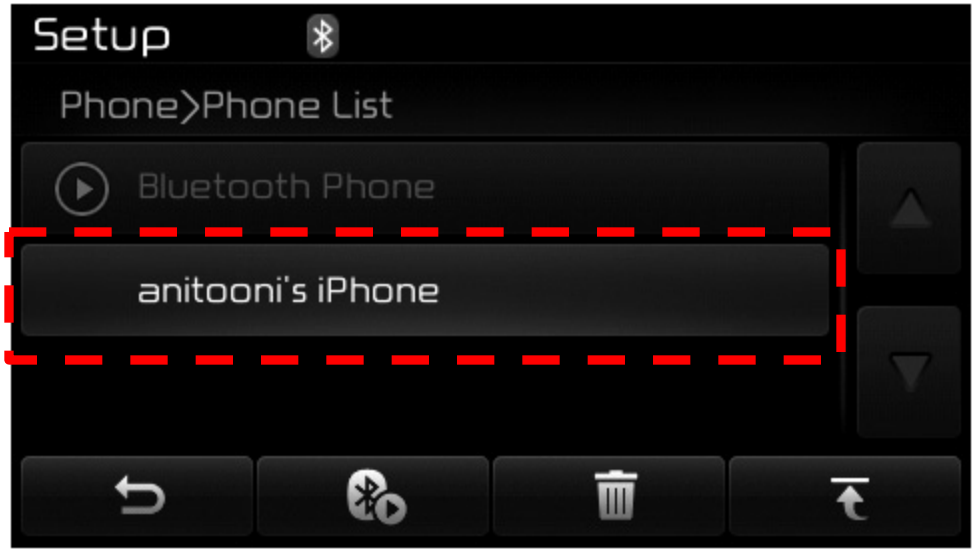
Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
a unit configured to control a connection from a second wireless communication apparatus when the connection with the first wireless communication apparatus is established	https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html "for Kia Picanto Morning 2014 2015 2016" 

Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
a unit configured to control a connection from a second wireless communication apparatus when the connection with the first wireless communication apparatus is established	http://webmanual.kia.com/DA_GEN2_V/AV/KOR/English/007_Calling_btconnect.html#id_h2_44 "Connecting a Paired Device"  1 Display the options list. • **User's Manual on Web (QR Code)**: Access the web manual via the QR code. For safety reasons, you can access the QR code only when your vehicle is stationary. 2 Return to the previous level. 3 Connect the device. 4 List of Bluetooth devices paired with the system. Press a device name to connect or disconnect the device. 5 Disconnect the device.

Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

Claim 20	
wherein the control unit sets up a second mode in which, in a state where the connection with the first wireless communication device is established	http://www.kceed.com/changing_priority-431.html **What is Priority?** It is possible to pair up to five Bluetooth® Wireless Technology devices with the car audio system. The "Change Priority" feature is used to set the connection priority of paired phones. However, the most recently connected phone will always be set as the highest priority. Press the SETUP key - Select [Phone] - Select [Paired Phone List]  {Note: second phone listed is second priority and in "second mode"}

Preliminary Claim Chart Showing Infringement of Claim 20 of the U.S. Patent No. 7,127,210 by Kia

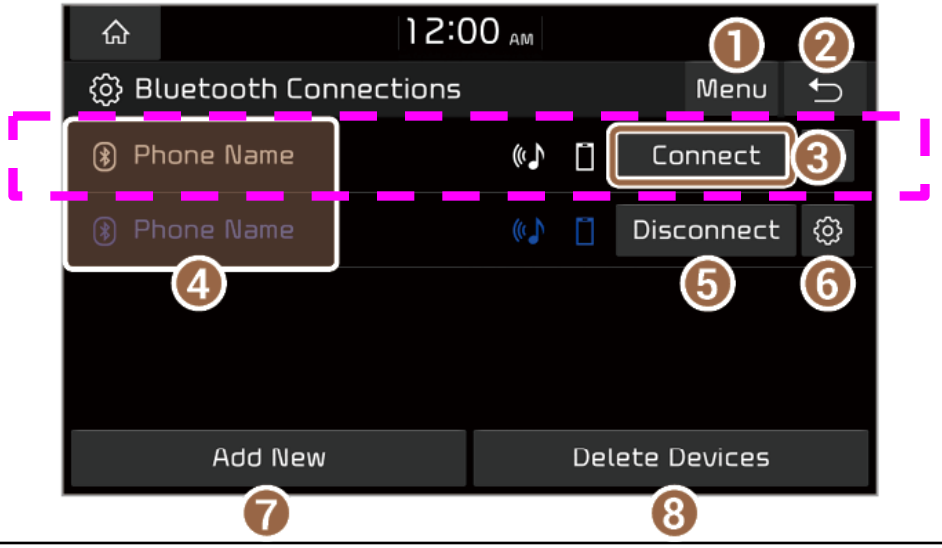
Claim 20	
the communication apparatus is inhibited from establishing a connection with the second wireless communication apparatus with respect to a connection request from the second wireless communication device.	Source: Kia "CAR MULTIMEDIA SYSTEM USER'S MANUAL – Soul Eco/Electric" page 188 **Information** • Up to 5 Bluetooth devices can be paired. • Only one Bluetooth device can be connected at a time. • During a Bluetooth device connection, another device cannot be paired. http://webmanual.kia.com/DA_GEN2_V/AV/KOR/English/007_Calling_btconnect.html#id_h2_44 "Connecting a Paired Device" 

EXHIBIT 8

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Kia Bluetooth System

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

1. A communication device, comprising:

a radio communication module configured to exchange data with a target communication terminal over a network;

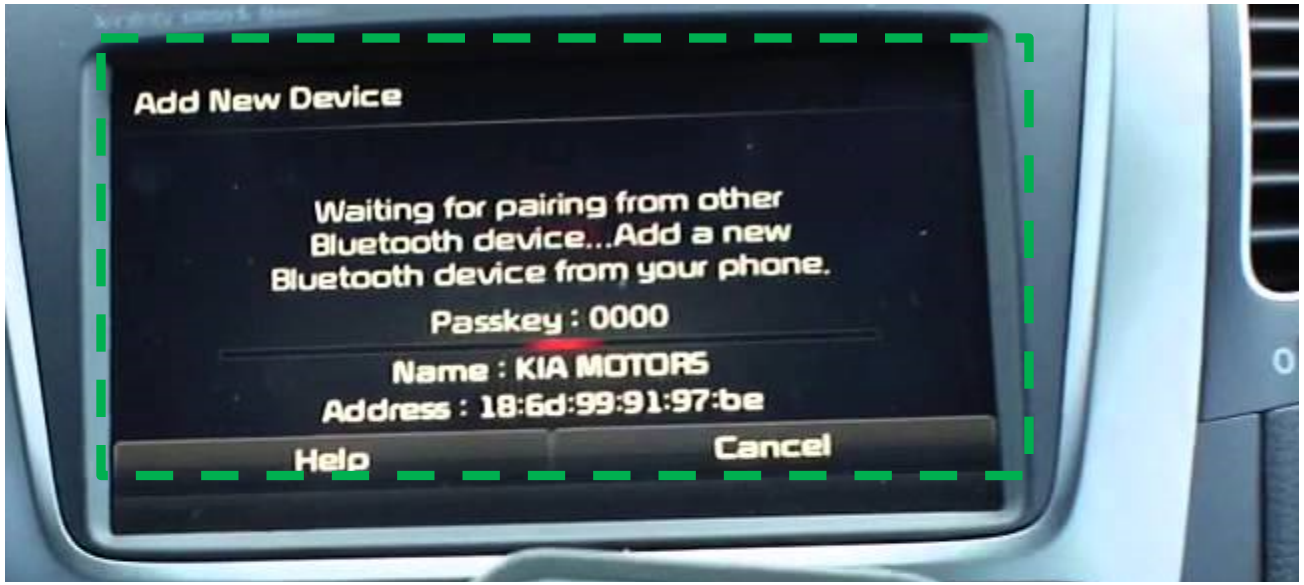
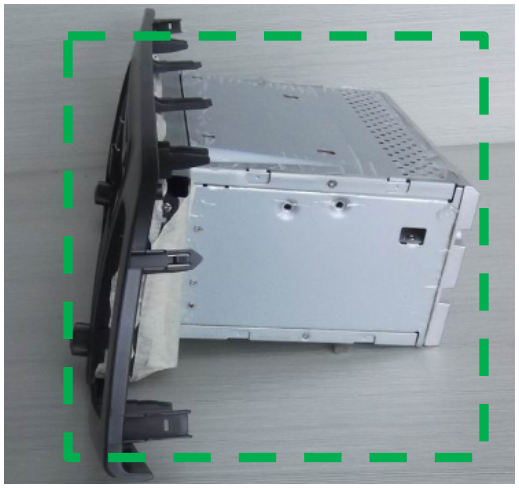
a service information memory configured to store service information so that predetermined functions can be performed with the target communication terminal;

a communication control information designating module configured to designate, by a user of the communication device, communication conditions for a newly established radio communication connection with the target communication terminal or for discriminating a disconnection of an existing radio communication connection with the target communication terminal;

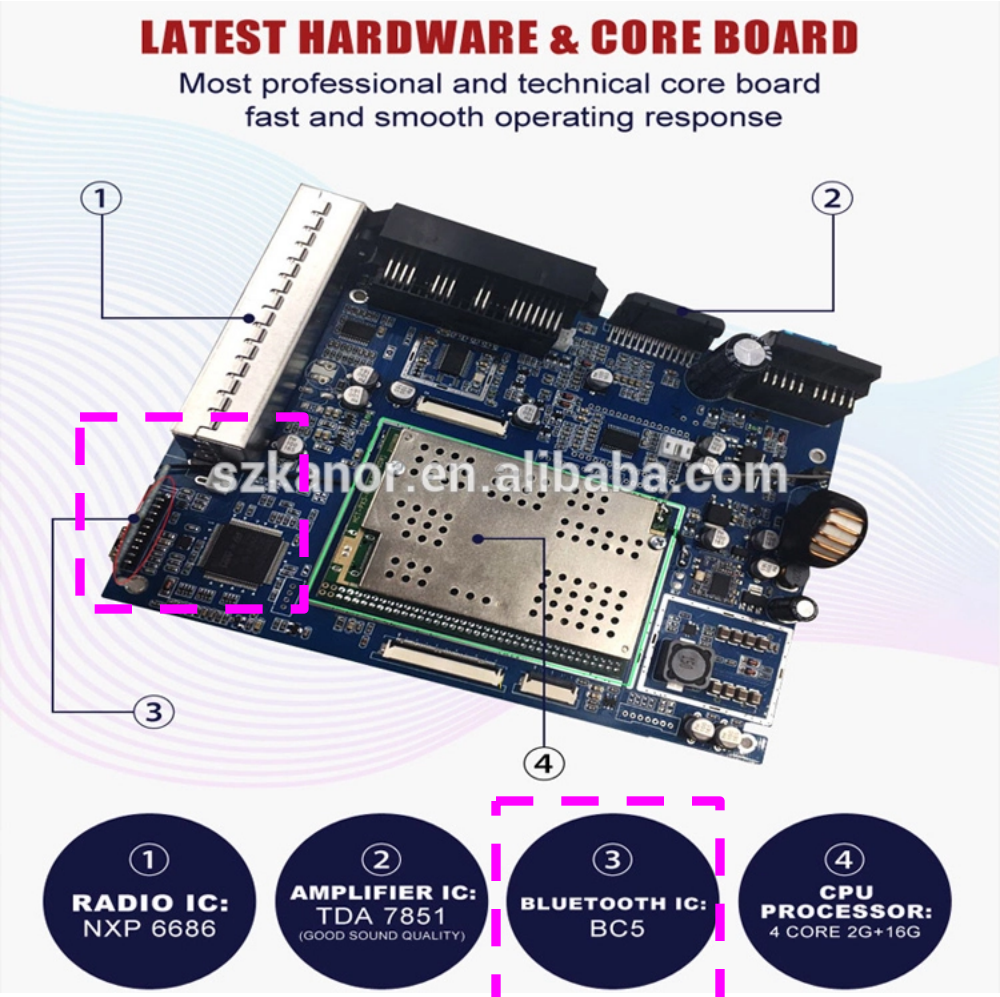
a memory configured to store the communication conditions designated by the communication control information designating module; and

a communication control module configured to determine whether the radio communication connection with the target communication terminal is in a connection status or a disconnection status based on the communication controlling information stored in the memory, and performing communication through the radio communication module by using service information read from the service information memory in accordance with the determination result.

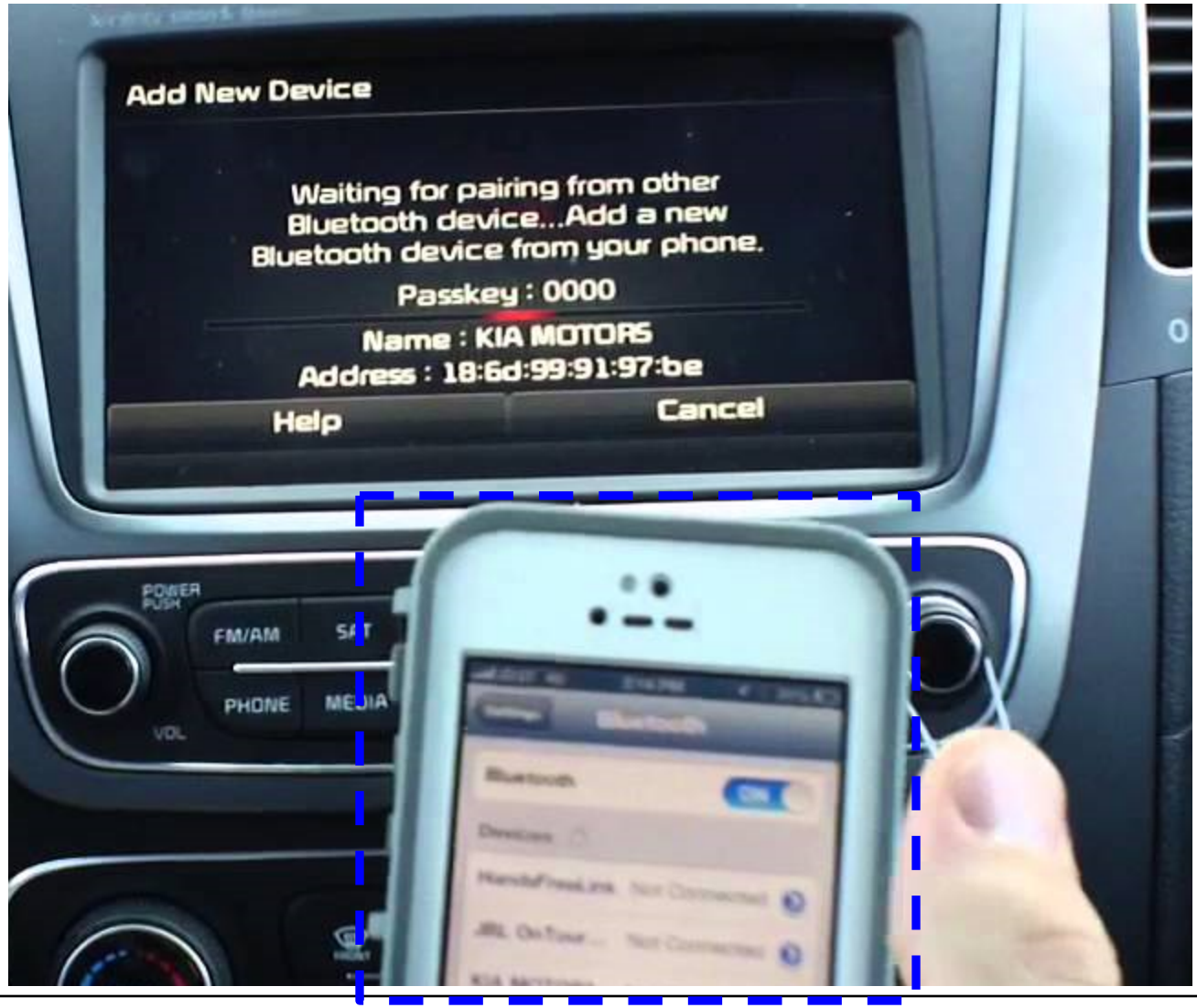
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
1. A communication device, comprising:	Source: https://www.youtube.com/watch?v=UcYrwSs3jgw   https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html

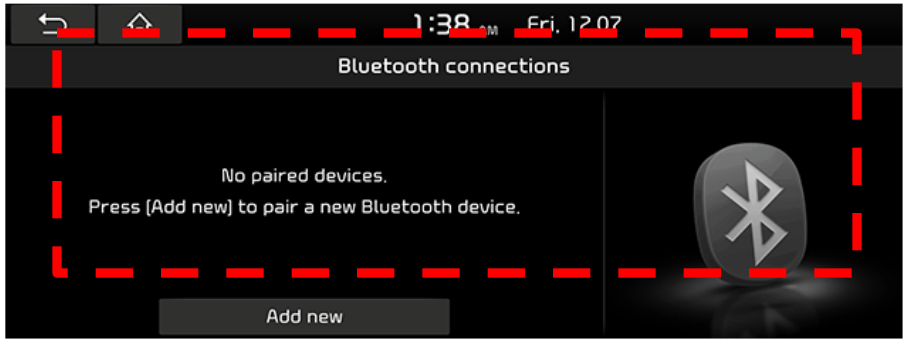
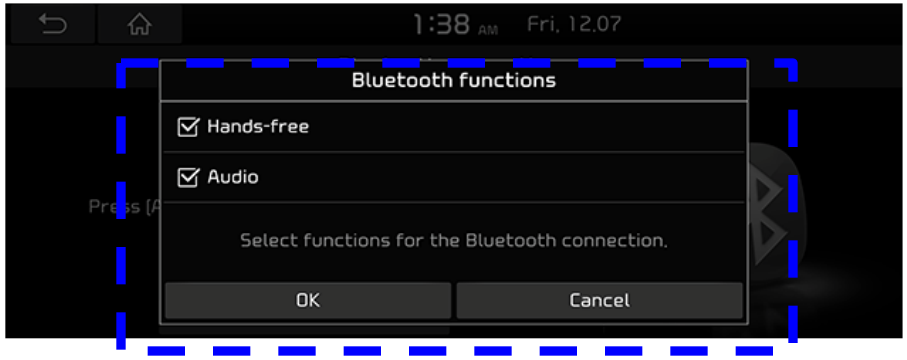
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
a radio communication module	https://www.alibaba.com/product-detail/Autoradio-2-din-android-8-1_60851585691.html Kia Picanto Morning 2014 2015 2016 

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
configured to exchange data with a target communication terminal over a network;	Source: https://www.youtube.com/watch?v=UcYrwSs3jgw 

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
a service information memory configured to store service information so that predetermined functions can be performed with the target communication terminal;	http://webmanual.kia.com/STD_GEN5_WIDE/AVNT/EU/English/bluetoothwirelesstechnology.html 2 Select the device you want to connect. If there is no device you want to connect, press [Add new].  3 Select the service to connect, press [OK]. When connecting the Bluetooth, Hands-free connection is available only for one Bluetooth connection. But Bluetooth audio is supported for multi-connection. 

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

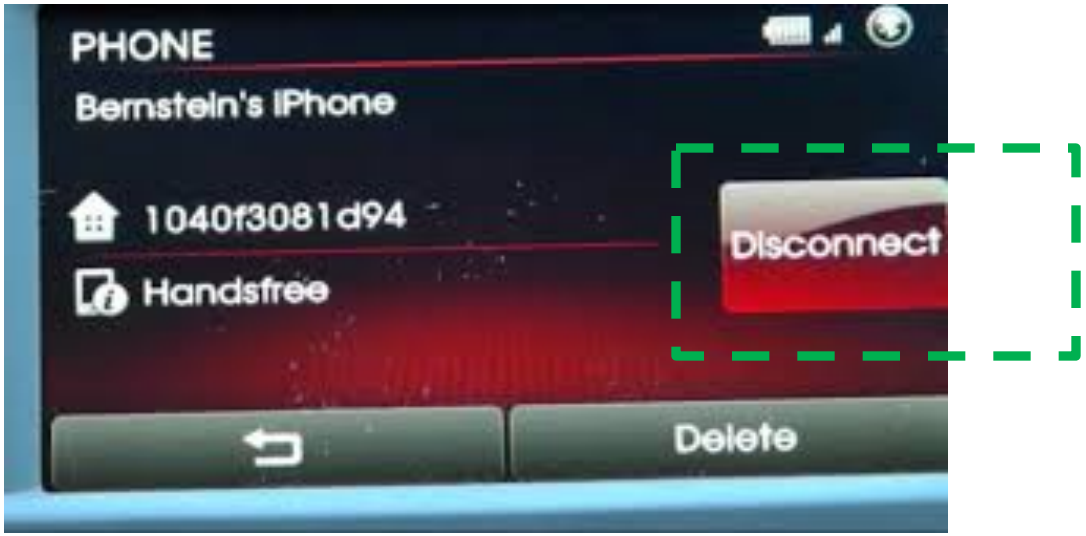
Claim 1	
a communication control information designating module configured to designate, by a user of the communication device, communication conditions for a newly established radio communication connection with the target communication terminal	Source: Kia "CAR MULTIMEDIA SYSTEM USER'S MANUAL – Soul Eco/Electric" page 188

Bluetooth Connection Settings

- Press the SETUP key ▶ Select Bluetooth ▶ Select Bluetooth Connection.
- Connect a Bluetooth device ▶ Press the PHONE key ▶ Select Connections.
- Connect a Bluetooth device ▶ Select All Menus from the Home screen ▶ Select Bluetooth Phone ▶ Select Bluetooth.

Features	Description
1 Paired Device List	Displays the paired Bluetooth device list. When selecting from the list, the device is connected or disconnected.
2 Bluetooth Audio Connection Status	An icon appears when you make a Bluetooth Audio connection.
3 Bluetooth Hands-Free Connection Status	An icon appears when you make a Bluetooth hands-free connection.
4 Add New	Register a new Bluetooth device.
5 Delete Devices	Select and delete a paired device.
6 Delete All	Delete all paired devices.
7 Help	Switches to the Bluetooth Connection Help screen.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
or for discriminating a disconnection of an existing radio communication connection with the target communication terminal;	Source: https://www.youtube.com/watch?v=1VmZS0nHQfQ How to remove your phone from your Kia's Uvo system 

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
a memory configured to store the communication conditions designated by the communication control information designating module; and	Source: https://www.ramcountryautoworld.com/used/Kia/2019-Kia-Optima-d4d7f75d0a0e0ae7498f7e896bd2ba26.htm

Detailed Specifications

+ **Convenience Features**
+ **Suspension/Handling**
− **Entertainment Features**

1st row LCD monitors: 2
AM/FM radio
Internal memory capacity (GB): 1 GB
Primary LCD size: 8.0"
Radio data system
Smart device integration: Apple CarPlay & Android Auto
Speakers: 6
Steering wheel mounted audio controls
Turn-by-turn navigation directions: UVO eServices
Wireless phone connectivity: Bluetooth

+ **Seats And Trim**

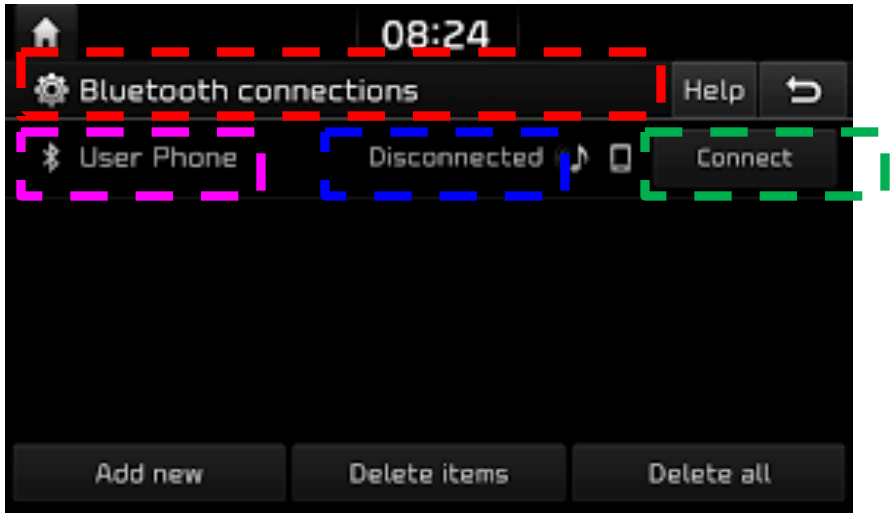
Used 2019 Kia
Optima LX LX Auto
Internet Price
Detailed Pricing
$17,981

Check For Savings

Ask | Drive

http://partner.lge.com/eu/portal/download/download/mobileExternalFileDownload.lge%3FfileId%3DWcWtjagNo2iJBziUs9jQ%26content%3Dmanual Page 18

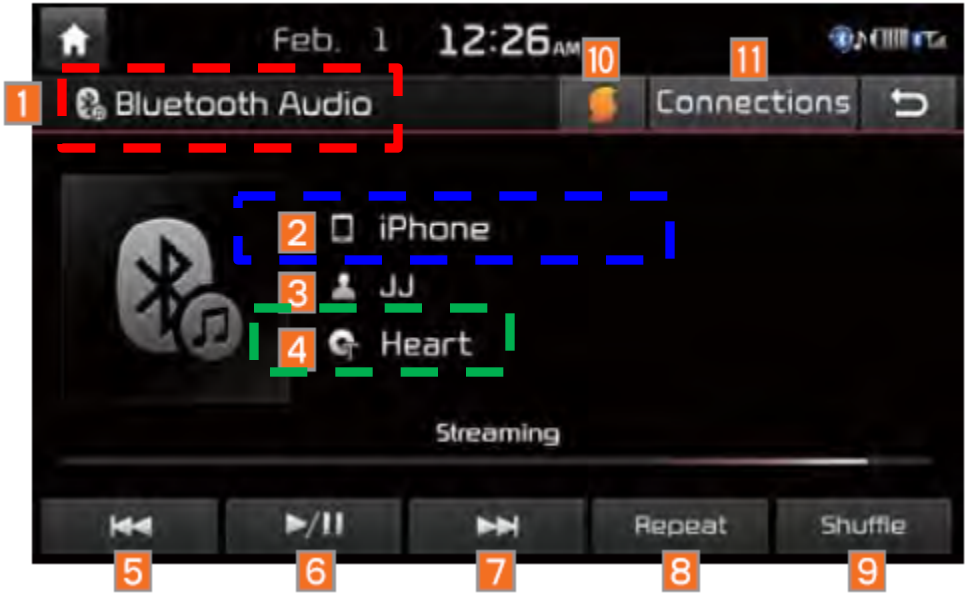
Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
a communication control module configured to determine whether the radio communication connection with the target communication terminal is in a connection status or a disconnection status based on the communication controlling information stored in the memory	http://partner.lge.com/eu/portal/download/download/mobileExternalFileDownload.lge%3FfileId%3DWcWtjagNo2iJBziUs9jQ%26content%3Dmanual Page 18  Source: Kia "CAR MULTIMEDIA SYSTEM USER'S MANUAL – Soul Eco/Electric" page 188 **Information** • Up to 5 Bluetooth devices can be paired. • Only one Bluetooth device can be connected at a time. • During a Bluetooth device connection, another device cannot be paired.

Preliminary Claim Chart Showing Infringement of Claim 1 of the U.S. Patent No. 7,184,707 by Kia

Claim 1	
and performing communication through the radio communication module by using service information read from the service information memory in accordance with the determination result.	Source: Kia "CAR MULTIMEDIA SYSTEM USER'S MANUAL – Soul Eco/Electric" page 62

Bluetooth® Audio Mode Display Controls



Features	Description
1 Mode	Displays the current operating mode
2 Phone Name	Displays name of connected phone
3 Artist Info	Name of current artist
4 Title	Name of current song