1993 公告本

申請日期	80. 2 7.
案號	80100981
類別	H04B 7/26

A4
C4

（以上各欄由本局填註）

發明 新型 專利說明書

一、發明創作名稱	中文	「於行動無線電系統中實施基地站與行動站間鑑認檢查之方法」
	英文	"A METHOD OF CARRYING OUT AN AUTHENTICATION CHECK BETWEEN A BASE STATION AND A MOBILE STATION IN A MOBILE RADIO SYSTEM"
二、發明創作人	姓名	1. 保羅・韋金森・戴特 PAUL WILKINSON DENT 2 艾立克斯・奎斯特・雷斯 ALEX KRISTER RAITH 3. 傑・艾立克・阿凱史坦那・達林 JAN ERIK AKE STEINAR DAHLIN
	籍貫（國籍）	1. 英 國 2 3. 瑞 典
	住、居所	1. 瑞典史泰海市史泰海拉斯卡 2. 瑞典奇斯塔市索洛卡坦街 19 號 3. 瑞典賈法拉市山英瓦吉街 152 號
三、申請人	姓名（名稱）	瑞典商 LM 艾瑞克生電話公司 TELEFONAKTIEBOLAGET LM ERICSSON
	籍貫（國籍）	瑞 典
	住、居所（事務所）	瑞典斯德哥爾摩市 S - 126 25
	代表人姓名	1. 蘭納・蓋瑞比 LENNART GRABE 2 泰吉・洛夫葛倫 TAGE LOVGREN

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

經濟部中央標準局印製

五、發明說明（ 1 ）

技術範圍

本發明係關於在行動電話系統中基地站及行動站間實施鑑認檢查之方法，特別是關於細胞型行動電話系統。所提出之方法亦可應用在其他行動無線電話系統，供立即呼叫系統之用。

背景技術

在例如細胞式行動電話系統中，在行動站與基地站間建立呼叫之先實施鑑認檢查。基地站詢問關於行動站有關鑑認之資料，令行動站提出鑑認號碼。行動站乃被迫對基站洩露身份，因此，基地站會知道行動站已被授權在系統中發出呼叫，故基地站及交換站會知曉那一行動站應為隨后建立之呼叫付賬。

換言之，行動站必須確定其係與真正的基地站連絡，即真正被授權之基地站確實奉命在行動站為呼叫之一方時與其構成通話（行動站係－A－訂戶），行動站亦必須確定其將為此次呼叫付賬。

為實施鑑認檢查，早先已知在基地站及行動站形成鑑認信號"響應"（Resp）信號。一任意號碼（RAND）在基地站能涵蓋之區域內由基地站送至行動站。呼叫之行動站以既定信號（Resp 1）回答。以相似方式，基地站自任意號碼形成相同之Resp 1及呼叫之行動站之身分。此等信號通常係重合的，故基地站乃命令行動站至一語言波道。

本發明之公布

五、發明說明（2）

因此，在上述實施鑑認檢查之已知方法中，先行為一已知行動站組成任意號碼響應對，即，對一收到之既定任意號碼 RAND 行動站即制定一組響應信號，基地站因此對數個不同任意號碼可收到數個響應信號。意即可建立"假的"基地站，能發送數個彼此不同之任意號碼，並收到相對應（不同之）響應信號號碼。假基地站因而可以製造一個未奉准在此系統中發出呼叫之訂戶。此項已有之鑑認檢查之缺點，是由於單向檢查所引起，即僅有基地站需要響應信號以證明行動站之真實性。

根據本發明之方法，鑑認檢查係雙向的，即，不僅基地站需要行動站之身分鑑定，行動站亦需要鑑定基地站。

本發明之目的因此在提供一創新之鑑認檢查方法，使假的基地站無法偽造來獲得行動電話系統中之鑑認密碼。

本發明之方法之特點見於申請專利範圍第 1 項所訂之步驟。本發明所提方法之進一步發展則訂於申請專利中之範圍 2 - 3。

圖說之簡要說明

茲將本發明參照伴隨之圖說予以更詳盡之說明，其中

圖 1 圖解說明二個基地站與數個行動站間之通信；

圖 2 為說明本發明所提方法之一具體實例之流程圖；

圖 3 為加入行動站之一鑑認計算法輸入及輸出值之方塊圖；

圖 4 為說明本發明方法另一具體實例之流程圖。

實施本發明之最佳模式

五、發明說明（ 3 ）

圖 1 說明一鑑認基地站以在一既定控制波道中發射任意號碼至多個行動站 MS1 - MSn 以聆聽各行動站。在各行動站中，自行動站 MSK 接收到一響應表示其欲在一指定語言波道中建立呼叫。如上所述，實施一項單向鑑認檢查，基地站要求自行動站 MSK 發出 - Resp 1 響應。此項鑑認將在隨后參考圖 2 作更詳盡說明。由於在此階段內，連接尚屬單向，假行動站 BSF 有可能由其他行動站在發送上述任意號碼 RAND 時以上述方式獲得響應。基地站 BSF 因此可能製造一堆 RAND - 響應回答，之後可以由行動站以未授權方式利用。

為了使此種未授權之利用不可能，本發明乃提出一鑑認方法，發表於圖 2 之流程圖。

一鑑認基地站 BS 在其基地站之涵蓋區內聆聽數個行動站 MS1 - MSn 。

此係利用發射任意數字 RAND ，方塊 1 一特定行動站 MSK 意欲建立呼叫，乃以信號 Resp 1 回答，方塊 2 。此信號係從數個輸入資料 PIN , ESN 及 DN 在行動站之微處理器形成，另加收到之任意號碼 RAND ，見圖 3 ，其中 PIN 代表行動站之個人鑑別號碼，ESN 代表行動站之電子序號，DT 代表所撥之號碼。行動站 MSK 因而係 A - 訂戶。微處理器 13 於是發送由 18 - 位元鑑認信號及 8 位元 RAND 信號組成之信號 Resp 1 ，此信號被送至基地站。

基地站從輸入信號 AUTH 及 RAND 以相應之方式計算 Resp 1 ，方塊 3 ，并與行動站所計算及發射之 Resp 信號之值

五、發明說明（ 4 ）

相比較，方塊 4 。當此等值重合時，基地站命令行動站至特定撥出之語言波道，方塊 5 ，通話乃以已知方式連接完成，方塊 6 。以上之方法為以前已熟知者。

根據本發明所提出之方法，基地站此時從一任意號碼 RAND 2 及行動站之個人鑑認號碼 PIN 形成一響應信號 Resp 2 ，PIN 號碼已為基地站所知（方塊 2 ，3 ）。Resp 2 及 RAND 2 均被送至行動站（方塊 7 ）。行動站從其 PIN 及接收之任意號碼 RAND 2 形成 Resp 2 之值，方塊 8 。此時在行動站將收到之 Resp 2 及形成之 Resp 2 之值作一比較（方塊 9 ）。如二值相合，行動站便形成 Resp 3 之值，並將此值送至基地站，（方塊 10 ）。在行動站又自 RAND 2 及 PIN 形成 Resp 3 。基地站以相似方式用 RAND 2 及 PIN 形成 Resp 3 ，此二號碼在基地站均已知悉，方塊 11 。於是將收到及形成之 Resp 3 之值予以比較（方塊 12 ）。如兩值相合，則呼叫之連接不斷而建立語言連接。

根據方塊 7 ，8 及 9 之方法步驟可提供一鑑認檢查，其中之行動站可決定基地站是否為真實，因為由基地站送來之信號 Resp 2 之鑑定在行動站發生，並與在行動站計算之 Resp 2 值比照。自基地站之信號 Resp 2 因此可用來作為來自該站之響應信號。上述之方法俾成本發明提供之方法與根據方塊 2 ，3 及 4 之已知方法二者之間之主要不同點。

根據方塊 10 ，11 及 12 所實施之檢查實質上係根據方塊 2 ，

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（5）

3及4之方法之重覆，即基地站檢查行動站為真。

本法與已知鑑認方法（方塊1－4）之重要差異在於行動動站亦要求基地站回應Resp 2，並依據方塊7－9證實此響應。一假基地站因此必須確實知悉如何計算此響應信號。此一檢查因之為雙向的。

根據方塊2，3及4之鑑認可在行動無線電系統之一總控制波道中完成，而根據方塊7－12之鑑認檢查可在基地站BS 及行動站MSK（方塊5及6）之間建立之語言波道完成。

圖4為一方塊圖說明第一法之各步驟，此情形係祇完成一個雙向鑑認檢查。在此情況下，方塊1－3所用之步驟取代圖2中方塊1－6之步驟。在此情況下，在雙向檢查之前，並不作單向（且已知）之鑑認檢查。一呼叫行動站，例如MSK要求與基地站BS 接通。當基地站接到此一呼叫請求時，便尋找一空着的語言波道，並命令行動站MSK進入此空着的波道。準此，在語言波道上不僅檢查便接通了。而實際之鑑認檢查於是根據上述方塊7－12（圖2）之方式實施，即僅實施一雙向鑑認檢查。

A5
B5

四、中文發明摘要（發明之名稱：於行動無線電系統中實施基地站與行動站間鑑認檢查之方法）

一種在行動電話系統中實施鑑認之方法，該系統中之真正基地站（BS）為衆多之行動站（MS1 - MSn）提供服務。較早已有從基地站（BS）至呼叫行動站（MSK）實施單向鑑認檢查。一假基地站（BSF）能以此方式，收集一些所謂之任意號碼（RAND - Response）響應對實施偽鑑認檢查。為避免此種偽檢查，特別引進一種另一單向從基地站至行動站之鑑認檢查，及由行動站至基地站之鑑認檢查。根據本方法之一具體實例，單向檢查被排除，僅雙向鑑認檢查被實施。

英文發明摘要（發明之名稱：A METHOD OF CARRYING OUT AN AUTHENTICATION CHECK BETWEEN A BASE STATION AND A MOBILE STATION IN A MOBILE RADIO SYSTEM）

A method for carrying out an authentication check in a mobile telephone system in which an authentic base station (BS) serves a plurality of mobile stations (MS1-MSn). It is earlier known to carry out a unidirectional check from the base station (BS) to a calling mobile station (MSk). A false base station (BSf) is able, in this way, to carry out a false authentication check, by collecting a number of so-called RAND-Response pairs. In order to avoid this, there is introduced a further unidirectional authentication check, base station-mobile station, and also an authentication check from the mobile station to the base station. According to one embodiment of the method, the unidirectional check is excluded and only the bidirectional authentication check is carried out.

附註：本案已向 瑞典國 地區 申請專利，申請日期：1995. 3. 8. 案號：9500850-6

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

1992[illegible]
第[illegible]81 號專利申請案
中文申請專利範圍修正本(81年12月)

六、申請專利範圍

1. 一種在行動無線電系統中之基地站(BS)及一行動站間實施鑑認檢查之方法，其中，在建立連接之前，基地站發出鑑認行動站有關之問題，並命令行動站發出第一個響應信號(Resp 1)，該信號在基地站就用來建立行動站之鑑認，其特徵為在基地站建立行動站(2、3、4)之鑑認之后，由基地站發出第二個響應信號(Resp 2)至行動站，行動站因之形成(8)一對應之第二響應信號(Resp 2)以建立(9)基地站之鑑認，在此鑑認建立之后，行動站送出第三個響應信號(Resp 3)，並在接通之前建立行動站之鑑認。

2. 根據申請專利範圍第1項之方法，其中該第二響應信號(Resp 2)係從基地站產生之一任意號碼(RAND 2)及行動站之辦證號碼(PIN)所形成，其中基地站之鑑認之建立係經由第二響應信號與行動站產生之信號加以比較(9)，與所收到之任意號碼(RAND 2)及在行動站可用之辦證號碼(PIN)無關。

3. 根據申請專利範圍第2項之方法，其中該送至基地站之第三個響應信號(Resp 3)係從任意號碼(RAND 2)及行動站之辦證號碼(PIN)所形成，其中該信號係送至基地站；其中該基地站以相似方式自任意號碼(RAND2)及行動站之辦證號碼(PIN)形成一對應之信號；其中在基地站將形成之信號與發出之信號作一比較(12)，當兩信號契合時，便進立語言連接。

4. 一種在行動無線電系統基地站(BS)及行動站(MSK)之間

六、申請專利範圍

在行動站要求並獲特定在一定波道建立連接后實施鑑認檢查之方法，其特徵為在基地站(BS)先形成第一響應信號(Resp 2)，將該第一響應信號送至行動站(MSK)，該行動站與之形成一對應之響應信號(Resp 2)，其目的在證實基地站之真實，在成立此種鑑定之后，行動站將第二響應信號(Resp 3)送至基地站，該站形成一對應之響應信號，並在建立連接之前，建立行動站之真實性。

5. 根據申請專利範圍第4項之方法，其中該第一響應信號(Resp 2)係由基地站產生之任意號碼(RAND 2)及行動站之識別號碼(PIN)所形成，其中基地站之真實性之建立係經由將該第一響應信號與在行動站產生之信號，及視收到之任意號碼(RAND 2)及行動站之識別號碼加以比較(9)而建立。

6. 根據申請專利範圍第4項之方法，其中該送至基地站之第二響應信號(Resp 3)係從該任意號碼(RAND 2)及行動站之識別號碼(PIN)所形成，該信號被送至基地站，且其中基地站以相似方式從任意號碼(RAND 2)及基地站可用之行動站之辨證號碼(PIN)形成一對應之信號；其中在基地站實施一比較(12)，即將基地站形成之信號與該站收到之信號予以比較，當信號契合時語言連接得以建立。

7. 一種在一包括一網路及一行動站之行動無線電系統中實施網路之鑑認檢查之方法，包含下列步驟：

在網路中計算對一任意號碼之響應；

六、申請專利範圍

從網路將響應及任意號碼送至行動站；

在行動站計算自網路收到之任意號碼之響應；及

將在網路中計算之響應與在行動站中計算之響應予以比較。

8. 根據申請專利範圍第7項之方法，其中之行動站無線電系統係一細胞行動電話系統。

9. 根據申請專利範圍第7項之方法，其中之行動無線電系統係一呼叫器系統。

10. 根據申請專利範圍第7項之方法，其中在網路中及行動站中計算之響應，除了任意號碼外，尚視其他資料而定。

11. 根據申請專利範圍第10項之方法，其中之其他資料包括行動站之個人辨證號碼。

12. 根據申請專利範圍第10項之方法，其中之其他資料包括行動站之電子序號。

13. 根據申請專利範圍第10項之方法，其中之其他資料包括撥號。

14. 一種用以在一行動無線電系統中鑑認一網路及一行動站之方法，包含下列步驟：

在每一網路及行動站中形成第一及第二響應信號，該信號等視從網路傳送至行動站之任意號碼而定，

將在網路中形成之第一響應信號傳送至行動站；

在行動站中將在行動站形成之第一響應信號與自網路接收之第一響應信號加以比較；

199250

六、申請專利範圍

將在行動站中形成之第二響應信號傳送至網路；及

將在網路中形成之第二響應信號與自行動站收到之第二響應信號加以比較。

15. 根據申請專利範圍第14項之方法，其中第一及第二響應信號除了任意號碼外尚視其他資料而定。

16. 根據申請專利範圍第15項之方法，其中之其他資料包括行動站之個人辨認號碼。

17. 根據申請專利範圍第15項之方法，其中之其他資料包括行動站之電子序號。

18. 根據申請專利範圍第15項之方法，其中之其他資料包括撥號。

19. 根據申請專利範圍第14項之方法，其中，在行動站形成之第二響應信號，僅在行動站中形成之第一響應信號與自網路中接收之第一響應信號相同時，傳送至行動站。

20. 根據申請專利範圍第14項之方法，尚包括在網路及行動站之間如在網路中形成之第二響應信號與自行動站接收之第二響應信號不相同時，建立語言通信之方法。

21. 根據申請專利範圍第14項之方法，尚包括在網路及行動站之間如在網路中形成之第二響應信號與自行動站接收之第二響應信號不相同時，結束語言通信之方法。

22. 一種控制一網路、及在該網路所涵蓋地區之一行動站之間所建立之呼叫之方法，該方法包括下列步驟：

自網路將第一任意號碼送至行動站；

六、申請專利範圍

在行動站中計算第一值，該值視自網中收到之第一任意信號而定；

自行動站將第一值送至網路；

在網路中計算與第一值對應之值；

將第一值與對應之第一值加以比較；

如第一值與對應之第一值符合時，分配行動站－語言波道；

在網路中計算第二值，該值視第二任意信號而定；

將第二值及自網路之第二任意信號送至行動站；

在行動站中計算與第二值對應之值；

將第二值與對應之第二值加以比較；

在行動站計算第三值，該值視第二任意信號而定；

由行動站將第三值送至網路；及

在網路中計算與第三值對應之值；

將第三值與對應之第三值加以比較；

如第三值與對應之第三值符合，建立一呼叫於網路與行動站之間。

23. 根據申請專利範圍第23項之方法，其中，第三值係在行動站中計算並在第二值與對應之第二值符合時，將其送往網路。

24. 根據申請專利範圍第23項之方法，其中，第一任意信號及第一值被送至控制波道。

25. 根據申請專利範圍第24項之方法，其中之第二任意信號，第二值及第三值被送至分配之語言波道。

六、申請專利範圍

26. 一種用以在一含網路及行動站之行動無線電系統實施鑑認之方法，包含下列步驟：

產生一任意號碼；

在網路及行動站之間交換此任意號碼；

在網路及行動站計算鑑認號碼，該號碼為任意號碼之函數；

將在行動站計算之鑑認號碼與自網路收到之鑑認號碼加以比較。

27. 根據申請專利範圍第26項之方法，其中在網路及在行動站計算之鑑認號碼為除了任意號碼外，至少尚為另一號碼之函數。

28. 根據申請專利範圍第27項之方法，其中之鑑認號碼為任意號碼及行動站之個人辨證號碼之函數。

29. 根據申請專利範圍第27項之方法，其中之鑑認號碼為任意號碼及行動站之電子序號之函數。

30. 根據申請專利範圍第27項之方法，其中之鑑認號碼為任意號碼，個人辨證號碼及行動站之電子序號之函數。

31. 一種用以在一行動無線電系統中之網路與行動站之間實施鑑認檢查之方法，包含下列步驟：

選擇第一任意值；

提供第一任意值至每一網路及行動站；

在每一網路及行動站中由第一任意值計算一第一鑑認值；

將在行動站計算之第一鑑認值送至網路；

六、申請專利範圍

將在網路中計算之第一鑑認值與自行動站收到之第一鑑認值加以比較；

選擇第二任意值；

將第二任意值提供給每一網路及行動站；

在每一網路及行動站中自第二任意值計算第二鑑認值；

將在網路中計算之第二鑑認值送至行動站；及

將在行動站中計算之第二鑑認值與自網路收到之第二鑑認值加以比較。

32. 根據申請專利範圍第32項之方法，其中第一鑑認值在控制波道上送出，而第二鑑認值在語言波道上送出。

33. 一種用以在一含網路及行動站之細胞行動電話系統實施鑑認方法，包含下列步驟；

在每一網路及行動站中自任意號碼輸入至鑑認算法計算一鑑認輸出；

將在網路及行動站中計算之鑑認輸出傳送至行動站；及

將在行動站計算之鑑認輸出與自網路收到之鑑認輸出互相比較。

34. 根據申請專利範圍第33項之方法，其中任意號碼輸入係許多輸入至鑑認算法中之一個，而鑑認輸出為自鑑認算法之許多輸出中之一個。

(修正本) 87.12

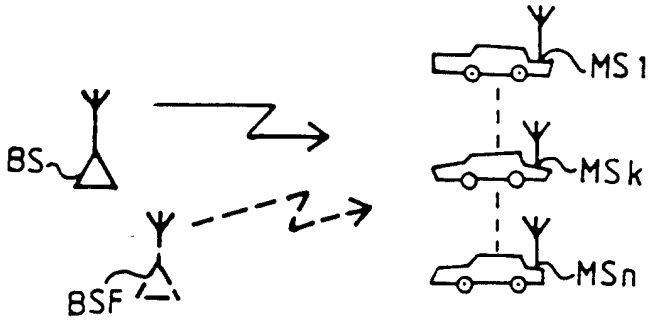

圖 1

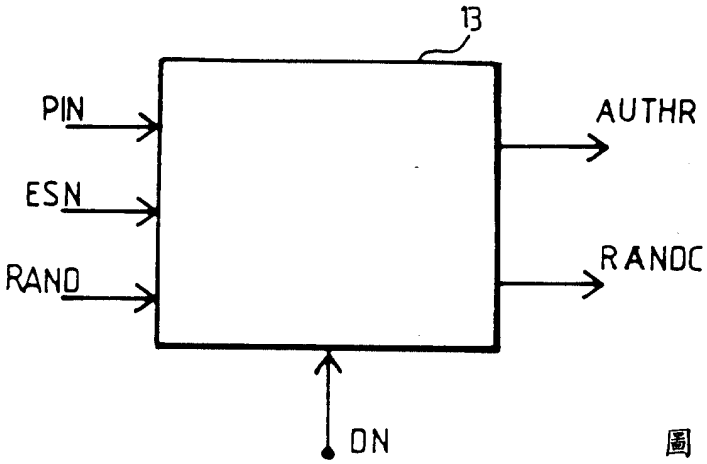

圖 3

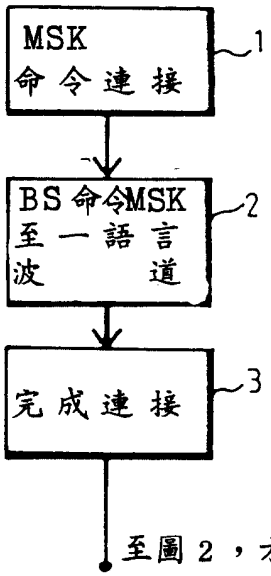

圖 4

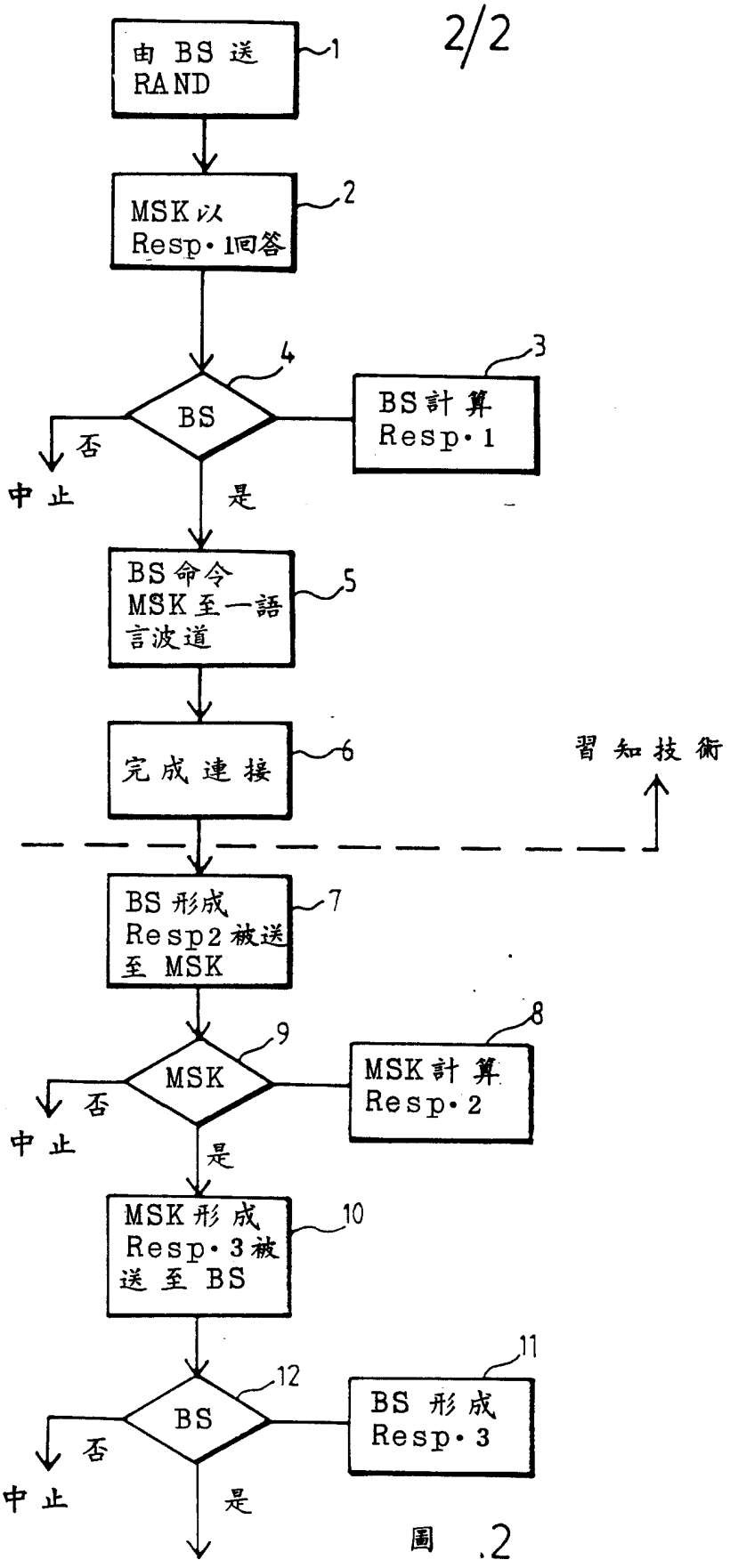
由 BS 送 RAND
1
MSK以 Resp·1回答
2
BS
4
BS計算 Resp·1
3
否
中止
是
BS命令 MSK至一語言波道
5
完成連接
6
習知技術
BS形成 Resp2被送至 MSK
7
MSK
9
MSK計算 Resp·2
8
否
中止
是
MSK形成 Resp·3被送至 BS
10
BS
12
BS形成 Resp·3
11
否
中止
是

圖 .2