I378702

101 年 4 月 02 日修正替換頁

公告本
101.4.2

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96131436

※ 申請日期：96.8.24　　※IPC 分類：H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

群組認證方法 / GROUP AUTHENTICATION METHOD

二、申請人：（共 2 人）

姓名或名稱：（中文/英文）

1. 財團法人工業技術研究院/ INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE

2. 國立交通大學/NATIONAL CHIAO TUNG UNIVERSITY

代表人：（中文/英文）1. 蔡清彥/CHING-YEN TSAY　（簽章）

2. 吳妍華/LEE WU, YAN-HWA　（簽章）

住居所或營業所地址：（中文/英文）

1. 新竹縣竹東鎮中興路四段 195 號/ NO. 195, SECTION 4, CHUNG HSING ROAD, CHUTUNG, HSINCHU, TAIWAN, R.O.C.

2. 新竹市大學路 1001 號/NO. 1001, DASYUE RD., HSINCHU CITY, 300, TAIWAN (R.O.C.)

國　籍：（中文/英文）1-2 中華民國/TW

三、發明人：（共 3 人）

姓　名：（中文/英文）

1. 陳鈺玟 / CHEN, YU-WEN
2. 王瑞堂 / WANG, JUI-TANG
3. 曾建超 / TSENG, CHIEN-CHAO

國　籍：（中文/英文）1-3 中華民國/TW

四、聲明事項：

☑ 主張專利法第二十二條第二項☑第一款或☐第二款規定之事實，其事實發生日期為： 2007 年 4 月 20 日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

一種群組認證方法，適用於通訊系統，此系統包括使用者群組、服務網路與家網路。使用者群組包括至少一行動台。家網路預先產生並分配群組認證金鑰給自己與同一使用者群組的多個行動台，並分別產生行動台認證金鑰給各行動台。家網路並產生群組列表，此群組列表記錄使用者群組之相關資訊。家網路具有資料庫，可記錄群組列表。服務網路具有資料庫，此資料庫用以記錄自家網路傳送之群組列表與群組認證資料。此方法包括：服務網路對行動台進行辨識動作；服務網路根據辨識動作的結果判斷通訊系統要進行完整的雙向認證動作或區域認證動作。

六、英文發明摘要：

A group authentication method applied to a communication system is disclosed. The communication system includes a user group, a serving network and a home network. Wherein, the user group includes at least one mobile station. The home network generates and pre-distributes a group authentication key to itself and all the mobile stations in the same user group. The home network also generates and pre-distributes unique mobile station authentication key to the corresponding mobile stations. The home network generates the group list correspondingly. The home network has a database used to record the group list.

The serving network has a database used to record group lists and group authentication data received from the home network. The method includes: proceeding an identification action for the mobile station in the serving network; and proceeding a full authentication action or a local authentication action according to the result of the identification action.

七、指定代表圖：

（一）本案指定代表圖為：圖 7。

（二）本代表圖之元件符號簡單說明:

700、701、702：步驟流程

MS_{M1-1}、MS_{M1-2}：行動台

HN：家網路

SN：服務網路

M1：群組

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

九、發明說明：

【發明所屬之技術領域】

本發明是有關於一種認證方法，且特別是有關於一種可提供群組認證的群組認證方法。

【先前技術】

隨著無線網路各種殺手級的應用不斷出現，即時通訊服務（real-time communication service）的需求也蓬勃發展。然而，無線網路的封包大多都於空氣中傳送，使得無線網路無法提供與有線網路同層級的安全性。且無線網路的頻寬與速度也遠比不上有線網路的效率，加上漫遊（roaming）於不同網域時轉送認證訊息造成的延遲，往往大幅增加了換手（handoff）時所需的時間。如何在確保資料傳輸的安全性下，加快漫遊時的換手速度，已成為許多研究機構與業界廠商所欲克服的問題。

現今網路中的安全認證與金鑰分配(Authentication and Key Agreement，簡稱 AKA）機制，大都是針對單一行動台(Mobile Station)所設計。例如 UMTS AKA 協定，當行動台漫遊時，當地提供網路服務的業者（就是所謂的服務網路，Serving Network）會依據行動台所註冊的家網路（Home Network）要求行動台的認證向量（Authentication Vectors），使得服務網路進而與行動台執行相互認證與主金鑰（Master key）的分配。

為了滿足不同的無線網路之需求，一般的認證與金鑰分配機制大抵可以分為兩個程序：a、.認證註冊登記與分配程序（Registration and Authentication Data Distribution）；b、.行動台認證與金鑰分配程序（User Authentication and Key Agreement）。服務網路會對漫遊至此服務網路的行動台要求執行雙向認證，首先，此服務網路向行動台所屬的家網路要求行動台相關的認證資料，接下來，服務網路與行動台根據所取得的認證資料進行一連串的產生、回覆認證質疑訊息（challenge message），並產生出認證成功後可用的主會議金鑰。

請參照圖 1，圖 1 為 UMTS AKA 的認證方法流程圖。此方法適用於通訊系統，此通訊系統包括行動台 MS1、服務網路 SN 與家網路 HN。其中，行動台 MS1 與家網路 HN 具有預先分配之加密金鑰（Secret Key）K（參見圖 2），家網路 HN 與行動台 MS1 有訊息認證碼（Message Authentication Code，簡稱 MAC）產生函數 f1、認證訊息產生函數 f2、密文金鑰（Cipher Key）產生函數 f3 與訊息完整性金鑰（Integrity Key）產生函數 f4。家網路 HN 更有認證金鑰（Authentication Key）產生函數 f5 與一組認證參數 AMF（Authentication Management Field）。而服務網路 SN 與家網路 HN 皆具有資料庫，分別儲存認證程序中所需使用的各種資料。當行動台 MS1 漫遊換手時，行動台 MS1 須向服務網路 SN 執行雙向認證。此方法的步驟包括辨識步驟

100、獲得認證向量步驟 101 與行動台認證與金鑰分配步驟 102。其中，辨識步驟 100 及獲得認證向量步驟 101 為上述之認證註冊與分配程序，行動台認證與金鑰分配步驟 102 為上述之行動台認證與金鑰分配程序。在此方法中，雙向認證是指進行獲得認證向量步驟 101 與行動台認證與金鑰分配步驟 102。

當此方法應用於通訊系統時，首先，此方法會進行辨識步驟 100，辨識步驟 100 的流程如下：（子步驟 100a）服務網路 SN 會對欲進行認證的行動台 MS1 索取識別資料；（子步驟 100b）行動台 MS1 產生識別資料並將識別資料傳給服務網路 SN，其中，此辨識資料有行動台 MS1 的身分代碼，此身分代碼可供服務網路 SN 辨識行動台 MS1 的身分；（子步驟 100c）服務網路 SN 接收 MS1 所產生的識別資料並辨識此行動台 MS1 的身分，服務網路 SN 的資料庫根據此識別資料建立此行動台專屬的資訊欄。

之後，此方法會進行獲得認證向量步驟 101，獲得認證向量步驟 101 的流程如下：（子步驟 101a）服務網路 SN 會轉送辨識資料給家網路 HN，並對家網路 HN 請求此行動台 MS1 的認證向量；（子步驟 101b）家網路 HN 接收此辨識資料，並根據此辨識資料產生數個認證向量 AV(1)、AV(2)、...、AV(n)且將數個認證向量 AV(1)~AV(n)傳送給服務網路 SN；（子步驟 101c）服務網路 SN 的資料庫會儲存此等認證向量

AV(1)~AV(n)。

最後，UMTS AKA 方法會進行行動台認證與金鑰分配步驟 102 以完成行動台 MS1 之認證，行動台認證與金鑰分配步驟 102 的流程如下：（子步驟 102a）服務網路 SN 從其資料庫選取所記錄的認證向量 AV(i)並將此認證向量 AV(i)的部分資訊 RAND(i)與 AUTN(i)（底下將參照圖 2 說明）傳送給行動台 MS1；（子步驟 102b）行動台 MS1 根據認證向量 AV(i)的部份資訊 RAND(i)與 AUTN(i)（底下將參照圖 3 說明）對家網路 HN 進行認證；（子步驟 102c）若行動台 MS1 成功地認證家網路 HN，則行動台 MS1 會根據認證向量 AV(i)的部分資訊 RAND(i)與預先分配之加密金鑰 K 產生行動台認證資料 RES(i)並將行動台認證資料 RES(i)傳送給服務網路 SN；（子步驟 102d）服務網路 SN 接收行動台認證資料 RES(i)，並根據行動台認證資料 RES(i)對行動台 MS1 進行認證並產生認證結果；（子步驟 102e）服務網路 SN 回覆認證結果給行動台 MS1；（子步驟 102f）行動台 MS1 接收此認證結果並確認此認證結果；（子步驟 102g）若認證結果表示服務網路 SN 成功地認證行動台 MS1，則服務網路 SN 會選取密文金鑰 CK(i)與訊息完整性金鑰 IK(i)進行安全通訊，而行動台則是利用 RAND(i)加上預先分配的加密金鑰 K，與密文金鑰產生函數 f3、訊息完整性金鑰產生函數 f4，計算出 CK(i)與 IK(i)進行安全通訊。

請參照圖2，圖2是UMTS AKA方法中認證向量AV(i)的產生方法示意圖。一般的UMTS AKA中，大概會產生數個認證向量AV(1)~AV(3)。家網路HN會根據識別資料的身分代碼從家網路HN的資料庫搜尋行動台MS1的加密金鑰K（參照200），家網路HN會產生序號SQN(i)（參照201）與亂數RAND(i)（參照202）。家網路HN將亂數RAND(i)、加密金鑰K、序號碼SQN(i)與一組認證參數AMF輸入認證訊息碼產生函數f1以產生認證訊息碼MAC(i)；家網路HN將亂數RAND(i)與加密金鑰K輸入認證訊息產生函數f2以產生認證訊息XRES(i)；家網路HN將亂數RAND(i)與加密金鑰K輸入密碼金鑰產生函數f3以產生密文金鑰CK(i)；家網路HN將亂數RAND(i)與加密金鑰K輸入訊息完整性金鑰產生函數f4以產生訊息完整性金鑰IK(i)；家網路HN將亂數RAND(i)與加密金鑰K輸入認證金鑰產生函數f5以產生隱藏金鑰AK(i)；家網路HN更將序號碼SQN(i)與隱藏金鑰AK(i)作一互斥或的運算以得到運算結果SQN(i)⊕AK(i)（參照203）。家網路HN將運算結果SQN(i)⊕AK(i)、一組認證參數AMF與訊息認證編碼MAC(i)合併成認證標籤（Authentication Token）AUTN(i)（亦即AUTN(i)={SQN(i)⊕AK(i)||AMF||MAC(i)}，||表示位元合併的運算子，例如{110||101}={110101}），之後，家網路HN將亂數RAND(i)、認證訊息XRES(i)、加密金鑰CK(i)、訊息完整性金鑰IK(i)與認證標籤

AUTN(i)合併成認證向量AV(i)(亦即AV(i)={RAND(i)||XRES(i)||CK(i)||IK(i)||AUTN(i)})。

圖3是行動台MS1根據認證向量AV(i)的部份資訊RAND(i)與AUTN(i)對家網路HN進行認證與產生行動台認證資料RES(i)的示意圖。首先，行動台MS1將亂數RAND(i)與行動台MS1的加密金鑰K輸入認證金鑰產生函數f5以產生隱藏金鑰AK(i)。接下來，行動台MS1將認證標籤AUTN(i)的運算結果SQN(i)⊕AK(i)與行動台MS1所產生的隱藏金鑰AK(i)做互斥或的動作，以產生序號SQN(i)。行動台MS1將接收的一組認證參數AMF、行動台MS1所產生的序號碼SQN(i)與行動台MS1的加密金鑰K輸入認證訊息碼產生函數f1以產生訊息認證編碼XMAC(i)，行動台MS1比對XMAC(i)與由服務網路SN傳來的MAC(i)以藉此進行認證。若行動台MS1成功地認證家網路HN，則行動台MS1會將認證向量AV(i)的亂數RAND(i)與行動台MS1的加密金鑰K輸入認證訊息產生函數f2以產生行動台認證資料RES(i)。同時，行動台MS1亦將行動台MS1的加密金鑰K與接收到的認證向量AV(i)之亂數RAND(i)輸入密碼金鑰產生函數f3以及訊息完整性金鑰產生函數f4以產生密文金鑰CK(i)與訊息完整性金鑰IK(i)，藉此提供之後進行安全通訊所需之密文金鑰CK(i)與訊息完整性金鑰IK(i)。行動台MS1會將產生的行動台認證資料RES(i)傳送給服務網路SN，SN比對行動台認證資料

RES(i)與認證訊息 XRES(i)以藉此進行認證。

另外，上述之行動台 MS1 對家網路 HN 進行認證與服務網路 SN 對行動台 MS1 認證之結果，若結果為認證失敗，則此通訊系統會中斷整個通訊，或會要求重新進行認證等。為了方便解說，圖 1 是假設每一認證結果皆為成功時所繪之示意圖，所以圖 1 沒有繪出認證失敗的步驟。

上述之 UMTS AKA 的認證方法中，服務網路 SN 的資料庫需要大量的記憶空間，以儲存 n 個認證向量 AV(1)~AV(n)，且 n 個認證向量 AV(1)~AV(n)所能提供的認證次數只有 n 次。另外，UMTS AKA 的認證方法中，家網路 HN 無法認證行動台 MS1，也就是家網路 HN 無法得知藉由服務網路 SN 向家網路 HN 要求認證向量 AV(1)~AV(n)的行動台 MS1 是否合法。

接下來，請參照圖 4，圖 4 是採用 IEEE AINA 2005 會議論文"Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption"中的 UMTS X-AKA 認證方法，行動台 MS1 第一次漫遊換手時的認證流程圖。此方法適用於通訊系統，此通訊系統包括行動台 MS1、服務網路 SN 與家網路 HN。其中，行動台 MS1 與家網路 HN 具有預先分配之加密金鑰，而服務網路 SN 與家網路 HN 皆具有資料庫。當行動台 MS1 第一次漫遊換手時，行動台 MS1 須向服務網路 SN 執行雙向認證。此方法的步驟包括辨識步驟 400、獲得

認證資料步驟 401 與行動台認證與金鑰分配步驟 402。其中，辨識步驟 400 及獲得認證資料步驟 401 為前述之認證登記與分配程序，行動台認證與金鑰分配步驟 402 為前述之行動台認證與金鑰分配程序。

當此方法應用於通訊系統時，首先，此方法會進行辨識步驟 400，辨識步驟 400 的流程如下：（子步驟 400a）服務網路 SN 會對欲進行認證的行動台 MS1 索取識別資料；（子步驟 400b）行動台 MS1 產生識別資料與時間標籤 t 並將識別資料與時間標籤 t 傳給服務網路 SN，其中，此辨識資料有行動台 MS1 的身分代碼，此身分代碼可供服務網路 SN 辨識行動台 MS1 的身分；（子步驟 400c）服務網路 SN 接收 MS1 所產生的識別資料並從服務網路 SN 的資料庫辨識此行動台 MS1 的身分，若此資料庫沒有記錄此行動台 MS1 所屬的認證資料，則服務網路 SN 的資料庫根據此識別資料建立此行動台專屬的資訊欄並進行步驟 401，若此資料庫有記錄此行動台 MS1 所屬的認證資料與暫時性認證金鑰，則從此資料庫選取認證資料與暫時性認證金鑰，並進行如圖 5 的步驟 501，在此圖 4 已假設下一個步驟為步驟 401（為了解說方便，假設行動台 MS1 為第一次漫遊換手的行動台。）。

之後，此方法會進行獲得認證資料步驟 401，獲得認證資料步驟 401 的流程如下：（子步驟 401a）服務網路 SN 會轉送辨識資料與時間標籤 t 給家網路 HN，

並對家網路 HN 請求此行動台 MS1 的認證資料；（子步驟 401b）家網路 HN 接收此辨識資料與時間標籤 t，並根據此辨識資料與時間標籤 t 產生認證資料（包含一把暫時性認證金鑰），然後，家網路 HN 將認證資料傳送給服務網路 SN；（子步驟 401c）服務網路 SN 的資料庫會儲存此認證資料與暫時性認證金鑰。

最後，UMTS X-AKA 方法會進行行動台認證與金鑰分配步驟 402 以完成行動台 MS1 之認證，行動台認證與金鑰分配步驟 402 的流程如下：（子步驟 402a）服務網路 SN 產生服務網路認證資料與亂數並將服務網路認證資料與亂數傳送給行動台 MS1；（子步驟 402b）行動台 MS1 根據服務網路認證資料與亂數來對服務網路 SN 進行認證；（子步驟 402c）若行動台 MS1 成功地認證服務網路 SN，則行動台 MS1 會根據認證資料的部分資訊與預先分配之加密金鑰產生行動台認證資料，並將行動台認證資料傳送給服務網路 SN；（子步驟 402d）服務網路 SN 接收行動台認證資料，並根據行動台認證資料對行動台 MS1 進行認證並產生認證結果；（子步驟 402e）服務網路 SN 回覆認證結果給行動台 MS1；（子步驟 402f）行動台 MS1 接收此認證結果並確認此認證結果；（子步驟 402g）若認證結果表示服務網路 SN 成功地認證行動台 MS1，則行動台 MS1 與服務網路 SN 同時會透過暫時性認證金鑰與隨機亂數產生主金鑰來保護雙方訊息的傳送安全。

請參照圖 5，圖 5 是採用 UMTS X-AKA 認證方法時，行動台 MS1 經第一次漫遊換手後的認證流程圖。此流程步驟包括辨識步驟 500 與行動台認證與金鑰分配步驟 501。其中，辨識步驟 500 為前述之認證登記與分配程序，行動台認證與金鑰分配步驟 501 為前述之行動台認證與金鑰分配程序。服務網路 SN 會判斷其資料庫是否存有此行動台 MS1 所屬的認證資料與暫時性認證金鑰，若有，則服務網路 SN 不再向家網路 HN 要求認證資料與暫時性認證金鑰。因為行動台 MS1 非第一次漫遊換手，所以服務網路 SN 的資料庫會有記錄行動台 MS1 所屬的認證資料與暫時性認證金鑰。

首先，此方法會進行辨識步驟 500，辨識步驟 500 的流程如下：（子步驟 500a）服務網路 SN 會對欲進行認證的行動台 MS1 索取識別資料；（子步驟 500b）行動台 MS1 產生識別資料與時間標籤 t 並將識別資料與時間標籤 t 傳給服務網路 SN，其中，此辨識資料有行動台 MS1 的身分代碼，此身分代碼可供服務網路 SN 辨識行動台 MS1 的身分；（子步驟 500c）服務網路 SN 接收 MS1 所產生的識別資料並辨識此行動台 MS1 的身分，服務網路 SN 根據識別資料搜尋其資料庫搜尋是否有其行動台 MS1 所屬的認證資料與暫時性認證金鑰，若沒有，則其流程應如圖 4 的方法流程圖所示，圖 5 是假設服務網路 SN 的資料庫已存有行動台 MS1 的認證資料與暫時性認證金鑰，因此服務網路 SN 會從其資

料庫找到行動台 MS1 所屬的認證資料與暫時性認證金鑰。

之後，UMTS XAKA 方法會進行行動台認證與金鑰分配步驟 501 以完成行動台 MS1 之認證，行動台認證與金鑰分配步驟 501 的流程如下：（子步驟 501a）服務網路 SN 根據產生服務網路認證資料與亂數並將服務網路認證資料與亂數傳送給行動台 MS1；（子步驟 501b）行動台 MS1 根據服務網路認證資料與亂數來對服務網路 SN 進行認證；（子步驟 501c）若行動台 MS1 成功地認證服務網路 SN，則行動台 MS1 會根據認證資料的部分資訊與預先分配之加密金鑰產生行動台認證資料，並將行動台認證資料傳送給服務網路 SN；（子步驟 501d）服務網路 SN 接收行動台認證資料，並根據行動台認證資料對行動台 MS1 進行認證並產生認證結果；（子步驟 501e）服務網路 SN 回覆認證結果給行動台 MS1；（子步驟 501f）行動台 MS1 接收此認證結果並確認此認證結果；（子步驟 501g） 若認證結果表示服務網路 SN 成功地認證行動台 MS1，則行動台 MS1 與服務網路 SN 同時會透過暫時性認證金鑰與隨機亂數產生主金鑰來保護雙方訊息的傳送安全。

另外，上述之行動台 MS1 對服務網路 SN 進行認證與服務網路 SN 對行動台 MS1 認證之結果，若結果為認證失敗，則可以此通訊系統會中斷整個通訊，或者會要求重新進行認證等。為了方便解說，圖 4 與圖 5

是假設每一認證結果皆為成功時所繪之示意圖，所以沒有畫出認證失敗的步驟。

簡言之，UMTS X-AKA 方法的精神在於家網路 HN 產生暫時性認證金鑰給服務網路 SN，並藉此授權服務網路 SN 對行動台 MS1 進行認證，使得行動台 MS1 進行再一次的漫遊認證時，家網路 HN 與服務網路 SN 之間的訊息交通流量（Traffic Load）可以降低。UMTS X-AKA 方法亦使服務網路 SN 的資料庫所需求的儲存空間也可以被減少，但是 UMTS XAKA 方法依然不能使家網路 HN 對行動台 MS1 進行認證。

接者，請參照圖 6，圖 6 是美國第 6,711,400 號專利所提供的認證方法流程圖。此方法適用於通訊系統，此通訊系統包括行動台 MS1、服務網路 SN 與家網路 HN。其中，行動台 MS1 與家網路 HN 具有預先分配之認證加密金鑰，而服務網路 SN 與家網路 HN 皆具有資料庫。當行動台 MS1 漫遊換手時，行動台 MS1 須向服務網路 SN 執行雙向認證。此方法的步驟包括辨識步驟 600、獲得認證資料步驟 601 與行動台認證與金鑰分配步驟 602。其中，辨識步驟 600 及獲得認證資料步驟 601 為上述之認證登記與分配程序，行動台認證與金鑰分配步驟 602 為上述之行動台認證與金鑰分配程序。在此方法，雙向認證是指進行獲得認證資料步驟 601 與行動台認證與金鑰分配步驟 602。

當此方法應用於通訊系統時，首先，此方法會進行

辨識步驟600，辨識步驟600的流程如下：（子步驟600a）行動台MS1利用預先分配的認證加密金鑰與第一亂數產生識別資料，並將識別資料與第一亂數傳送給服務網路SN，其中，此辨識資料有行動台MS1的身分代碼，此身分代碼可供服務網路SN辨識行動台MS1的身分；（子步驟600b）服務網路SN接收MS1所產生的識別資料並辨識此行動台MS1的身分，服務網路SN的資料庫根據此識別資料建立此行動台專屬的資訊欄。

之後，此方法會進行獲得認證資料步驟601，獲得認證資料步驟601的流程如下：（子步驟601a）服務網路SN會轉送辨識資料與第一亂數給家網路HN，並對家網路HN請求此行動台MS1的認證資料；（子步驟601b）家網路HN接收此辨識資料與第一亂數，並根據此辨識資料取出認證加密金鑰；（子步驟601c）家網路HN先產生第二亂數，再根據第一亂數、第二亂數與認證加密金鑰產生認證資料、密碼金鑰與比對資料，並將認證資料、密碼金鑰、比對資料與第二亂數傳送給服務網路SN；（子步驟601d）服務網路SN接收認證資料、密碼金鑰、比對資料與第二亂數，且服務網路SN的資料庫會儲存此密碼金鑰與比對資料。

最後，此方法會進行行動台認證與金鑰分配步驟602以完成行動台MS1之認證，行動台認證與金鑰分配步驟602的流程如下：（子步驟602a）服務網路SN從其資料庫傳送認證資料與第二亂數傳送給行動台

MS1；（子步驟 602b）行動台 MS1 根據認證資料對家網路 HN 進行認證；（子步驟 602c）若行動台 MS1 成功地認證家網路 HN，則行動台 MS1 會根據預先分配的認證加密金鑰與第二亂數產生行動台認證資料與密碼金鑰並將行動台認證資料傳送給服務網路 SN；（子步驟 602d）服務網路 SN 接收行動台認證資料，並根據行動台認證資料與資料庫內的比對資料對行動台 MS1 進行認證並產生認證結果；（子步驟 602e）服務網路 SN 回覆認證結果給行動台 MS1；（子步驟 602f)行動台 MS1 接收此認證結果並確認此認證結果；（子步驟 602g）若認證結果表示服務網路 SN 成功地認證行動台 MS1，則行動台 MS1 與服務網路 SN 會計算出主金鑰進行安全通訊。

另外，上述之行動台 MS1 對家網路 HN 進行認證與服務網路 SN 對行動台 MS1 認證之結果，若結果為認證失敗，則可以此通訊系統會中斷整個通訊，或者會要求重新進行認證等。為了方便解說，圖 6 是假設每一認證結果皆為成功時所繪之示意圖，因此沒有畫出認證失敗的步驟。

簡言之，美國第 6,711,400 號專利所提供的認證方法是由行動台 MS1 指定第一亂數給家網路 HN，因此能確保認證資料的新鮮性（Freshness），且服務網路 SN 僅是負責轉送由家網路 HN 產生的認證資料與驗證行動台 MS1 的行動台認證資料。但此方法的認證資料，

每次僅會產生一份，而且只能使用一次，如此一來將會增加服務網路 SN 與家網路 HN 間的管理訊息（signaling）的多餘負擔（overhead）（亦即，會增加服務網路 SN 與家網路 HN 之間的訊息交通量（traffic load）與造成頻寬的浪費。）。

然而，在群組通訊服務日漸發達的今天，無線網路的發展上也逐漸出現了群組的概念，在一個服務網路裡面會有很大的機率是同時服務屬於同一群組的行動台，也就是說，群組內的行動台大部分會一起漫遊。例如同一家公司的員工一起參加某一個會議或者是同一個學校的學生一起到校外博物館、餐館。然而現今網路上並沒有提供群組認證的安全機制，使得經常一起漫遊之同群組的行動台必須分開認證，另外服務網路與家網路發出的認證請求與回覆訊息更加重了網路的流量負擔瞬間大量的認證訊息，因此可能會浪費服務網路與家網路之間的頻寬。

然而，前述的方法都是針對單一個行動台認證所設計的，當網路環境出現群組通訊的情形時，上述的方法都會面臨相同的問題：服務網路必須分別為每一個行動台轉送認證請求至相同家網路，然後服務網路同時接收家網路傳來之每個行動台所屬的認證資料。本發明提出利用群組資料共享的概念，一方面透過共享群組認證資料達到群組成員認證金鑰先期傳遞（Group Authentication Key Pre-distribution）的效果，另一外面

用區域認證（local authentication）來降低服務網路與家網路之間的資料傳輸所佔用的頻寬。

【發明內容】

本發明的目的在提供一種群組認證的方法，此方法適用於任何需要遠端認證通訊系統，此通訊系統包括使用者群組、服務網路與家網路。其中，使用者群組包括至少一行動台。服務網路具有第一資料庫，此第一資料庫用以記錄自該家網路傳送之群組列表與群組認證資料。此通訊系統預先分配群組認證金鑰與行動台認證金鑰給行動台與家網路，家網路並產生群組列表。家網路具有第二資料庫，第二資料庫用以記錄群組列表，此方法包括：服務網路對行動台進行一辨識動作；服務網路根據服務網路對行動台進行該辨識動作的結果判斷整個認證通訊系統是否需要家網路提供認證資料才能完成認證。如果服務網路資料庫已經有認證資料，服務網路可以直接與行動台執行區域認證（Local Authentication）。而如果服務網路資料庫沒有行動台的認證資料，此時服務網路需要向家網路取得認證資料，才會有能力與行動台執行完整的雙向認證（Full Authentication）。

本發明的另一目的在提供一種用於家網路、服務網路與使用者群組彼此進行認證的群組認證方法。其中，使用者群組有行動台，行動台與家網路具有群組認證金

鑰（Group Authentication Key）與行動台認證金鑰。家網路有群組列表，行動台有行動台身分編號、群組編號與初始值。服務網路具有資料庫，資料庫可以記錄自家網路傳送的群組列表，此方法包括：（a）產生辨識資料於行動台，其中，辨識資料包括第一認證訊息碼與行動台身分編號；（b）傳送辨識資料至服務網路；（c）檢查該行動台編號是否紀錄於該資料庫內的該群組列表，若否，（c-no-1）傳送該辨識資料至該家網路；（c-no-2）根據該識別資料產生第二認證訊息碼於家網路；（c-no-3）比較第一認證訊息碼與第二認證訊息碼；（c-no-4）若第一認證訊息碼與第二認證訊息碼相同，則家網路成功地認證行動台；（c-no-5）利用群組認證金鑰產生暫時性群組認證金鑰於家網路；（c-no-6）傳送群組認證資料與群組列表給服務網路，其中，群組認證資料包括暫時性群組認證金鑰；（c-no-7）紀錄該群組列表與該群組認證資料於該服務網路的該資料庫；若是，（c-yes-1）根據行動台身分編號從服務網路的資料庫獲得群組認證資料；（d）利用群組認證資料產生第三認證訊息碼於服務網路；（e）傳送服務網路認證資料至行動台，服務網路認證資料包括第三認證訊息碼；（f）利用服務網路認證資料產生暫時性群組認證金鑰於行動台與利用暫時性群組認證金鑰產生第四認證訊息碼於行動台；（g）比較第三認證訊息碼與第四認證訊息碼於行動台，若第三認證訊息碼與第四認證訊息碼

相同，則行動台成功地認證服務網路與家網路；（h）利用群組認證資料計算出主金鑰於服務網路；（i）利用服務網路認證資料與暫時性群組認證金鑰產生主金鑰與第五認證訊息碼於行動台；（j）傳送第五認證訊息碼至服務網路；（k）利用群組認證資料產生第六認證訊息碼於服務網路；（l）比較第五認證訊息碼與第六認證訊息碼於服務網路，若第五認證訊息碼與第六認證訊息碼相同，則服務網路成功地認證該行動台；（m）利用主金鑰保護服務網路與行動台欲進行傳輸之傳輸資料，以進行服務網路與行動台之間的安全通訊。

綜上所述，本發明提出一個基於群組認證金鑰的群組認證方法，同一個群組裡面的每一個行動台共享一把群組認證金鑰。當有群組內的第一個行動台率先漫遊到服務網路，並進行執行完整的雙向認證時，服務網路會向家網路取得行動台的認證資料，在完整的雙向認證過程中，服務網路會向行動台所屬的家網路取得一把暫時性群組金鑰（Group Transient Key，簡稱 GTK），接下來其他同群組的行動台就會直接使用這把群組暫時金鑰。接下來如果有同群組的行動台想在該服務網路進行認證時，可利用服務網路的資料庫裡所存放的群組暫時金鑰，與行動台直接進行區域認證，而不用再回到家網路要求認證資料。本方法不需額外的訊息交換即可達到金鑰先期投遞的效果，另外，行動台直接進行區域認證，可大幅降低認證所造成的換手延遲。

為讓本發明之上述和其他目的、特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式，作詳細說明如下。

【實施方式】

在群組通訊的原則下，住在同一社區的使用者、在同一公司上班的使用者、常搭同一路線公車的使用者，都可以被視為是一種群組，而這個群組的成員，常會在相同的地方漫遊並執行認證程序。基於這個特性，本發明提出群組認證（Group Authentication）的概念與架構，讓屬於同一群組的行動台可以共享群組認證資料，加快同一群組中的行動台在漫遊換手時的認證速度。

請參照圖 7，為本發明一實施例中所提出群組金鑰認證方法之詳細流程圖，是行動台為所屬群組中第一個進入漫遊的行動台之狀況。

此方法適用通訊系統，此通訊系統包括行動台群組 M1、服務網路 SN 與家網路 HN。其中，行動台群組 M1 有行動台 MS_{M1-1} 與 MS_{M1-2}。在此通訊系統進行資料傳輸之前，家網路 HN 會先負責分配行動台 MS_{M1-1} 與 MS_{M1-2} 屬於群組 M1。且家網路 HN 會先分配好行動台認證金鑰與群組認證金鑰給行動台 MS_{M1-1} 與 MS_{M1-2} 與家網路 HN（亦即，行動台 MS_{M1-1} 與 MS_{M1-2} 與家網路 HN 具有已知的行動台認證金鑰與群組認證金鑰），當

行動台群組 M1 內的行動台 MS_{M1-1} 與 MS_{M1-2} 加入或離開，家網路 HN 會重新設定群組認證金鑰。家網路 HN 與服務網路 SN 皆有資料庫，資料庫可以儲存群組列表（Group List）、家網路產生的群組認證資料 $AUTH_H$ 與行動台產生的群組識別資料 $AUTH_{M1}$ 等。

如下表所示，群組列表記錄群組編號、群組認證金鑰、目前群組成員的行動台身份編號（ID）、每個成員都有唯一的初始值（Initial Value）、以及其他群組相關資訊，如計費方式等。行動台 MS_{M1-1} 會記錄所屬群組 M1 的行動台群組編號 G1、行動台身分編號 MS1-1、初始值 IV1-1 與群組相關資訊，而行動台 MS_{M1-2} 會記錄所屬群組 M1 的群組編號 G1、行動台身分編號 MS1-2、初始值 IV1-2 與群組相關資訊。

群組編號	群組認證金鑰	行動台身份編號	初始值	群組相關資訊
G1	GAK1	MS1-1	IV1-1	.....
		MS1-2	IV1-2	.....
		.....	.....	.....
.....	.....	.....	.....	.....

群組認證金鑰的產生與分配可參考"Chik How Tan and Joseph Chee Ming Teo, "An Authenticated Group Key Agreement for Wireless Networks," *Wireless Communications and Networking Conference*, Vol. 4,2005, pp. 2100-2105."與"D. Wallner, F. Harder and R.

Agee, "Key Management for Multicast: Issues and Architectures," *RFC2626*, June 1999."。而群組列表中的初始值 IVi-j 值（i 表示第 i 個群組，第 j 個行動台），為一個位元數非常大，大到難以猜測且難以重覆，使得行動台在每個群組中的初始值 IVi-j 都不同。利用這個初始值 IVi-j，可以在之後的認證程序中，達到讓行動台與服務網路同步的效果。

請繼續參照圖 7，家網路 HN 與行動台 MS1 有行動台認證訊息產生函數 f^0、服務網路認證訊息產生函數 f^1、群組認證訊息產生函數 f^2、金鑰產生函數 f^3。另外，家網路 HN 更有一組認證參數 AMF。當行動台 MS_{M1-1} 為群組 MS1 第一個進入漫遊換手的行動台時，行動台 MS_{M1-1} 必須與服務網路 SN 執行完整的雙向認證。此時，本發明所提供的方法包括辨識步驟 700、家網路認證步驟 701 與行動台認證與金鑰分配步驟 702。辨識步驟 700 及家網路認證步驟 701 為前述之認證登記與分配程序，行動台認證與金鑰分配步驟 702 為前述之行動台認證與金鑰分配程序。

在本發明中，完整的雙向認證是指進行家網路認證步驟 701 與行動台認證與金鑰分配步驟 702。完整的雙向認證顧名思義就是服務網路 SN 會向行動台 MS_{M1-1} 進行認證，而且行動台 MS_{M1-1} 也會對服務網路 SN 進行認證。此外，家網路 HN 會對行動台 MS_{M1-1} 進行認證，行動台 MS_{M1-1} 也會對家網路 HN 進行認證。

當此方法應用於通訊系統時，首先，辨識步驟 700 包括子步驟 700a~700c。在子步驟 700a 中，服務網路 SN 會對欲進行認證的行動台 MS_{M1-1} 索取識別資料 $AUTH_{M1}$。而在子步驟 700b 中，行動台 MS_{M1-1} 產生識別資料 $AUTH_{M1}$ 並將識別資料 $AUTH_{M1}$ 傳給服務網路 SN，其中，此辨識資料 $AUTH_{M1}$ 有行動台 MS_{M1-1} 的行動台身分編號 MS1-1，此行動台身分編號 MS1-1 可供服務網路 SN 辨識行動台 MS_{M1-1} 的身分。

接著，在子步驟 700c 中，服務網路 SN 接收 MS1 所產生的識別資料 $AUTH_{M1}$ 並辨識此行動台 MS_{M1-1} 的身分，服務網路 SN 判斷其資料庫的群組列表是否有記錄行動台身分編號 MS1-1，因為行動台 MS_{M1-1} 為群組 M1 第一個進入服務網路 SN 進行漫遊的行動台，服務網路 SN 的資料庫內之群組列表並沒有行動台身分編號 MS1-1，因此下一個步驟會進入家網路認證步驟 701，若服務網路 SN 的資料庫具有記錄群組 M1 的群組列表，則下一個步驟有所差異，詳細內容如圖 16 的步驟 1601，稍後再說明。

家網路認證步驟 701 包括子步驟 701a~701d 等步驟。在子步驟 701a 中，服務網路 SN 會轉送識別資料 $AUTH_{M1}$ 給家網路 HN，並對家網路 HN 請求此行動台 MS_{M1-1} 所屬行動台群組的群組列表與群組認證資料 $AUTH_H$。而接著子步驟 701b 中，家網路 HN 會根據識別資料 $AUTH_{M1}$ 對行動台 MS_{M1-1} 進行認證，若認證成

功，則下一個步驟會進入子步驟 701b，若否，則中斷通訊，在圖 7 的狀況，假設家網路 HN 對行動台 MS_{M1-1} 進行認證所得到的結果為成功。而後，在子步驟 701c 中，家網路 HN 根據識別資料 $AUTH_{M1}$ 產生群組認證資料 $AUTH_H$ 並將群組認證資料 $AUTH_H$ 與所需的群組列表傳送給服務網路 SN。而子步驟 701d 則是服務網路 SN 的資料庫會儲存群組列表與群組認證資料 $AUTH_H$。

在圖 7 假設第一認證訊息碼 MAC_{M1-1} 與第二認證訊息碼 $XMAC_{M1-1}$ 比對的結果是兩者相同。因為，服務網路 SN 替行動台 MS_{M1-1} 向家網路 HN 請求群組認證資料 $AUTH_H$ 有此認證機制（利用第一認證訊息碼 MAC_{M1-1} 與第二認證訊息碼 $XMAC_{M1-1}$ 的比對），因此能確保服務網路 SN 是真實地跟家網路 HN 請求群組認證資料 $AUTH_H$，而非隨意地向家網路 HN 請求群組認證資料 $AUTH_H$。

而行動台認證與金鑰分配步驟 702 的步驟包括子步驟 702a~702h，將在底下詳細說明。首先，在子步驟 702a 中，服務網路 SN 會根據服務網路 SN 所接收到的群組認證資料 $AUTH_H$、群組列表與識別資料 $AUTH_{M1}$ 產生服務網路認證資料 $AUTH_{SM1-1}$，並將服務網路認證資料 $AUTH_{SM1-1}$ 傳送給行動台 MS_{M1-1}。其次，子步驟 702b 的行動台 MS_{M1-1} 接收服務網路認證資料 $AUTH_{SM1-1}$，並根據服務網路認證資料 $AUTH_{SM1-1}$ 對服務網路 SN 進行認證以判斷此服務網路 SN 對行動台 MS_{M1-1} 而言是

否為家網路 HN 所認定之合法提供服務的服務網路 SN，若是，則進入子步驟 702d，若否，則中斷通訊或要求重新認證。在圖 7 的狀況是預設認證的結果是服務網路 SN 對行動台 MS_{M1-1} 而言為家網路 HN 認定之合法提供服務的服務網路 SN。

接著，在子步驟 702c 中，行動台 MS_{M1-1} 對服務網路 SN 進行認證的同時，服務網路 SN 在等待行動台 MS_{M1-1} 進行認證期間可以預先計算主金鑰（Mater Key）MK，以供之後欲進行安全通訊之用。而後接著子步驟 702d，行動台 MS_{M1-1} 根據服務網路認證資料 $AUTH_{SM1-1}$ 計算主金鑰 MK 與第五認證碼訊息碼 MAC_{M1}，並將此第五認證碼訊息碼 MAC_{M1} 傳送給服務網路 SN。而後在子步驟 702e 中，服務網路 SN 接收第五認證碼訊息碼 MAC_{M1} 並根據其資料庫所記錄的群組列表之資訊與暫時性群組認證金鑰 GTK_{M1} 產生第六認證訊息碼 $XMAC_{M1}$，服務網路 SN 對第五認證訊息碼 MAC_{M1} 與第六認證訊息碼 $XMAC_{M1}$ 進行比對並產生認證結果。接著在子步驟 702f 中，服務網路 SN 回覆認證結果給行動台 MS_{M1-1}。而子步驟 702g 中，行動台 MS_{M1-1} 確認證結果，若認證結果表示認證成功，則服務網路 SN 與行動台 MS_{M1-1} 進入子步驟 702h，若認證結果表示認證失敗，則中斷通訊。圖 7 的狀況是假設認證結果顯示為認證成功，因此子步驟 702h 中，服務網路 SN 與行動台 MS_{M1-1} 使用主金鑰 MK 產生加密金鑰（Cipher Key）或

是完整性驗證金鑰（Integrity Key），對所欲傳送的資料加密以進行安全通訊。

在上述之子步驟 701b 中，家網路 HN 對行動台 MS_{M1-1} 進行認證，若認證失敗，除了上述之中斷整個通訊的方式之外，也能是重新進行認證，也就是從子步驟 700a 重新開始，或要求重新傳送識別資料 $AUTH_{M1}$。在上述之子步驟 702b 中，行動台 MS_{M1-1} 對服務網路 SN 進行認證以判斷此服務網路 SN 對行動台 MS_{M1-1} 而言是否為家網路 HN 認定之合法提供服務的服務網路 SN，若否，則除了可以中斷通訊之外，亦可以重新進行認證（也就是從子步驟 700a 重新開始）或要求重新傳送群組認證資料 $AUTH_H$ 或服務網路認證資料 $AUTH_{SM1-1}$。

在子步驟 702g 中，若認證結果表示認證失敗，除了中斷通訊之外，亦可以重新進行認證，也就是從子步驟 700a 重新開始，或要求重新傳送第五認證訊息碼 MAC_{M1}。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 700b 所提到產生識別資料 $AUTH_{M1}$ 的方法，請參照圖 8 所示之一實施例。在此實施例中，行動台 MS_{M1-1} 產生第一亂數 RN_{M1-1}，行動台將第一亂數 RN_{M1-1} 與行動台認證金鑰 K_{M1-1} 輸入行動台認證訊息產生函數 f^0 以藉此產生第一認證訊息碼 MAC_{M1-1}。行動台 MS_{M1-1} 將群組編號 G1、行動台身份代號 MS1-1、第

一亂數 RN_{M1-1} 第一認證訊息碼 MAC_{M1-1} 合併成識別資料 $AUTH_{M1}$（$AUTH_{M1}=\{G1||MS1-1||RN_{M1-1}||MAC_{M1-1}\}$）。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 701b 中，家網路 HN 會根據識別資料 $AUTH_{M1}$ 對行動台 MS_{M1-1} 進行認證的方法，請參照圖 9 所示之一實施例。如圖 9 所示，家網路 HN 擷取識別資料 $AUTH_{M1}$ 的第一亂數 RN_{M1-1} 與第一認證訊息碼 MAC_{M1-1}，並將第一亂數 RN_{M1-1} 與家網路 HN 自己所儲存的行動台認證金鑰 K_{M1-1} 輸入行動台認證訊息產生函數 f^0 以藉此產生第二認證訊息碼 $XMAC_{M1-1}$。家網路再將第一認證訊息碼 MAC_{M1-1} 與家網路自行產生的第二認證訊息碼 $XMAC_{M1-1}$ 進行比對，若第一認證訊息碼 MAC_{M1-1} 與第二認證訊息碼 $XMAC_{M1-1}$ 相同則繼續進行下一個子步驟 701c，若不同，則中斷通訊。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 701c 中產生群組認證資料 $AUTH_H$ 的方法，請參照圖 10 所示之一實施例。如圖 10 所示，家網路 HN 會先產生第二亂數 RN_H，然後家網路 HN 將第二亂數 RN_H、家網路 HN 所具有的群組認證金鑰 GAK1、一組認證參數 AMF 以及 $AUTH_{M1}$ 中的第一亂數 RN_{M1-1} 輸入金鑰產生函數 f^3 以計算出群組 M1 目前在服務網路 SN 可用來進行認證的暫時性群組認證金鑰 GTK_{M1}。等到暫時性群組認證金鑰 GTK_{M1} 計算完畢後，家網路 HN 會將產生暫時性群組認證金鑰 GTK_{M1} 所需

的第二亂數 RN_H、一組認證參數 AMF、第一亂數 RN_{M1-1}，連同計算完畢的暫時性群組認證金鑰 GTK_{M1} 一起合併在群組認證資料 $AUTH_H$ 中（$AUTH_H=\{RN_H||AMF||RN_{M1-1}||GTK_{M1}\}$），並傳送給服務網路 SN。雖然第一亂數 RN_{M1-1} 為行動台 MS_{M1-1} 所產生的亂數，但顧慮到之後的群組內的行動台 MS_{M1-1} 可能會改變暫時性群組認證金鑰 GTK_{M1} 的輸入以產生新的暫時性群組認證金鑰，故仍需將除了群組認證金鑰 GAK1 以外的必要參數 RN_H、AMF 與 RN_{M1-1} 傳給行動台 MS_{M1-1}，讓行動台 MS_{M1-1} 可以有產生暫時性群組認證金鑰 GTK_{M1} 的依據。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 702a 中產生服務網路認證資料 $AUTH_{SM1-1}$ 的方法，請參照圖 11 所示。在圖 11 中，服務網路 SN 會先將行動台 MS_{M1-1} 在服務網路 SN 的認證次數 i 與群組列表中行動台 MS_{M1-1} 的初始值 IV1-1 相加以得到第一暫時總合，之後，行動台 MS_{M1-1} 將識別資料 $AUTH_{M1}$ 中的第一亂數 RN_{M1-1} 與第一暫時總合相乘以得到第一暫時乘積。然後，行動台 MS_{M1-1} 將群組認證資料 $AUTH_H$ 中的暫時性群組認證金鑰 GTK_{M1} 與第一暫時乘積輸入服務網路認證訊息產生函數 f^1，以計算出第三認證訊息碼 MAC_S。

接著，服務網路 SN 產生第三亂數 RN_{SM1-1}，服務網路 SN 將群組認證資料 $AUTH_H$ 中的一組認證參數

AMF、第二亂數 RN_H、識別資料 $AUTH_{M1}$ 中的第一亂數 RN_{M1-1}、剛產生的第三認證訊息碼 MAC_S 與第三亂數 RN_{SM1-1} 合併成服務網路認證資料 $AUTH_{SM1-1}$（$AUTH_{SM1-1}=\{AMF||RN_H||RN_{M1-1}||MAC_S||RN_{SM1-1}\}$）。其中，一組認證參數 AMF、第二亂數 RN_H 與第一亂數 RN_{M1-1} 是要讓行動台 MS_{M1-1} 計算產生暫時性群組認證金鑰 GTK_{M1}，第三認證訊息碼 MAC_S 是用以讓行動台 MS_{M1-1} 認證服務網路 SN，第三亂數 RN_{SM1-1} 是用以讓行動台 MS_{M1-1} 計算出可供服務網路 SN 認證行動台 MS_{M1-1} 的第五認證訊息碼 MAC_{M1}。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 702b 中，行動台 MS_{M1-1} 對服務網路 SN 進行認證的方法，請參照圖 12 之一實施例。在圖 12 中，行動台 MS_{M1-1} 收到服務網路認證資料 $AUTH_{SM1-1}$ 後，會將服務網路認證資料 $AUTH_{SM1-1}$ 的一組認證參數 AMF、第二亂數 RN_H 與第一亂數 RN_{M1-1}、行動台 MS_{M1-1} 具有的群組認證金鑰 GAK1 輸入金鑰產生函數 f^3 以產生暫時性群組認證金鑰 GTK_{M1}。行動台 MS_{M1-1} 計算出了暫時性群組認證金鑰 GTK_{M1} 後，才能繼續計算之後的第四認證訊息碼 $XMAC_S$。接著，行動台 MS_{M1-1} 將行動台 MS_{M1-1} 記錄的初始值 IV1-1 與行動台 MS_{M1-1} 在服務網路 SN 的認證次數 i 相加以獲得第二暫時總合，並將第二暫時總合與第一亂數 RN_{M1-1} 相乘以獲得第二暫時乘積。行動台 MS_{M1-1} 將第二暫時乘積與計算出的暫

時性群組認證金鑰 GTK_{M1} 輸入服務網路認證訊息產生函數 f^1 以產生第四認證訊息碼 $XMAC_S$。行動台 MS_{M1-1} 將第四認證訊息碼 $XMAC_S$ 與接收到的服務網路認證資料 $AUTH_{SM1-1}$ 中的第三認證訊息碼 MAC_S 進行比對。若第四認證訊息碼 $XMAC_S$ 與第三認證訊息碼 MAC_S 相同，則代表行動台 MS_{M1-1} 成功地認證了服務 SN，同時也認證了家網路 HN，因為行動台 MS_{M1-1} 必須產生正確的暫時性群組認證金鑰 GTK_{M1}，才能通過接下來的認證。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 702c 中計算主金鑰 MK 的方法，請參照圖 13 之一實施例。如圖 13 所示，當行動台 MS_{M1-1} 在驗證服務網路 SN 的服務網路認證資料 $AUTH_{SM1-1}$ 時，服務網路 SN 也利用時間先計算主金鑰 MK，等稍後行動台 MS_{M1-1} 傳回讓服務網路 SN 認證行動台 MS_{M1-1} 的認證訊息碼，且服務網路 SN 也成功認證行動台 MS_{M1-1} 時，即可以省去計算主金鑰 MK 的時間。服務網路 SN 將第一亂數 RN_{M1-1}、第三亂數 RN_{SM1-1} 與暫時性群組認證金鑰 GTK_{M1} 輸入金鑰產生函數 f^3 以計算出主金鑰 MK。

上述之子步驟 702c 也可以在行動台 MS_{M1-1} 傳回讓服務網路 SN 認證行動台 MS_{M1-1} 的第五認證碼訊息碼 MAC_{M1}，且服務網路 SN 也成功認證行動台 MS_{M1-1} 之後才進行，但上述之實施例的方法可以省下一段服務網

路計算主金鑰 MK 的時間。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 702d 中計算主金鑰 MK 與產生第五認證碼訊息碼 MAC_{M1} 的方法，請參照圖 14 之一實施例。當行動台 MS_{M1-1} 成功認證服務網路 SN 為家網路 HN 所認定之合法提供服務的服務網路 SN 後，行動台 MS_{M1-1} 接著要產生讓服務網路 SN 可以認證行動台 MS_{M1-1} 的第五認證訊息碼 MAC_{M1}。行動台 MS_{M1-1} 先將只有服務網路 SN 與行動台 MS_{M1-1} 彼此才會知道的初始值 IV1-1 與認證次數 i 相加以獲得第三暫時總合，並將第三暫時總合與自服務網路認證資料 $AUTH_{SM1-1}$ 中取出第三亂數 RN_{SM1-1} 相乘以獲得第三暫時乘積。

然後，行動台 MS_{M1-1} 將之前計算出之暫時性群組認證金鑰 GTK_{M1} 與第三暫時乘積輸入群組認證訊息產生函數 f^2 以計算出第五認證碼訊息碼 MAC_{M1} 供服務網路 SN 認證行動台 MS_{M1-1}。另外，行動台 MS_{M1-1} 也將由行動台 MS_{M1-1} 與服務網路 SN 各自產生的第一亂數 RN_{M1-1}、第三亂數 RN_{SM1-1} 與暫時性群組認證金鑰 GTK_{M1} 輸入金鑰產生函數 f^3 來計算出接下來行動台 MS_{M1-1} 與服務網路 SN 進行安全通訊所需的主金鑰 MK。

圖 7 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 702e 中產生認證結果的方法，請參照圖 15 所示。在圖 15 中，服務網路 SN 先將行動台

MS_{M1-1} 對服務網路 SN 認證次數的 i 與初始值 IV1-1 相加以獲得第四暫時總合，並將第四暫時總合與第三亂數 RN_{SM1-1} 相乘以獲得第四暫時乘積。之後，服務網路 SN 將第四暫時乘積與暫時性群組認證金鑰 GTK_{M1} 輸入群組認證訊息產生函數 f^2 以計算出第六認證碼訊息碼 $XMAC_{M1}$。最後服務網路 SN 對第六認證碼訊息碼 $XMAC_{M1}$ 與第五認證碼訊息碼 MAC_{M1} 進行比對以獲得認證結果。

上述之行動台 MS_{M1-1} 對服務網路 SN 與家網路 HN 進行認證、服務網路 SN 對行動台 MS_{M1-1} 進行認證與家網路 HN 對行動台 MS_{M1-1} 進行認證的方法僅是本發明之一種實施方法，非用以限定本發明。凡屬於本發明之精神經熟知本領域之技藝者做潤飾或部分修改者，應當在本發明之保護範圍內。

請參照圖 16，為本發明另一實施例中所提出一種群組金鑰認證方法之流程示意圖。行動台 MS_{M1-2} 為所屬群組 M1 非第一個進入漫遊的行動台之狀況。因行動台 MS_{M1-2} 不是群組 MS1 第一個進入漫遊換手的行動台，因此，行動台 MS_{M1-2} 可以直接自服務網路 SN 的資料庫得到暫時性群組認證金鑰 GTK_{M1}。因此，行動台 MS_{M1-2} 在獲得可產生暫時性群組認證金鑰 GTK_{M1} 的參數並計算出暫時性群組認證金鑰 GTK_{M1} 後，可以直接向服務網路 SN 進行認證，而服務網路 SN 也可以直接向行動台 MS_{M1-2} 進行認證，進而減少家網路 HN 與服

務網路 SN 之間的交通流量以避免頻寬的浪費。

另外，行動台 MS_{M1-2} 亦可以強制要求服務網路 SN 進行如同圖 7 的服務網路 SN 所進行之完整的雙向認證（也就是說，服務網路 SN 可以根據行動台 MS_{M1-2} 所傳送的訊息判斷是否進行完整的雙向認證，將認證訊息轉送回家網路 HN，並要求新鮮的群組認證資料 $AUTH_H$）。圖 16 的流程包括辨識步驟 1600、取得暫時性群組認證金鑰步驟 1601 與行動台認證與金鑰分配步驟 1602。其中，辨識步驟 1600 及取得暫時性群組認證金鑰步驟 1601 為前述之認證登記與分配程序，行動台認證與金鑰分配步驟 1602 為前述之行動台認證與金鑰分配程序。在本發明中，區域認證是指進行取得暫時性群組認證金鑰步驟 1601 與行動台認證與金鑰分配步驟 1602。區域認證顧名思義就是服務網路 SN 會僅向行動台 MS_{M1-2} 進行認證，而沒有向家網路 HN 要求認證行動台 MS_{M1-2}。

首先，辨識步驟 1600 的流程包括子步驟 1600a~1600c。在子步驟 1600a 中，服務網路 SN 會對欲進行認證的行動台 MS_{M1-2} 索取識別資料。接著，在子步驟 1600b 中，行動台 MS_{M1-2} 產生識別資料 $AUTH_{M1}$ 並將識別資料 $AUTH_{M1}$ 傳給服務網路 SN，其中，此識別資料 $AUTH_{M1}$ 有行動台 MS_{M1-2} 的行動台身分編號 MS1-2，此行動台身分編號 MS1-2 可供服務網路 SN 辨識行動台 MS_{M1-2} 的身分。而後，在子步驟 1600c 中，

服務網路 SN 接收 MS_{M1-2} 所產生的識別資料 $AUTH_{M1}$ 並辨識此行動台 MS_{M1-2} 的身分，服務網路 SN 判斷其資料庫的群組列表是否有記錄行動台身分編號 MS1-2。

因為行動台 MS_{M1-2} 不是群組 M1 第一個進入服務網路 SN 進行漫遊的行動台，服務網路 SN 的資料庫內之群組列表會有行動台身分編號 MS1-2，因此下一個步驟會進入取得暫時性群組認證金鑰步驟 1601。另外，行動台 MS_{M1-2} 亦可以要求服務網路 SN 進行如同圖 7 的服務網路 SN 進行完整的雙向認證，例如在識別資料 $AUTH_{M1}$ 補上旗標（Flag）以指示服務網路 SN 在其資料庫內之群組列表會有行動台身分編號 MS1-2 時是否進行完整的雙向認證，在此假設行動台 MS_{M1-2} 沒有要求服務網路 SN 進行如同圖 7 的完整的雙向認證。

而上述取得暫時性群組認證金鑰步驟 1601 的流程如下：服務網路 SN 從自己的資料庫取得行動台 MS_{M1-2} 所屬群組的群組認證資料 $AUTH_H$，其中，群組認證資料 $AUTH_H$ 包括暫時性群組認證金鑰 GTK_{M1}（$AUTH_H=\{RN_H||AMF||RN_{M1-1}||GTK_{M1}\}$）。緊接著繼續進行行動台認證與金鑰分配步驟 1602。

行動台認證與金鑰分配步驟 1602 包括例如子步驟 1602a～1602h。在子步驟 1602a 中，服務網路 SN 會根據服務網路 SN 從其資料庫所找到的資料產生服務網路認證資料 $AUTH_{SM1-2}$，並將服務網路認證資料 $AUTH_{SM1-2}$ 傳送給行動台 MS_{M1-2}。而後，在子步驟 1602b

中，行動台 MS_{M1-2} 接收服務網路認證資料 $AUTH_{SM1-2}$，並根據服務網路認證資料 $AUTH_{SM1-2}$ 對服務網路 SN 進行認證以判斷此服務網路 SN 對行動台 MS_{M1-2} 而言是否為家網路 HN 認定之合法提供服務的服務網路 SN，若是，則進入子步驟 1602d，若否，則中斷通訊。在圖 16 的狀況是預設認證的結果是服務網路 SN 對行動台 MS_{M1-2} 而言為合法提供服務的服務網路 SN。

接著，在子步驟 1602c 中，行動台 MS_{M1-2} 在對服務網路 SN 進行認證的同時，服務網路 SN 可以預先計算主金鑰 MK，以供之後欲進行安全通訊之用。而後，在子步驟 1602d 中，行動台 MS_{M1-2} 根據服務網路認證資料 $AUTH_{SM1-2}$ 計算主金鑰 MK 與第五認證碼訊息碼 MAC_{M1}，並將此第五認證碼訊息碼 MAC_{M1} 傳送給服務網路 SN。在子步驟 1602e 中，服務網路 SN 接收第五認證碼訊息碼 MAC_{M1} 並根據其資料庫所記錄的群組列表之資訊與暫時性群組認證金鑰 GTK_{M1} 產生第六認證訊息碼 $XMAC_{M1}$，服務網路 SN 對第五認證訊息碼 MAC_{M1} 與第六認證訊息碼 $XMAC_{M1}$ 進行比對並產生認證結果。

而在子步驟 1602f 中，服務網路 SN 回覆認證結果給行動台 MS_{M1-2}。在子步驟 1602g 中，行動台 MS_{M1-2} 確認證結果，若認證結果表示認證成功，則服務網路 SN 與行動台 MS_{M1-2} 進入子步驟 1602h，若認證結果表示認證失敗，則中斷通訊，圖 16 的狀況是假設認證結

果顯示為認證成功。而在子步驟 1602h 中，服務網路 SN 與行動台 MS_{M1-2} 使用主金鑰 MK 來保護傳送的資料。

在上述之子步驟 1602b 中，行動台 MS_{M1-2} 對服務網路 SN 進行認證，以判斷此服務網路 SN 對行動台 MS_{M1-2} 而言，是否為家網路 HN 所認定之合法提供服務的服務網路 SN。若不是家網路 HN 所認定之合法提供服務的服務網路 SN，則除了可以中斷通訊之外，亦可以重新進行認證（從子步驟 1600a 重新開始）或要求重新傳送服務網路認證資料 $AUTH_{SM1-1}$。在子步驟 1602g 中，若認證結果表示認證失敗，除了中斷通訊之外，亦可以重新進行認證（從子步驟 1600a 重新開始）或要求重新傳送第五認證訊息碼 MAC_{M1}。

圖 16 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 1600b 產生識別資料 $AUTH_{M1}$ 方法之一實施例，請參照圖 17 所示。在此實施例中，行動台 MS_{M1-2} 產生第一亂數 RN_{M1-2}，行動台將第一亂數 RN_{M1-2} 與行動台認證金鑰 K_{M1-2} 輸入行動台認證訊息產生函數 f^0，以藉此產生第一認證訊息碼 MAC_{M1-2}。行動台 MS_{M1-2} 將群組編號 G1、行動台身份代號 MS1-2、第一亂數 RN_{M1-2} 第一認證訊息碼 MAC_{M1-2} 合併成識別資料 $AUTH_{M1}$（$AUTH_{M1}=\{G1||MS1\text{-}2||RN_{M1-2}||MAC_{M1-2}\}$）。

圖 16 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 1602a 中產生服務網路認證資料

$AUTH_{SM1-2}$ 方法之一實施例，請參照圖 18 所示。在此實施例中，服務網路 SN 會先將行動台 MS_{M1-2} 在服務網路 SN 的認證次數 i 與群組列表中行動台 MS_{M1-2} 的初始值 IV1-2 相加以得到第一暫時總合，之後，服務網路 SN 將行動台識別資料 $AUTH_{M1}$ 中的第一亂數 RN_{M1-2} 與第一暫時總合相乘以得到第一暫時乘積。然後，服務網路 SN 從資料庫中取出暫時性群組認證金鑰 GTK_{M1} 與第一暫時乘積輸入服務網路認證訊息產生函數 f^1，以計算出第三認證訊息碼 MAC_S。接著，服務網路 SN 產生第三亂數 RN_{SM1-2}，服務網路 SN 將從資料庫中找到的認證資料之一組認證參數 AMF、第二亂數 RN_H、識別資料 $AUTH_{M1}$ 中的第一亂數 RN_{M1-2}、剛產生的第三認證訊息碼 MAC_S 與第三亂數 RN_{SM1-2} 合併成服務網路認證資料 $AUTH_{SM1-2}$（$AUTH_{SM1-2}=\{AMF||RN_H||RN_{M1-2}||MAC_S||RN_{SM1-2}\}$）。其中，一組認證參數 AMF、第二亂數 RN_H 與第一亂數 RN_{M1-2} 是要讓行動台 MS_{M1-2} 計算產生暫時性群組認證金鑰 GTK_{M1}，第三認證訊息碼 MAC_S 是用以讓行動台 MS_{M1-2} 認證服務網路，第三亂數 RN_{SM1-2} 是用以讓行動台 MS_{M1-2} 計算出可供服務網路 SN 認證行動台 MS_{M1-2} 的認證訊息碼。

圖 16 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 1602b 中行動台 MS_{M1-2} 對服務網路 SN 進行認證方法之一實施例，請參照圖 18 所示。在此

實施例中，行動台 MS_{M1-2} 收到服務網路認證資料 $AUTH_{SM1-2}$ 後，會將服務網路認證資料 $AUTH_{SM1-2}$ 的一組認證參數 AMF、第二亂數 RN_H 與第一亂數 RN_{M1-2}、行動台 MS_{M1-2} 具有的群組認證金鑰 GAK1 輸入金鑰產生函數 f^3 以產生暫時性群組認證金鑰 GTK_{M1}。行動台 MS_{M1-2} 計算出了暫時性群組認證金鑰 GTK_{M1} 後，才能繼續計算之後的第四認證訊息碼 $XMAC_S$。

接著，行動台 MS_{M1-2} 將行動台 MS_{M1-2} 記錄的初始值 IV1-2 與行動台 MS_{M1-2} 在服務網路的認證次數 i 相加以獲得第二暫時總合，並將第二暫時總合與第一亂數 RN_{M1-2} 相乘以獲得第二暫時乘積。行動台 MS_{M1-2} 將第二暫時乘積與計算出的暫時性群組認證金鑰 GTK_{M1} 輸入服務網路認證訊息產生函數 f^1 以產生第四認證訊息碼 $XMAC_S$。行動台 MS_{M1-2} 將第四認證訊息碼 $XMAC_S$ 與接收到的服務網路認證資料 $AUTH_{SM1-2}$ 中的第三認證訊息碼 MAC_S 進行比對。若第四認證訊息碼 $XMAC_S$ 與第三認證訊息碼 MAC_S 相同，則代表行動台 MS_{M1-2} 成功地認證了服務 SN，同時也認證了家網路 HN，因為行動台 MS_{M1-2} 必須產生正確的暫時性群組認證金鑰 GTK_{M1}，才能通過接下來的認證。

圖 16 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 1602c 中計算主金鑰 MK 方法之一實施例，請參照圖 20 所示。在此實施例中，當行動台 MS_{M1-2} 在驗證服務網路 SN 的服務網路認證資料

$AUTH_{SM1-2}$時，服務網路 SN 也利用時間先計算主金鑰 MK，等稍後行動台 MS_{M1-2}傳回讓服務網路 SN 認證行動台 MS_{M1-2}的認證訊息碼，且服務網路 SN 也成功認證行動台 MS_{M1-2}時，即可以省去計算主金鑰 MK 的時間。服務網路 SN 將第一亂數 RN_{M1-2}、第三亂數 RN_{SM1-1}與暫時性群組認證金鑰 GTK_{M1}輸入金鑰產生函數 f^3 以計算出主金鑰 MK。

上述之子步驟 1602c 也可以在行動台 MS_{M1-2}傳回讓服務網路 SN 認證行動台 MS_{M1-2}的第五認證碼訊息碼 MAC_{M1}，且服務網路 SN 也成功認證行動台 MS_{M1-2}之後才進行，但上述之實施例的方法可以省下一段服務網路計算主金鑰 MK 的時間。

圖 16 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟 1602d 中計算主金鑰 MK 與產生第五認證碼訊息碼 MAC_{M1} 方法之一實施例，請參照圖 21 所示。在此實施例中，當行動台 MS_{M1-2} 成功認證服務 SN 為合法提供服務的服務網路 SN 後，行動台 MS_{M1-2} 接著要產生讓服務網路 SN 可以認證行動台 MS_{M1-2} 的第五認證訊息碼 MAC_{M1}。行動台 MS_{M1-2} 先將只有服務網路 SN 與行動台 MS_{M1-2} 彼此才會知道的初始值 IV1-2 與認證次數 i 相加以獲得第三暫時總合，並將第三暫時總合與自服務網路認證資料 $AUTH_{SM1-2}$ 中取出服務網路 SN 產生的第三亂數 RN_{SM1-2} 相乘以獲得第三暫時乘積。

然後，行動台 MS_{M1-2} 將之前計算出之暫時性群組認證金鑰 GTK_{M1} 與第三暫時乘積輸入群組認證訊息產生函數 f^2 以計算出第五認證碼訊息碼 MAC_{M1} 供服務網路 SN 認證行動台 MS_{M1-2}。另外，行動台 MS_{M1-2} 也將由行動台 MS_{M1-2} 與服務網路 SN 各自產生的第一亂數 RN_{M1-2}、第三亂數 RN_{SM1-2} 與暫時性群組認證金鑰 GTK_{M1} 輸入金鑰產生函數 f^3 來計算出接下來行動台 MS_{M1-2} 與服務網路 SN 進行安全通訊所需的主金鑰 MK。

圖 16 所述本發明實施例的群組金鑰認證方法的方法中，關於子步驟中 1602e 中產生認證結果方法之一實施例，請參照圖 22 所示。在此實施例中，服務網路 SN 先將行動台 MS_{M1-2} 對服務網路 SN 認證次數的 i 與初始值 IV1-2 相加以獲得第四暫時總合，並將第四暫時總合與第三亂數 RN_{SM1-2} 相乘以獲得第四暫時乘積。之後，服務網路 SN 將第四暫時乘積與暫時性群組認證金鑰 GTK_{M1} 輸入群組認證訊息產生函數 f^2 以計算出第六認證碼訊息碼 $XMAC_{M1}$。最後服務網路 SN 對第六認證碼訊息碼 $XMAC_{M1}$ 與第五認證碼訊息碼 MAC_{M1} 進行比對以獲得認證結果。

上述之行動台 MS_{M1-2} 對服務網路 SN 與家網路 HN 進行認證、服務網路 SN 對行動台 MS_{M1-2} 進行認證的方法僅是本發明之一種實施方法，非用以限定本發明。凡屬於本發明之精神經熟知本領域之技藝者做潤飾或部

分修改者，應當在本發明之保護範圍內。

圖 7 與圖 16 的行動台 MS_{M1-1} 與 MS_{M1-2} 是屬於群組 M1，然而上述之的例子僅是為了方便說明，實際上行動台 MS_{M1-1} 與 MS_{M1-2} 也可以同時屬於其他群組（亦即行動台 MS_{M1-1} 與 MS_{M1-2} 可以同時屬於至少一個以上的群組。）

本發明所提出群組認證機制可以應用在蜂巢式電信網路（Cellular Network）的認證機制。當群組中的第一個行動台在漫遊區的服務網路通過認證過後，漫遊區的服務網路之認證伺服器會有可認證群組的群組認證資料。稍後要認證的行動台沒有直接與註冊的家網路（Home Network, Home AAA Server, H-AAA）之認證伺服器直接認證，而是透過行動台漫遊當地的服務網路之認證伺服器（Visited AAA Server, V-AAA）執行認證程序。在不失安全性的情況下，使用本發明所提供之方法可以減少 H-AAA 與 V-AAA 之間的群組認證資料的傳送。

本發明所提出群組認證機制亦可以應用於 802.11 網路的認證機制。請參照圖 23，圖 23 是本發明之群組認證方法應用於 802.11 網路。群組 MN 包括多個行動台 MN_1~MN_n 在同一個 802.11 網路的存取點（Access Point，AP） AP_1 底下漫遊換手，存取點 AP_1 負責認證 MN_1~MN_n。當存取點 AP_1 為 MN_1 做認證時，存取點 AP_1 會向家網路的認證伺服器 AAA server 索取群組認證資

料與群組列表時，AAA server 會將可認證多個 MN_1~MN_n 的群組認證資料與群組列表傳回給 AP_1。當 AP_1 認證完 MN_1 後，可直接用先前認證 MN_1 時索取的群組認證資料認證 MN_2。

本發明所提出群組認證機制亦可以應用於一般手持式遊戲裝置。一般手持式遊戲裝置的遊戲對戰多是利用功率較小的無線電波交換訊息，對戰的機台容易受限於環境與距離，若是在外想透過無線上網對戰，又可能因換手延遲，無法達成即時通訊的要求。將原本點對點（end-to-end）影音傳輸的兩個遊戲裝置視為同一個群組的兩個行動台，當兩個手持式遊戲裝置一起漫遊時，由其中一個先執行完整的雙向認證後，另一個就可以直接和漫遊區的網路做區域性認證，讓即時資料的傳輸不因漫遊認證程序而受到影響。

本發明所提出群組認證機制亦可以應用於門禁管理系統。公司為了安全起見，公司門禁管理系統裡的公司員工的認證資料經過一次認證之後立即要丟棄，不能重複使用。透過本發明所提供之認證方法，將同部門或公司內所有的同事視為是一個群組，再虛擬一個首位認證成員，可事先將所有的認證資料由使用者資料庫傳至門禁系統負責刷卡認證的機器上，省去員工刷卡時，認證訊息來回門禁系統與使用者資料庫的時間。

參照圖 24，圖 24 是本發明之群組認證之方法應用於行動路由器（Mobile Router，簡稱 MR）的示意圖。

在公車上 BUS1~BUS4 設置行動路由器，讓搭乘公車 BUS1~BUS4 的人可以透過行動路由器上網。將同一條路線的公車上BUS1~BUS4所設置的行動路由器視為同一個群組，它們具有時常漫遊到相同的服務網路 SN、隨著同路線公車 BUS1~BUS4 行走相同路徑、屬於相同家網路 HN 的特性。設定路線重疊的多個行動路由器擁有共同的一把群組認證金鑰，則此行動路由器的群組在固定的路線上漫遊時，可利用共享群組認證資料，減少在漫遊路徑上認證時的延遲，加快換手速度，進而可以在公車上提供通訊品質較好網路即時服務（Real-Time Services），例如網路電話（VoIP）。

上述之群組認證之方法亦可以應用於 TETRA（Terrestrial Trunked Radio）網路的群組通訊。在 TETRA 網路上的行動台（無線電或者是車機）具有群體特性（分別是群組通訊與群體移動）。也就是說，一堆行動台通常會因為某些目的會在某個時間點同時通訊或者是一起移動。針對這個特點，TETRA 網路提供行動台群組安全機制，使得行動台群組進行群組通訊時，可以很輕易透過此安全機制保護資料的傳送。當然，由於 TETRA 網路本身已經具有群體的特性了，在不需要修改架構下，立即可以使用本發明所提供之群組認證方法，加入行動台群組在漫遊時的換手速度。

綜上所述，在本發明所提出的群組認證機制，讓漫遊的群組可以利用家網路認證資料共享的優點，一方面

透過首位認證的行動台為其他行動台達到群組金鑰先期投遞的效果，讓後繼認證的行動台不用多餘的訊息來回於服務網路與家網路之間，即可先行進行區域認證；另一方面藉由服務網路持有暫時性群組認證金鑰，在暫時性群組認證金鑰的有效期限內，能簡化所有行動台的認證與再認證程序。

和以往缺乏群體概念的網路比較起來，本發明所提出的認證方法更適合應用在即時影音通訊或是欲提供群組通訊的系統上。若將群組的概念加以擴充，將兩個正在進行點對點影音通訊的行動台視為同一個群組的兩個行動台，當兩個行動台一起漫遊時，由其中一個先執行完整的雙向完整認證後，另一個就可以直接和漫遊區的服務網路做區域性認證，讓即時資料的傳輸不因漫遊認證程序而受到影響。

雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

圖 1 為 UMTS AKA 的認證方法流程圖。

圖 2 是 UMTS AKA 方法中認證向量 AV(i)的產生方法示意圖。

圖 3 是行動台 MS1 根據認證向量 AV(i)的部份資訊

Rand(i)與AUTN(i)對家網路HN進行認證與產生行動台認證資料RES(i)的示意圖。

圖4是採用UMTS XAKA認證方法時行動台MS1第一次漫遊換手時的認證流程圖。

圖5是採用UMTS XAKA認證方法時行動台MS1經第一次漫遊換手後的認證流程圖。

圖6是美國公告核准專利第6711400號專利所提供的認證方法流程圖。

圖7為本發明所提供的群組金鑰認證方法的一種狀況之方法流程圖。

圖8是上述步驟700b產生識別資料$AUTH_{M1}$中MAC_{M1-1}的方法示意圖。

圖9為子步驟701b中家網路HN會根據識別資料$AUTH_{M1}$對行動台MS_{M1-1}進行認證的方法示意圖。

圖10為子步驟701c中家網路HN產生群組認證資料$AUTH_H$的方法示意圖。

圖11是子步驟702a中產生服務網路認證資料$AUTH_{SM1-1}$的方法示意圖。

圖12是子步驟702b中行動台MS_{M1-1}對服務網路SN進行認證的方法示意圖。

圖13是子步驟702c中計算主金鑰MK的方法示意圖。

圖14是子步驟702d中計算主金鑰MK與產生第五認證碼訊息碼MAC_{M1}的方法示意圖。

圖 15 是子步驟中 702e 中產生認證結果的方法示意圖。

圖 16 為本發明所提供的群組金鑰認證方法的另一種狀況之方法流程圖。

圖 17 是上述步驟 1600b 產生識別資料 $AUTH_{M1}$ 的方法示意圖。

圖 18 是子步驟 1602a 中產生服務網路認證資料 $AUTH_{SM1-2}$ 的方法示意圖。

圖 19 是子步驟 1602b 中行動台 MS_{M1-2} 對服務網路 SN 進行認證的方法示意圖。

圖 20 是子步驟 1602c 中計算主金鑰 MK 的方法示意圖。

圖 21 是子步驟 1602d 中計算主金鑰 MK 與產生第五認證碼訊息碼 MAC_{M1} 的方法示意圖。

圖 22 是子步驟中 1602e 中產生認證結果的方法示意圖。

圖 23 是本發明之群組認證方法應用於 802.11 網路。

圖 24 是本發明之群組認證之方法應用於行動路由器（mobile router）的示意圖。

【主要元件符號說明】

MS1、MS_{M1-1}、MS_{M1-2}、MN_1~MN_n：行動台

HN：家網路

SN：服務網路

M1、MN ：群組

100、101、102：步驟流程

400、401、402：步驟流程

500、501：步驟流程

600、601、602：步驟流程

700、701、702：步驟流程

1600、1601、1602：步驟流程

AAA server：認證伺服器

BUS1~BUS4：公車

AP_1：存取點

十、申請專利範圍：

1.一種群組認證的方法，該方法適用於一通訊系統，該通訊系統包括一第一群組、一服務網路與一家網路，其中，該第一群組包括至少一行動台，該服務網路具有一第一資料庫，該第一資料庫用以記錄自該家網路傳送之一群組列表與一群組認證資料，該通訊系統預先分配一群組認證金鑰與一行動台認證金鑰給該行動台與該家網路，該家網路並產生該群組列表，該家網路具有一第二資料庫，該第二資料庫用以記錄該家網路所產生的該群組列表，該方法包括：

該服務網路對該行動台進行一辨識動作；以及

該服務網路根據該服務網路對該行動台進行該辨識動作的結果判斷該通訊系統要進行一完整的雙向認證動作或一區域認證動作，

其中，該區域認證動作包括取得暫時性認證金鑰步驟，包括該服務網路從該第一資料庫取得該群組認證資料，其中，群組認證資料包括暫時性群組認證金鑰；以及行動台認證與金鑰分配步驟。

2.如申請專利範圍第1項所述之方法，其中，該群組列表包括一群組編號、該群組認證金鑰、一行動台身分編號、一初始值與一群組相關訊息，且該行動台具有該群組編號、該行動台身分編號與該初始值。

3.如申請專利範圍第2項所述之方法，該辨識動作包括以下步驟：

該服務網路向該行動台請求一識別資料；

該行動台產生一第一亂數，該行動台根據該行動台認證金鑰與該第一亂數與產生該識別資料；以及

該行動台傳送該識別資料給該服務網路。

4.如申請專利範圍第 3 項所述之方法，其中，該行動台具有一行動台認證訊息產生函數，該識別資料產生的方法包括：

該行動台將該第一亂數與該行動台認證金鑰輸入該行動台認證訊息產生函數以計算出一第一認證訊息碼；以及

該行動台將該群組編號、該行動台身分編號、該第一亂數與該第一認證訊息碼合併以產生該識別資料。

5.如申請專利範圍第 4 項所述之方法，其中，該服務網路判斷該通訊系統要進行該完整的雙向認證或該區域認證動作的判斷方式為根據該行動台是否要求該通訊系統進行該完整的雙向認證動作，

若是，則進行該完整的雙向認證動作，

若否，則判斷該行動台所傳送之該識別資料中的該行動台身分編號是否在記錄於該第一資料內的該群組列表，

若否，則進行該完整的雙向認證動作，

若是，則進行該區域認證動作。

6.如申請專利範圍第 5 項所述之方法，該完整的雙向認證動作包括以下步驟：

101. 4. 02
年 月 日修正替換頁

家網路認證步驟；以及

行動台認證與金鑰分配步驟。

7.如申請專利範圍第 6 項所述之方法，其中，該家網路認證步驟包括：

該服務網路轉送該辨識資料給該家網路，並對家網路請求該行動台所屬的該群組列表與該群組認證資料；

該家網路根據該辨識資料對該行動台進行認證；

若該家網路成功地認證該行動台，則該家網路產生該群組認證資料，並將該群組認證資料與所該行動台所屬的該群組列表傳送給該服務網路；

該第一資料庫儲存該群組認證資料與該行動台所屬的該群組列表。

8.如申請專利範圍第 7 項所述之方法，其中，該家網路亦具有該行動台認證訊息產生函數，該家網路根據該辨識資料對該行動台進行認證的方法包括：

該家網路擷取該辨識資料的該第一亂數與該第一認證訊息碼，並將該第一亂數與該行動台認證金鑰輸入該行動台認證訊息產生函數以藉此產生一第二認證訊息碼；以及

該家網路對該第一認證訊息碼與該第二認證訊息進行比對，若該第一認證訊息碼與該第二認證訊息兩者相同，則該家網路成功地認證該行動台。

9.如申請專利範圍第 8 項所述之方法，其中，該家網路具有一金鑰產生函數與一組認證參數，該群組認證

101 年 4 月 02 日修正替換頁
101-4-2

資料產生的方法包括：

該家網路產生一第二亂數，該家網路將該第一亂數、該第二亂數、該群組認證金鑰與該組認證參數輸入該金鑰產生函數以計算出一暫時性群組認證金鑰；以及

該家網路將該第二亂數、該組認證參數、該第一亂數與暫時性群組認證金鑰合併以產生該群組認證資料。

10.如申請專利範圍第 9 項所述之方法，其中，該行動台認證與金鑰分配步驟包括：

該服務網路根據該群組認證資料、該群組列表與該識別資料產生一服務網路認證資料，並將該服務網路認證資料傳送給該行動台；

該行動台接收該服務網路認證資料，並根據該服務網路認證資料對該服務網路進行認證以判斷該服務網路對該行動台而言是否為合法提供服務的該服務網路；

若該服務網路對該行動台而言為合法提供服務的該服務網路，則該服務網路計算一主金鑰；

該行動台根據該服務網路認證資料計算該主金鑰與一第五認證碼訊息碼，並將該第五認證碼訊息碼傳送給該服務網路；

該服務網路接收該第五認證碼訊息碼，並根據該第一資料庫所記錄的該群組列表之資訊與該暫時性群組認證金鑰產生一第六認證訊息碼，該服務網路對該第五認證訊息碼與該第六認證訊息碼進行比對並產生一認證結果；

該服務網路回覆該認證結果給行動台；以及

該行動台確認該認證結果，若該認證結果表示認證成功，則該服務網路與該行動台使用該主金鑰對所欲傳送的資料加密以進行安全通訊。

11.如申請專利範圍第 10 項所述之方法，其中，該服務網路具有一服務網路認證訊息產生函數，該服務網路認證資料的產生方法包括：

該服務網路將該行動台在該服務網路的認證次數與該初始值相加以得到一第一暫時總合；

該行動台將該第一亂數與該第一暫時總合相乘以得到一第一暫時乘積；

該行動台將該暫時性群組認證金鑰與該第一暫時乘積輸入該服務網路認證訊息產生函數以計算出一第三認證訊息碼；以及

該服務網路產生一第三亂數，該服務網路將該組認證參數、該第二亂數、該第一亂數、該第三認證訊息碼與該第三亂數合併成該服務網路認證資料。

12.如申請專利範圍第 11 項所述之方法，其中，該行動台具有該服務網路認證訊息產生函數與該金鑰產生函數，該行動台根據該服務網路認證資料對該服務網路進行認證的方法包括：

該行動台接收該服務網路認證資料並擷取該服務網路認證資料中的該組認證參數、該第二亂數與該第一亂數，該行動台將擷取到的該組認證參數、該第二亂數

101. 4. 02
年 月 日修正替換頁
101-4-2

與該第一亂數、該群組認證金鑰輸入該金鑰產生函數以產生該暫時性群組認證金鑰；

該行動台將該初始值與該行動台在該服務網路的認證次數相加以獲得一第二暫時總合；

該行動台將該第二暫時總合與該第一亂數相乘以獲得一第二暫時乘積；

該行動台將該第二暫時乘積與該暫時性群組認證金鑰輸入該服務網路認證訊息產生函數以產生一第四認證訊息碼；以及

該行動台將該第四認證訊息碼與接收到的該服務網路認證資料中的該第三認證訊息碼進行比對。

13.如申請專利範圍第 12 項所述之方法，其中，該服務網具有該金鑰產生函數，該服務網路計算該主金鑰的方法包括：

該服務網路將該第一亂數、該第三亂數與該暫時性群組認證金鑰輸入該金鑰產生函數以計算出該主金鑰。

14.如申請專利範圍第 13 項所述之方法，其中，該行動台具有一群組認證訊息產生函數，該行動台產生該第五認證訊息碼的方法包括：

若該行動台成功認證該服務網路為合法提供服務的服務網路，則該行動台將該初始值與該認證次數相加以獲得一第三暫時總合，並將該第三暫時總合與該第三亂數相乘以獲得一第三暫時乘積；以及

該行動台將該暫時性群組認證金鑰與該第三暫時

101. 4. 02
年 月 日修正替換頁
101-4-2

乘積輸入該群組認證訊息產生函數以計算出該第五認證碼訊息碼。

15.如申請專利範圍第 14 項所述之方法，其中，該行動台產生該主金鑰的方法包括：

該行動台將該第一亂數、該第三亂數與該暫時性群組認證金鑰輸入該金鑰產生函數以產生該主金鑰。

16.如申請專利範圍第 15 項所述之方法，其中，該服務網路具有該群組認證訊息產生函數，該第六認證訊息碼的產生方法包括：

該服務網路將該認證次數與該初始值相加以獲得一第四暫時總合，並將該第四暫時總合與該第三亂數相乘以獲得一第四暫時乘積；以及

該服務網路將該第四暫時乘積與該暫時性群組認證金鑰輸入該群組認證訊息產生函數以計算出該第六認證碼訊息碼。

17.如申請專利範圍第 1 項所述之方法，該通訊系統更包括一第二群組、該行動台可同時屬於該第一群組與該第二群組。

18.一種群組認證方法，適用於一家網路、一服務網路與一使用者群組彼此進行認證，該使用者群組有一行動台，該行動台與該家網路有一群組認證金鑰與一行動台認證金鑰，該家網路有一群組列表，該行動台有一行動台身分編號、一群組編號與一初始值，該服務網路具有一資料庫，該資料庫可以記錄自該家網路傳送的該

群組列表，此方法包括：

產生一辨識資料於該行動台，其中，該辨識資料包括一第一認證訊息碼與該行動台身分編號；

傳送該辨識資料至該服務網路；

檢查該行動台編號是否紀錄於該資料庫內的該群組列表，若否：

傳送該辨識資料至該家網路；

根據該識別資料產生一第二認證訊息碼於該家網路；

比較該第一認證訊息碼與該第二認證訊息碼；

若該第一認證訊息碼與該第二認證訊息碼相同，則該家網路成功地認證該行動台；

利用該群組認證金鑰產生一暫時性群組認證金鑰於該家網路；

傳送一群組認證資料與該群組列表給該服務網路，其中，該群組認證資料包括該暫時性群組認證金鑰；以及

紀錄該群組列表與該群組認證資料於該服務網路的該資料庫；

若是：

根據該行動台身分編號從該服務網路的該資料庫獲得該群組認證資料；

利用該群組認證資料產生一第三認證訊息碼於該服務網路；

101年 4月 02日修正替換頁
101-4-2

傳送一服務網路認證資料至該行動台，該服務網路認證資料包括該第三認證訊息碼；

利用該服務網路認證資料產生該暫時性群組認證金鑰於該行動台與利用該暫時性群組認證金鑰產生一第四認證訊息碼於該行動台；

比較該第三認證訊息碼與該第四認證訊息碼於該行動台，若該第三認證訊息碼與該第四認證訊息碼相同，則該行動台成功地認證該服務網路與該家網路；

利用該群組認證資料計算出一主金鑰於該服務網路；

利用該服務網路認證資料與該暫時性群組認證金鑰產生該主金鑰與一第五認證訊息碼於該行動台；

傳送該第五認證訊息碼至該服務網路；

利用該群組認證資料產生一第六認證訊息碼於該服務網路；

比較該第五認證訊息碼與該第六認證訊息碼於該服務網路，若該第五認證訊息碼與該第六認證訊息碼相同，則該服務網路成功地認證該行動台；以及

利用主金鑰加密該服務網路與該行動台欲進行傳輸之一傳輸資料，以進行該服務網路與該行動台之間的安全通訊。

19.如申請專利範圍第 18 項所述之方法，其中，該群組列表包括該群組編號、該群組認證金鑰、該行動台身分編號、該初始值與一群組相關訊息。

101. 4. 02
年 月 日修正替換頁
101-4-2

20. 如申請專利範圍第 18 項所述之方法，其中，該識別資料更包括一旗標，當在檢查該行動台編號是否紀錄於該資料庫內的該群組列表時，該旗標可以使得檢查該行動台編號是否紀錄於該資料庫內的該群組列表的結果為否。

21.如申請專利範圍第 18 項所述之方法，該第一認證訊息碼產生的方法包括：

產生一第一亂數於該行動台；以及

利用該第一亂數與該行動台認證金鑰計算出該第一認證訊息碼。

22.如申請專利範圍第 18 項所述之方法，其中，該識別資料更包括該第一亂數、群組編號。

23.如申請專利範圍第 18 項所述之方法，根據該識別資料產生一第二認證訊息碼於該家網路的方法包括：

利用該識別資料中的該第一亂數與該家網路具有的該行動台認證金鑰計算出該第二認證訊息碼。

24.如申請專利範圍第 18 項所述之方法，其中，該家網路具有一組認證參數，利用該群組認證金鑰產生該暫時性群組認證金鑰於該家網路的方法包括：

產生一第二亂數於該家網路；

利用該組認證參數、該第二亂數與該第一亂數計算出該暫時性認證金鑰。

25.如申請專利範圍第 24 項所述之方法，該群組認證資料更包括該組認證參數、該第一與該第二亂數。

26.如申請專利範圍第 25 項所述之方法，其中，利用該群組認證資料產生該第三認證訊息碼於該服務網路的方法包括：

利用該群組列表中的該初始值、該行動台對該服務網路進行認證的次數、該第一亂數與該暫時性群組認證金鑰計算出該第三認證訊息碼。

27.如申請專利範圍第 25 項所述之方法，其中，該服務網路產生一第三亂數，該服務網路認證資料更包括該第一與該第二亂數、該組認證參數與該第三亂數。

28.如申請專利範圍第 27 項所述之方法，其中，利用該服務網路認證資料產生該暫時性群組認證金鑰於該行動台與利用該暫時性群組認證金鑰產生該第四認證訊息碼於該行動台的方法包括：

利用該組認證參數、該第一亂數與該第二亂數計算出該暫時性群組認證金鑰；以及

利用該暫時性群組認證金鑰、該初始值與該行動台對該服務網路進行認證的次數計算出該第四認證訊息碼。

29.如申請專利範圍第 27 項所述之方法，其中，利用該群組認證資料計算出該主金鑰於該服務網路的方法包括：

利用該暫時性群組認證金鑰、該第一與該第三亂數計算出該主金鑰。

30.如申請專利範圍第 28 項所述之方法，其中，利

101 年 4 月 02 日修正替換頁
101-4-2

用該服務網路認證資料與該暫時性群組認證金鑰產生該主金鑰與該第五認證訊息碼於該行動台的方法包括：

利用該第三亂數、該初始值、該行動台對該服務網路進行認證的次數與該暫時性群組認證金鑰產生該第五認證訊息碼；以及

利用該暫時性群組認證金鑰、該第一與該第三亂數計算出該主金鑰。

31.如申請專利範圍第 27 項所述之方法，其中，利用該群組認證資料產生該第六認證訊息碼於該服務網路的方法包括：

利用利用該第三亂數、該初始值、該行動台對該服務網路進行認證的次數與該暫時性群組認證金鑰產生該第六認證訊息碼。

32.如申請專利範圍第 18 項所述之方法，該通訊系統更包括一第二群組、該行動台可同時屬於該第一群組與該第二群組。

十一、圖式：

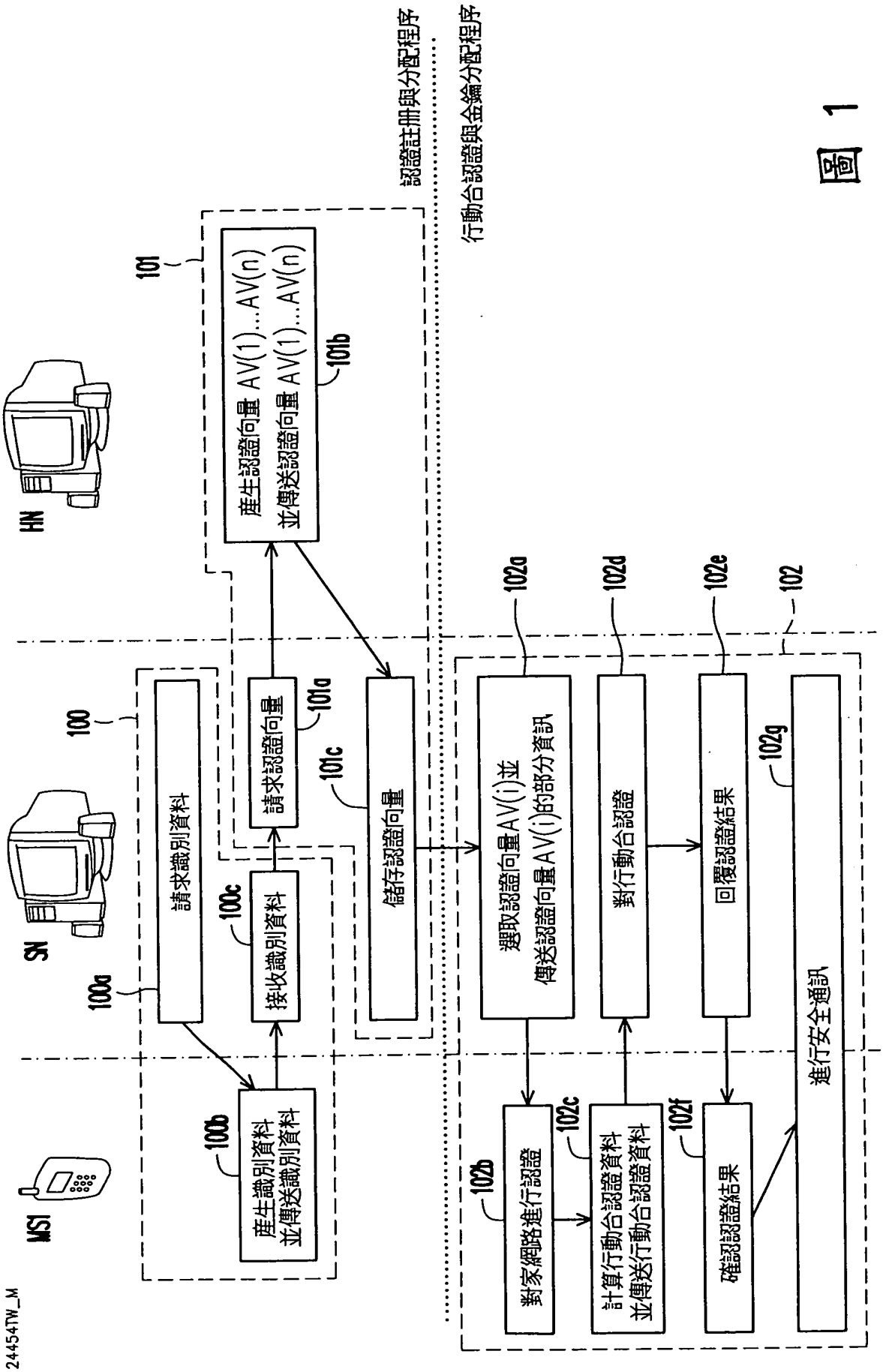
認證註冊與分配程序
行動台認證與金鑰分配程序
101
產生認證向量 AV(1)...AV(n)
並傳送認證向量 AV(1)...AV(n)
101b
HN
100
請求識別資料
100a
請求認證向量
101a
101c
接收識別資料
100c
SN
儲存認證向量
102a
102d
102e
102
選取認證向量AV(i)並
傳送認證向量AV(i)的部分資訊
對行動台認證
回覆認證結果
102g
進行安全通訊
產生識別資料
並傳送識別資料
100b
MS1
對家網路進行認證
102b
102c
計算行動台認證資料
並傳送行動台認證資料
102f
確認認證結果
24454TW_M

圖 1

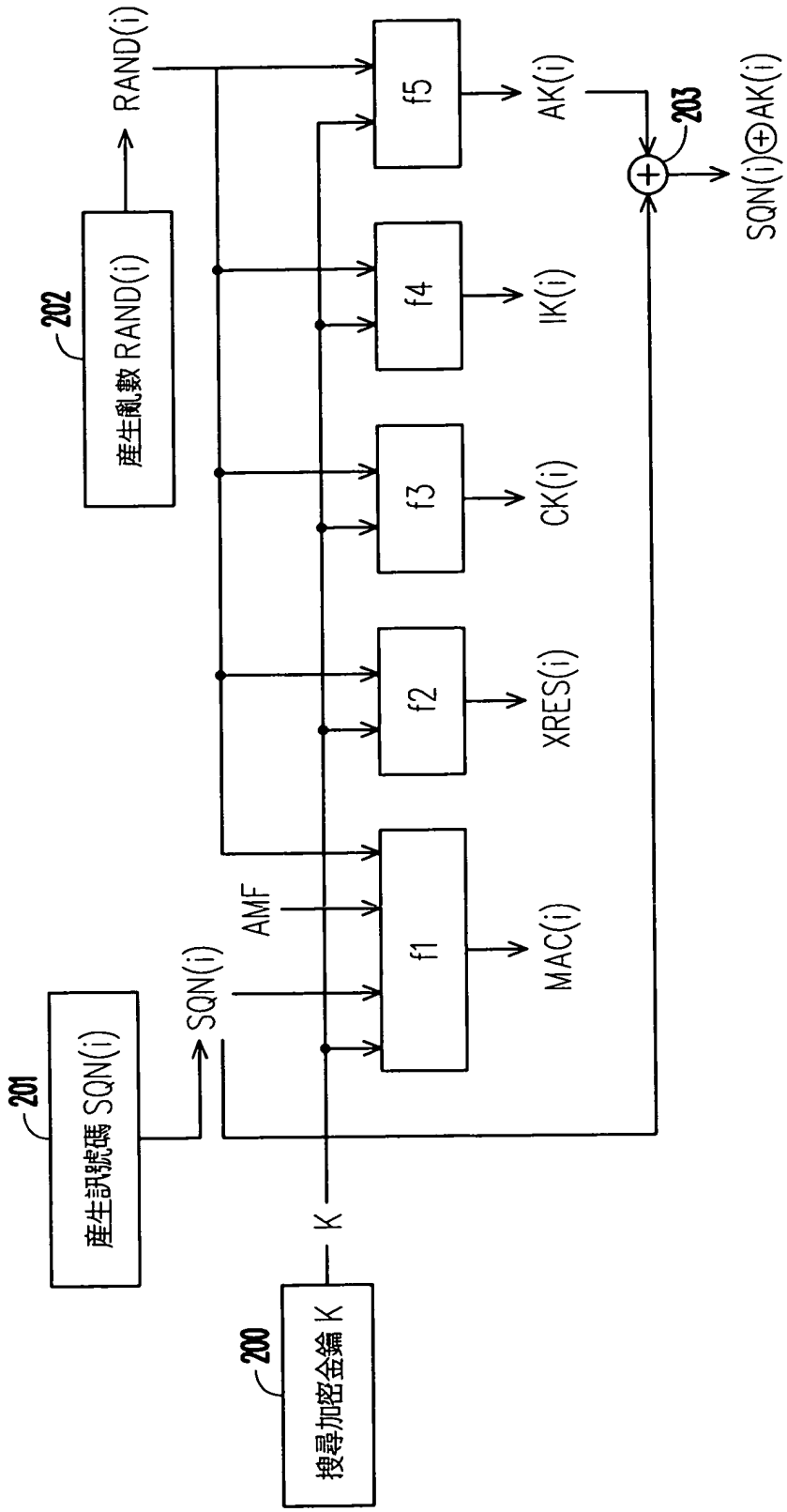
200
搜尋加密金鑰 K
201
產生訊號碼 SQN(i)
202
產生亂數 RAND(i)
203
RAND(i)
SQN(i)
AMF
K
f1
f2
f3
f4
f5
MAC(i)
XRES(i)
CK(i)
IK(i)
AK(i)
SQN(i)⊕AK(i)

圖 2

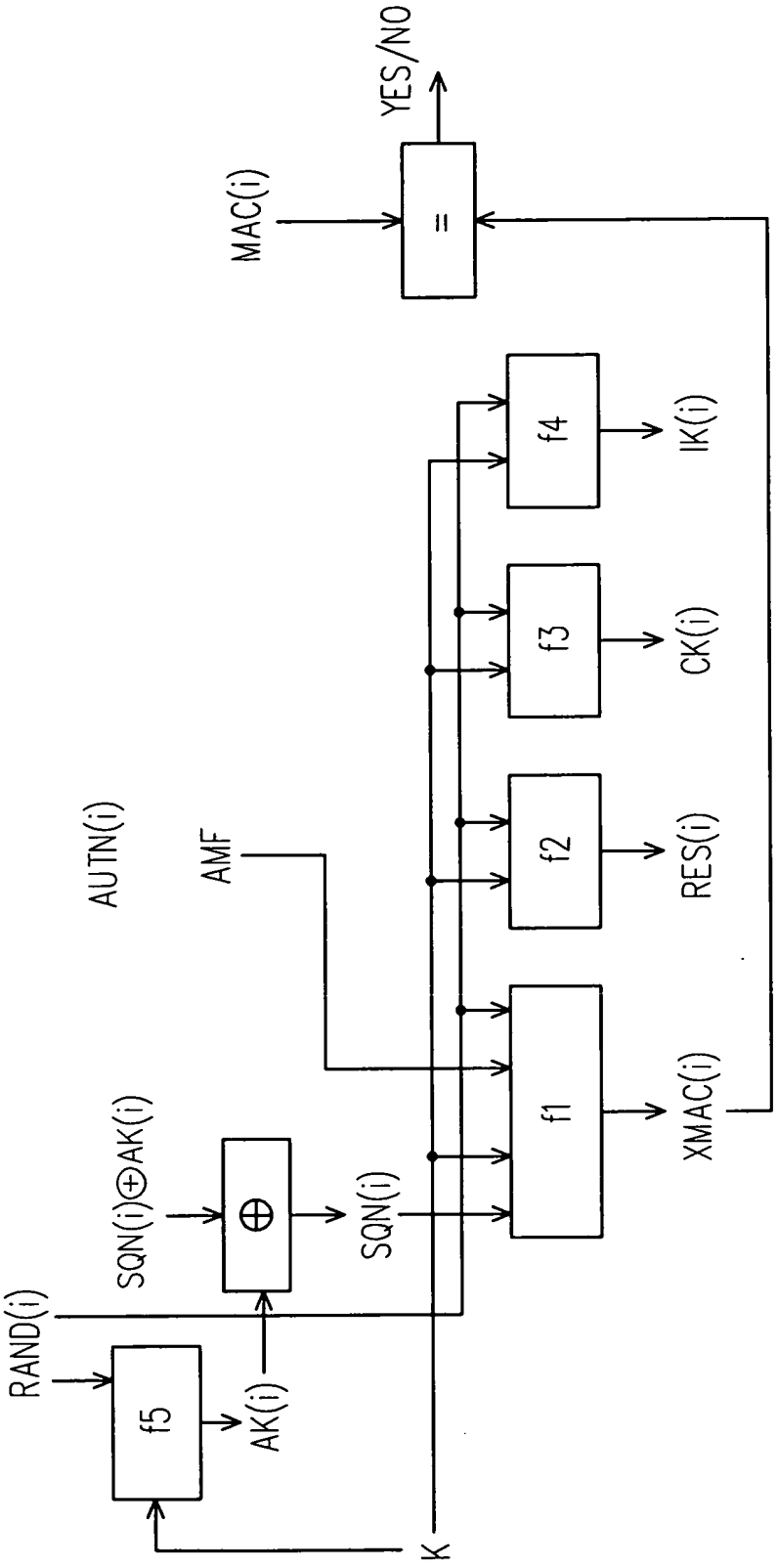
YES/NO
MAC(i)
=
f4
IK(i)
f3
CK(i)
f2
RES(i)
f1
XMAC(i)
AUTN(i)
AMF
SQN(i)⊕AK(i)
⊕
SQN(i)
RAND(i)
f5
AK(i)
K

圖 3

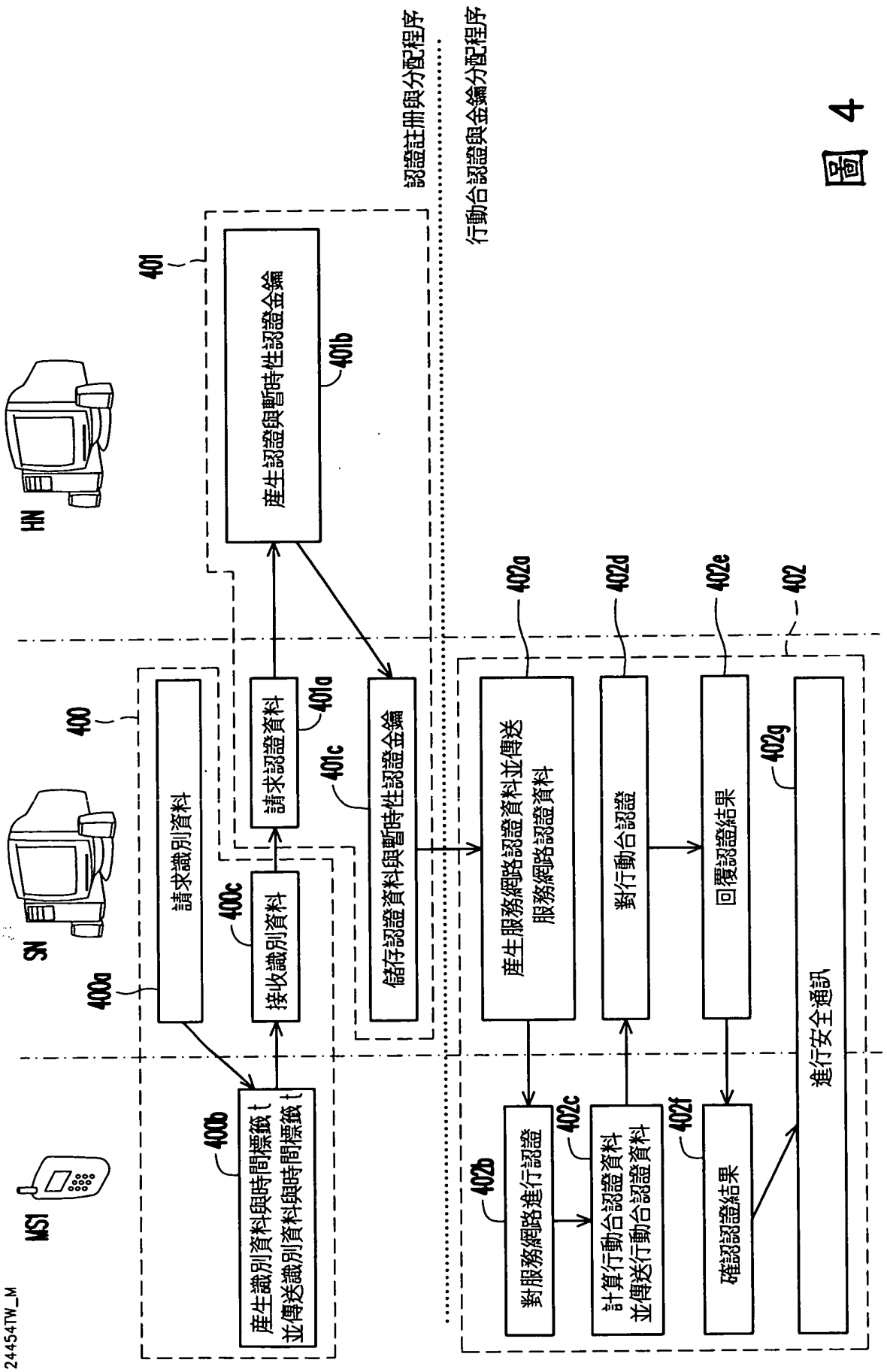
認證註冊與分配程序
行動台認證與金鑰分配程序
401
產生認證與暫時性認證金鑰
401b
HN
400
請求識別資料
400a
請求認證資料
401a
401c
接收識別資料
400c
儲存認證資料與暫時性認證金鑰
SN
產生識別資料與時間標籤t
並傳送識別資料與時間標籤t
400b
MS1
402
402a
產生服務網路認證資料並傳送
服務網路認證資料
402d
對行動台認證
402e
回覆認證結果
402g
進行安全通訊
對服務網路進行認證
402b
402c
計算行動台認證資料
並傳送行動台認證資料
402f
確認認證結果
24454TW_M

圖 4

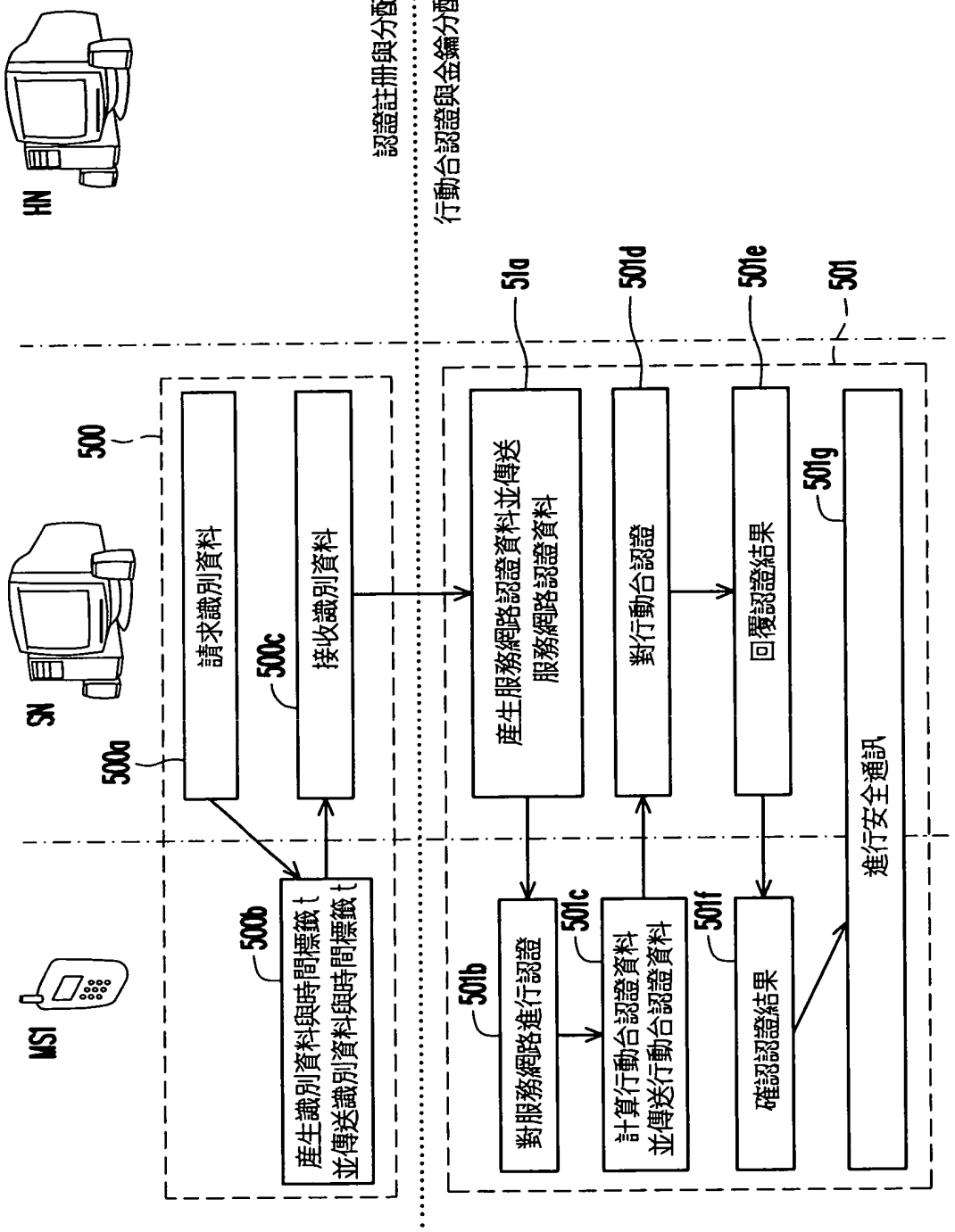
HN
認證註冊與分配程序
行動台認證與金鑰分配程序
SN
MS1
500
500a
500b
500c
請求識別資料
產生識別資料與時間標籤t
並傳送識別資料與時間標籤t
接收識別資料
51a
501d
501e
501
501b
501c
501f
501g
產生服務網路認證資料並傳送
服務網路認證資料
對服務網路進行認證
對行動台認證
回覆認證結果
計算行動台認證資料
並傳送行動台認證資料
確認認證結果
進行安全通訊

圖 5

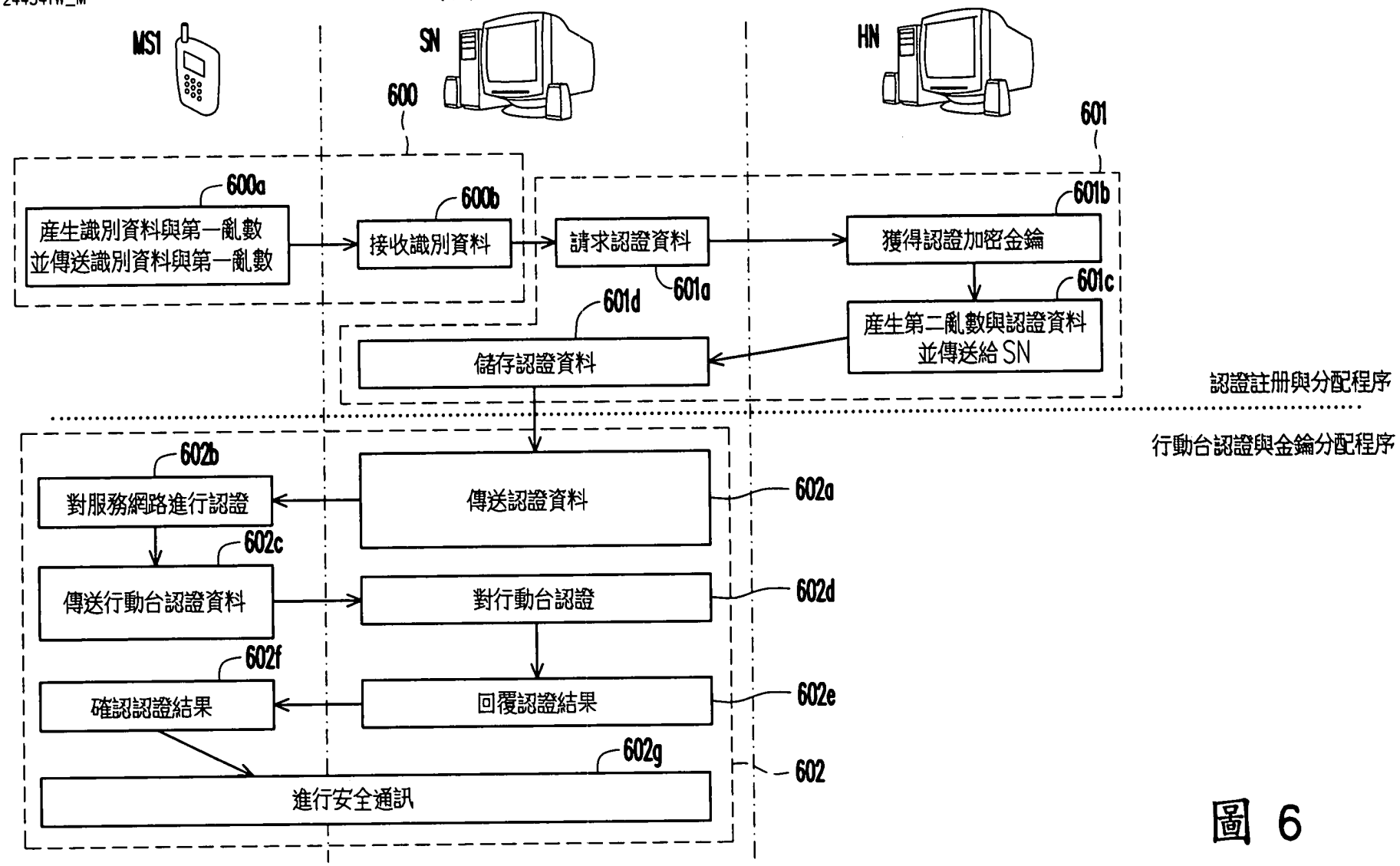
MS1
SN
HN
600
601
600a
產生識別資料與第一亂數
並傳送識別資料與第一亂數
600b
接收識別資料
請求認證資料
601a
601b
獲得認證加密金鑰
601c
產生第二亂數與認證資料
並傳送給 SN
601d
儲存認證資料
認證註冊與分配程序
行動台認證與金鑰分配程序
602b
對服務網路進行認證
傳送認證資料
602a
602c
傳送行動台認證資料
對行動台認證
602d
602f
確認認證結果
回覆認證結果
602e
602g
進行安全通訊
602

圖 6

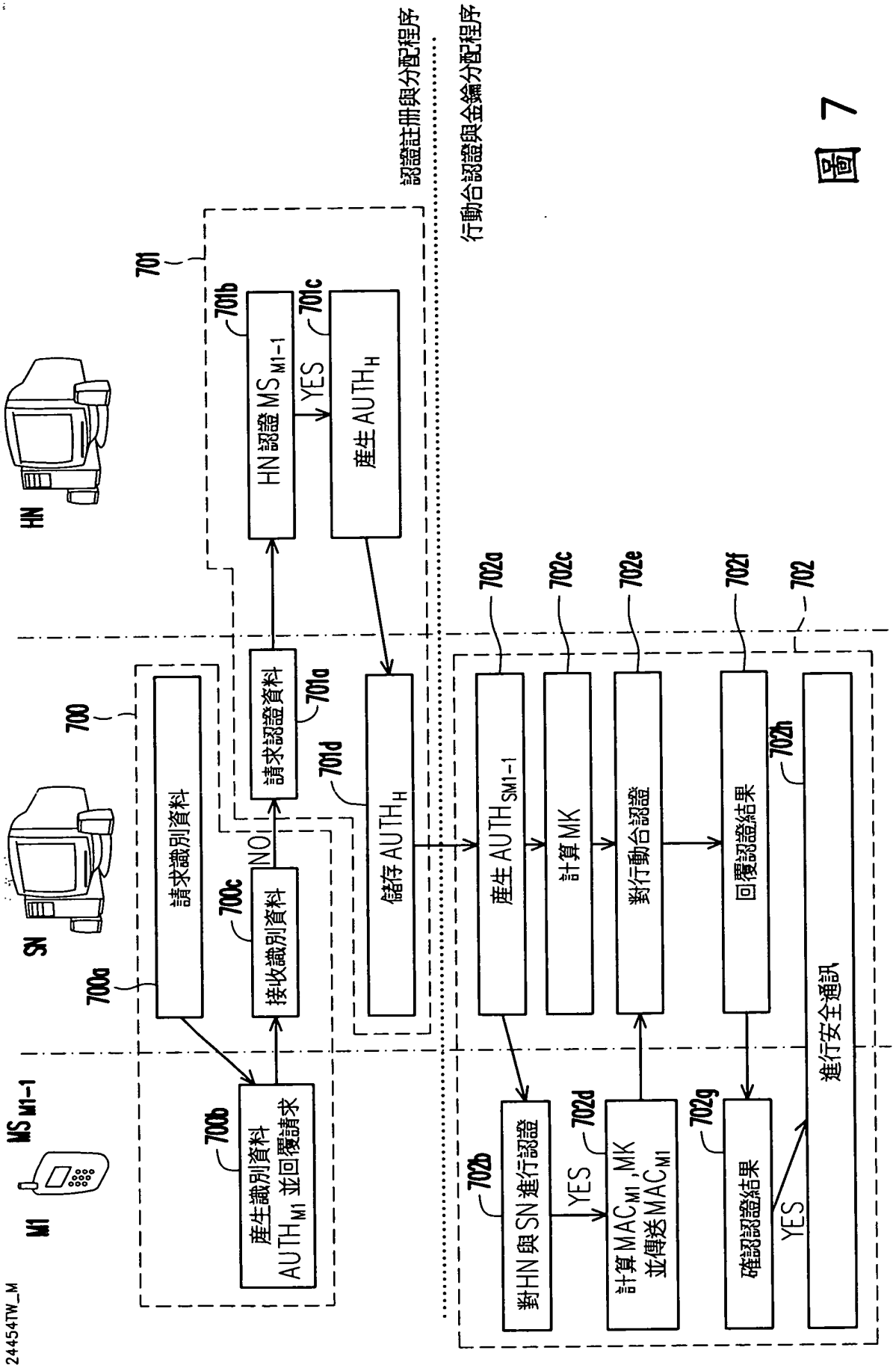
認證註冊與分配程序
行動台認證與金鑰分配程序
HN
SN
MS M1-1
M1
700
700a
700b
700c
701
701a
701b
701c
701d
702
702a
702b
702c
702d
702e
702f
702g
702h
請求識別資料
產生識別資料
AUTH M1 並回覆請求
接收識別資料
NO
請求認證資料
HN 認證 MS M1-1
YES
產生 AUTH H
儲存 AUTH H
產生 AUTH SM1-1
計算 MK
對行動台認證
回覆認證結果
進行安全通訊
對HN與SN進行認證
YES
計算 MAC M1 ,MK
並傳送 MAC M1
確認認證結果
YES
24454TW_M

圖 7

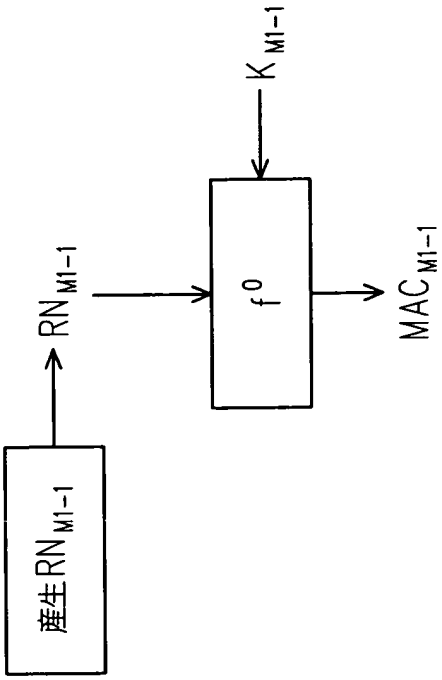

圖 8

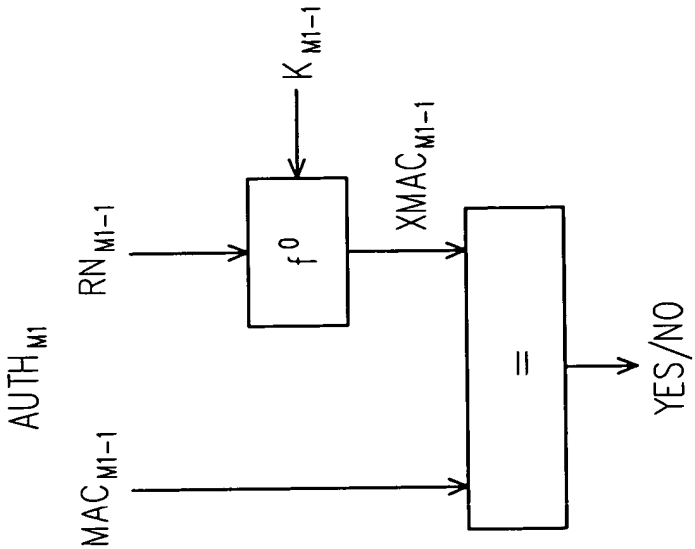

圖 9

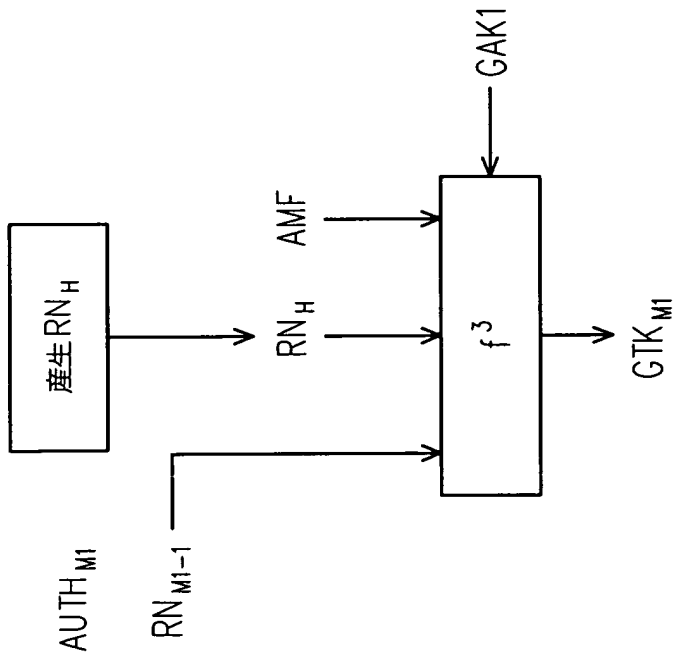

圖 10

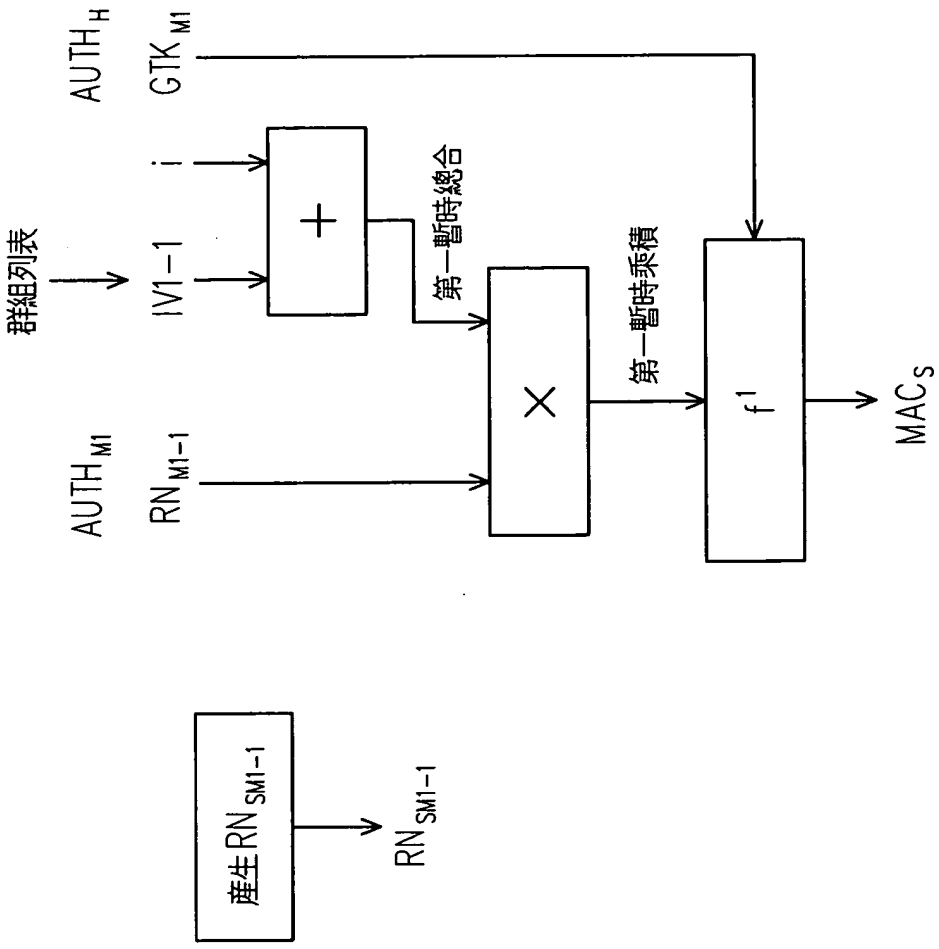
群組列表
AUTH_H
GTK_M1
IV1-1
i
+
第一暫時總合
AUTH_M1
RN_M1-1
×
第一暫時乘積
f^1
MAC_S
產生RN_SM1-1
RN_SM1-1

圖 11

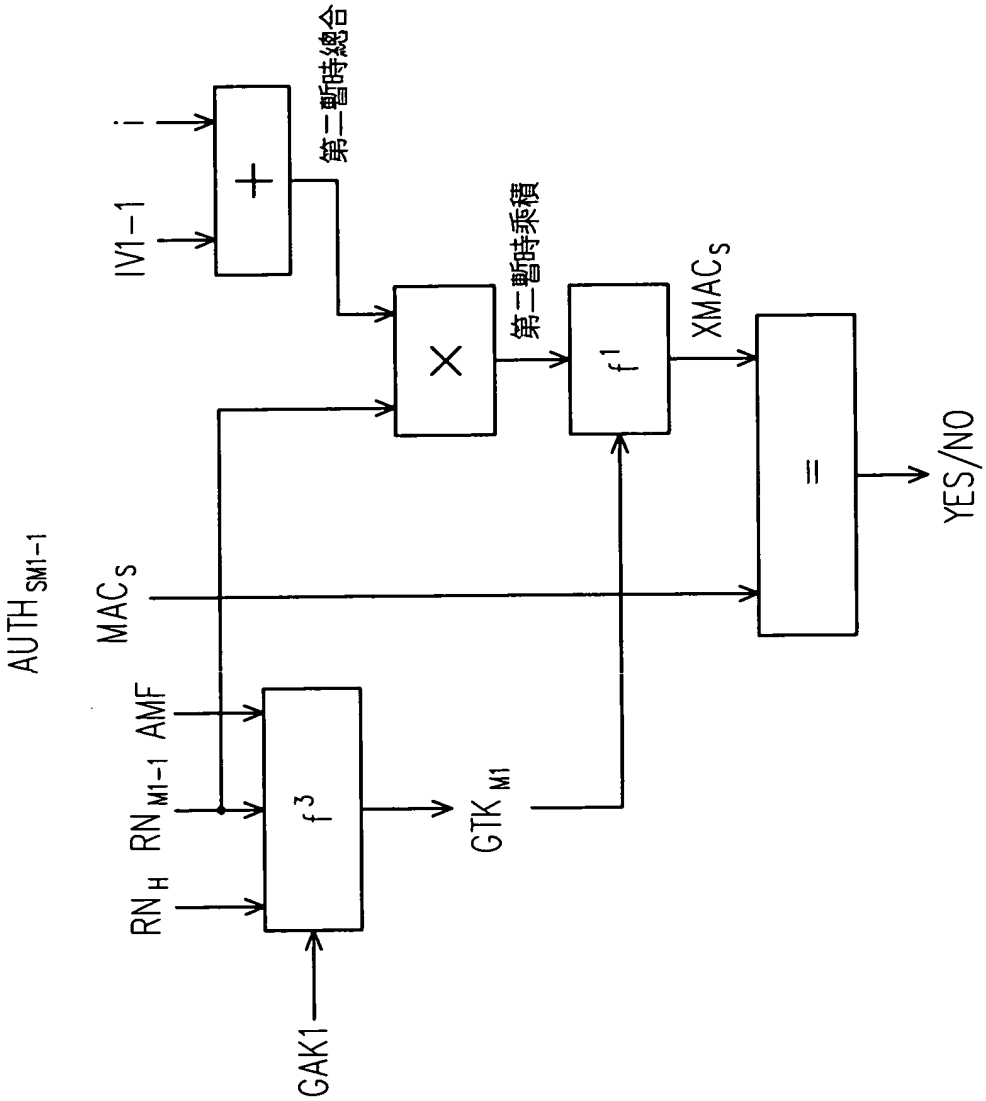
AUTH SM1-1
MAC S
RN M1-1 AMF
RN H
GAK1
f 3
GTK M1
IV1-1
i
+
第二暫時總合
×
第二暫時乘積
f 1
XMAC S
=
YES/NO

圖 12

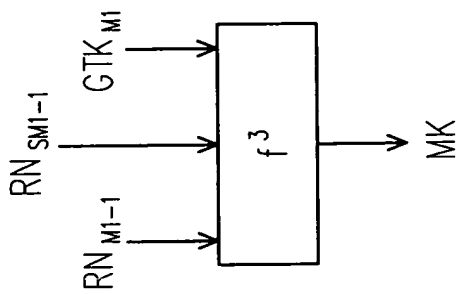

圖 13

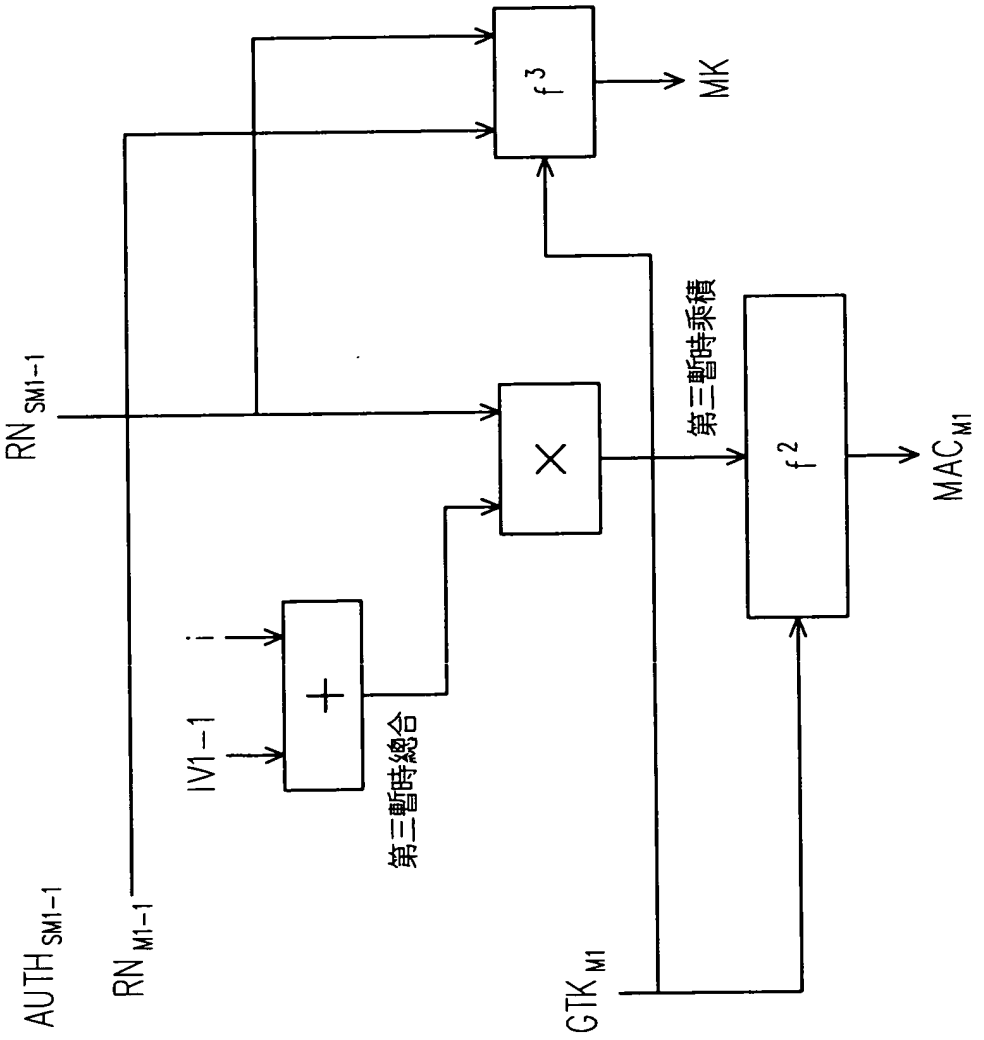
RN SM1-1
AUTH SM1-1
RN M1-1
IV1-1
i
第三暫時總合
第三暫時乘積
GTK M1
f3
MK
f2
MAC M1

圖14

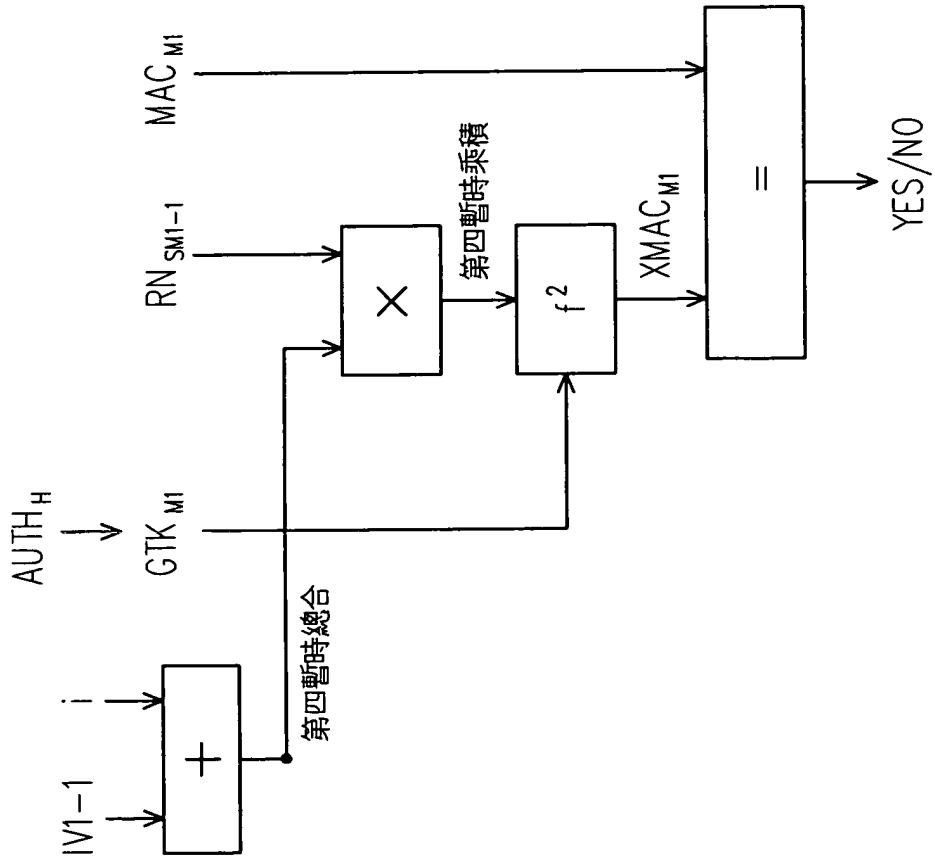

圖 15

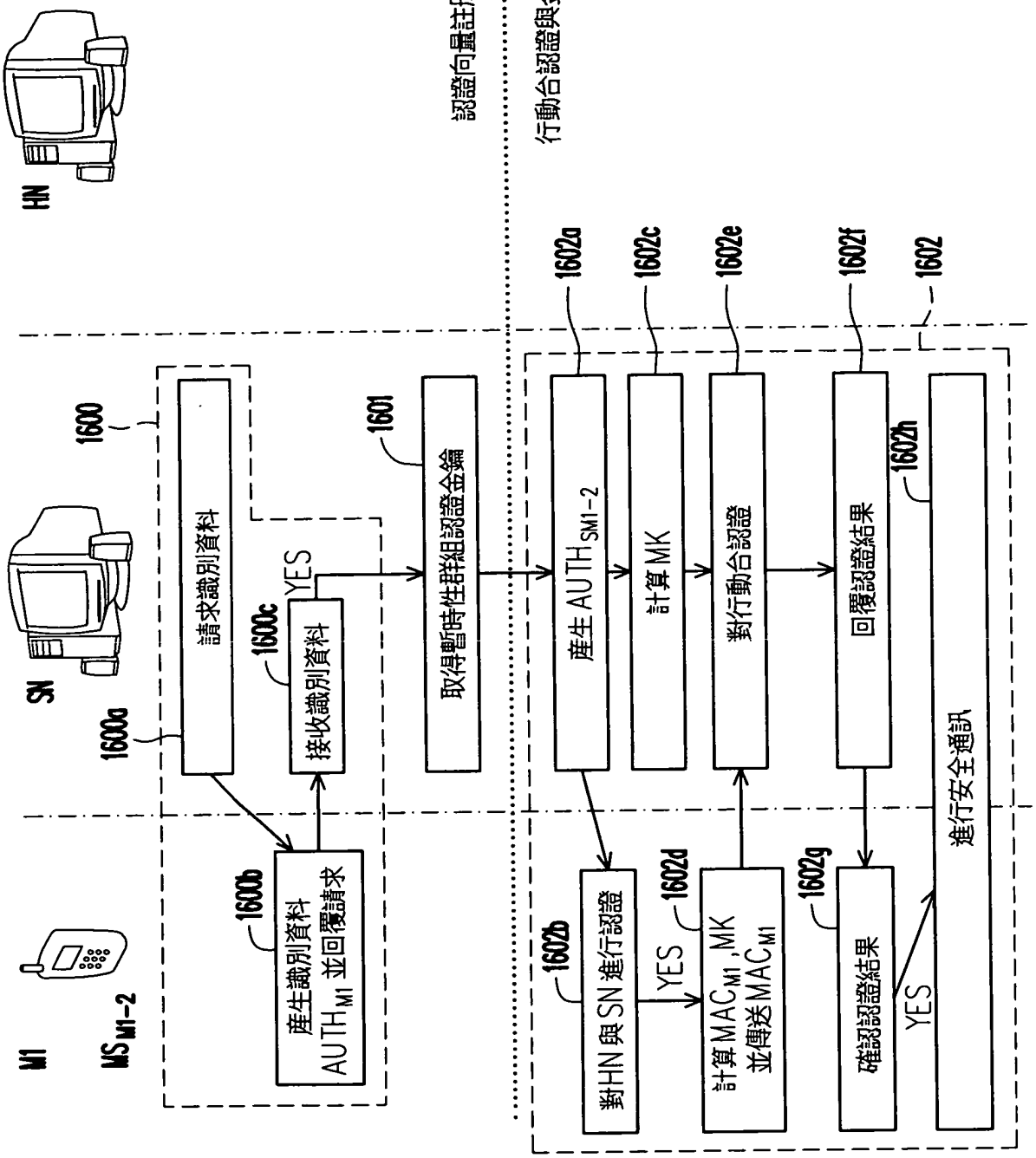
HN
認證向量註冊與分配程序
行動台認證與金鑰分配程序
SN
MS M1-2
M1
1600
1600a
1600b
1600c
1601
1602
1602a
1602b
1602c
1602d
1602e
1602f
1602g
1602h
請求識別資料
接收識別資料
YES
產生識別資料
AUTH M1 並回覆請求
取得暫時性群組認證金鑰
產生 AUTH SM1-2
計算 MK
對行動台認證
回覆認證結果
對HN 與 SN 進行認證
YES
計算 MAC M1 ,MK
並傳送 MAC M1
確認認證結果
YES
進行安全通訊

圖 16

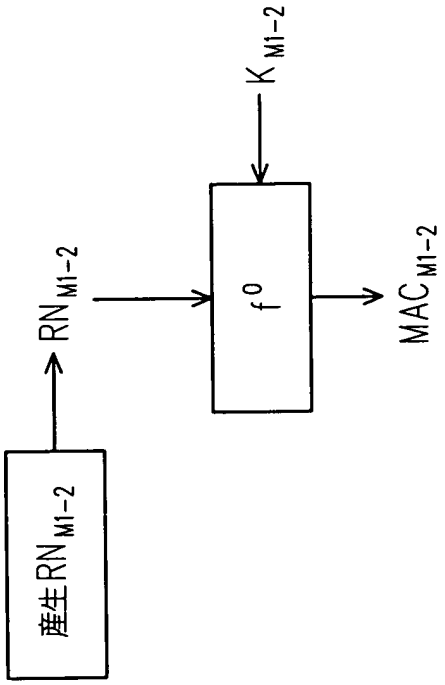

圖17

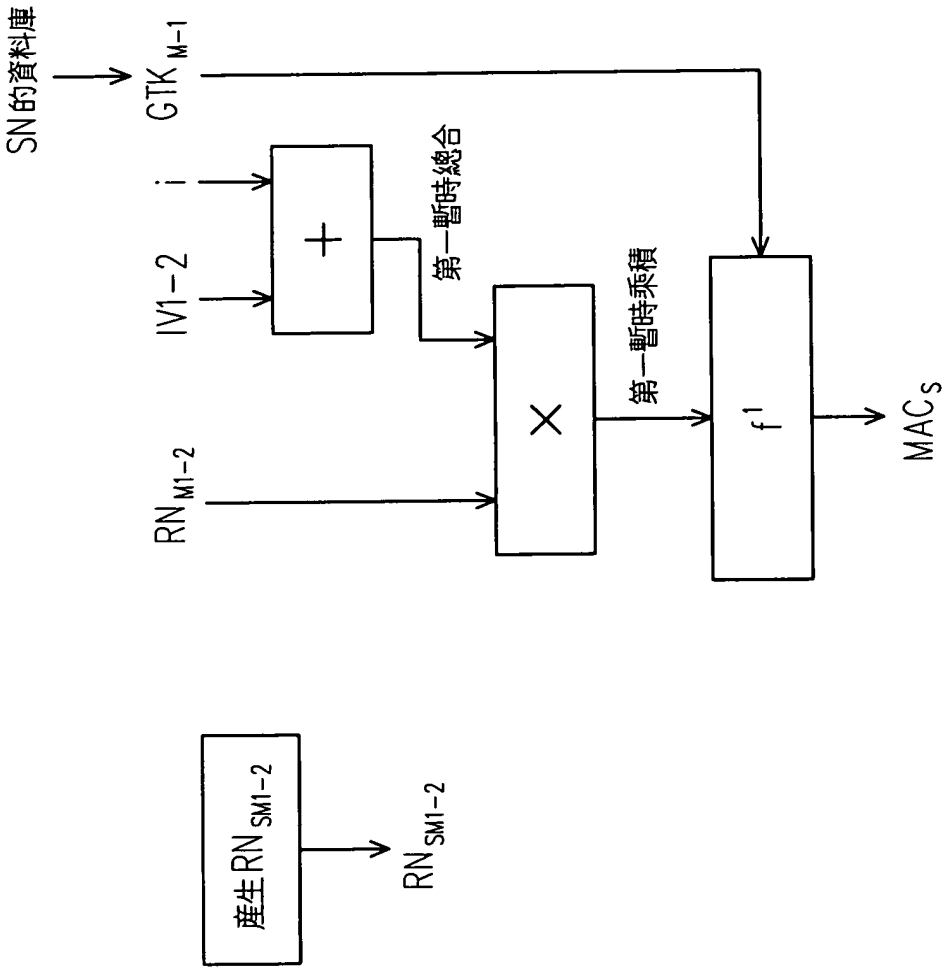
SN的資料庫
GTK M-1
i
IV1-2
+
第一暫時總合
RN M1-2
×
第一暫時乘積
f 1
MAC S
產生RN SM1-2
RN SM1-2

圖18

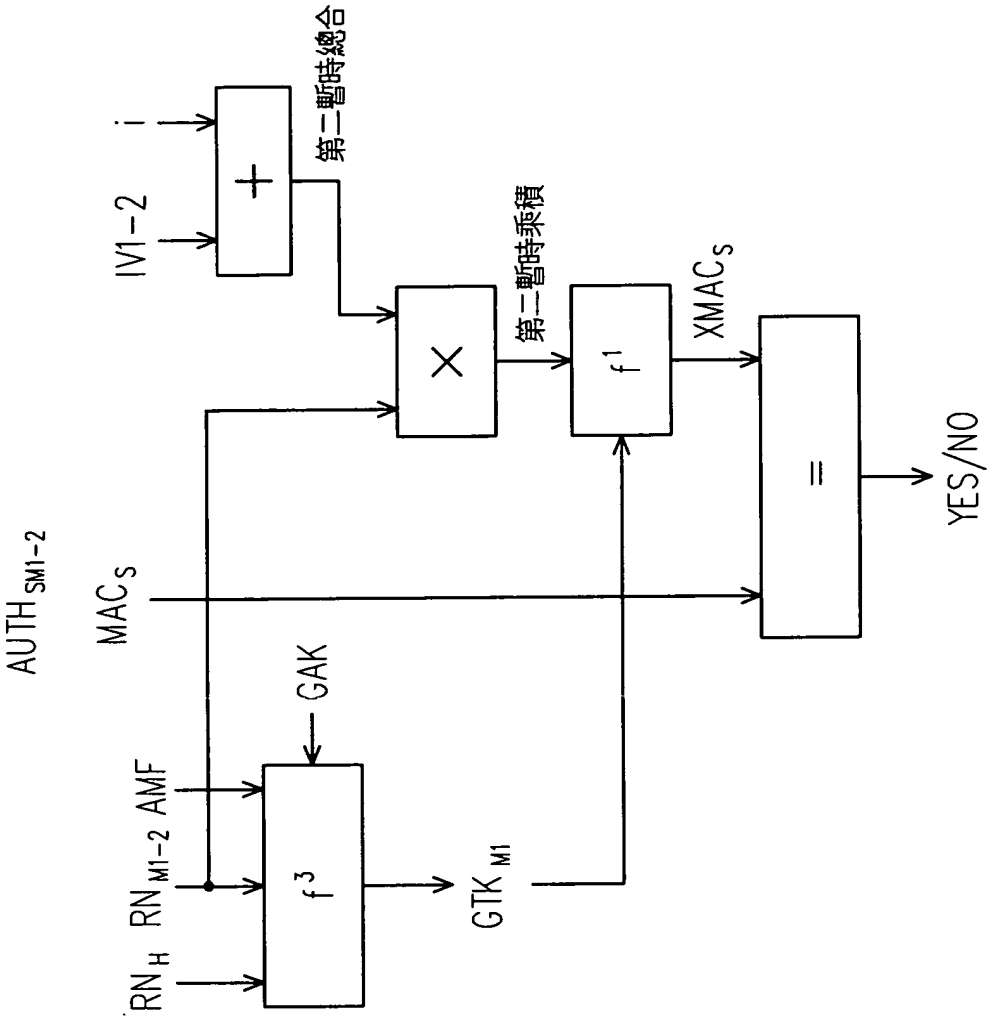
AUTH SM1-2
MAC S
RN H
RN M1-2
AMF
GAK
f 3
GTK M1
IV1-2
i
+
第二暫時總合
×
第二暫時乘積
f 1
XMAC S
=
YES/NO

圖 19

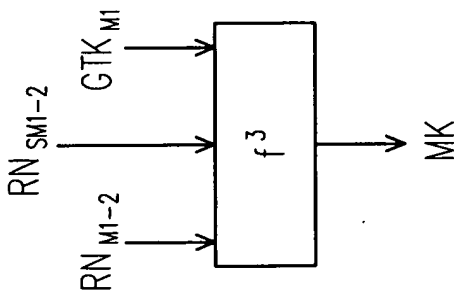

圖20

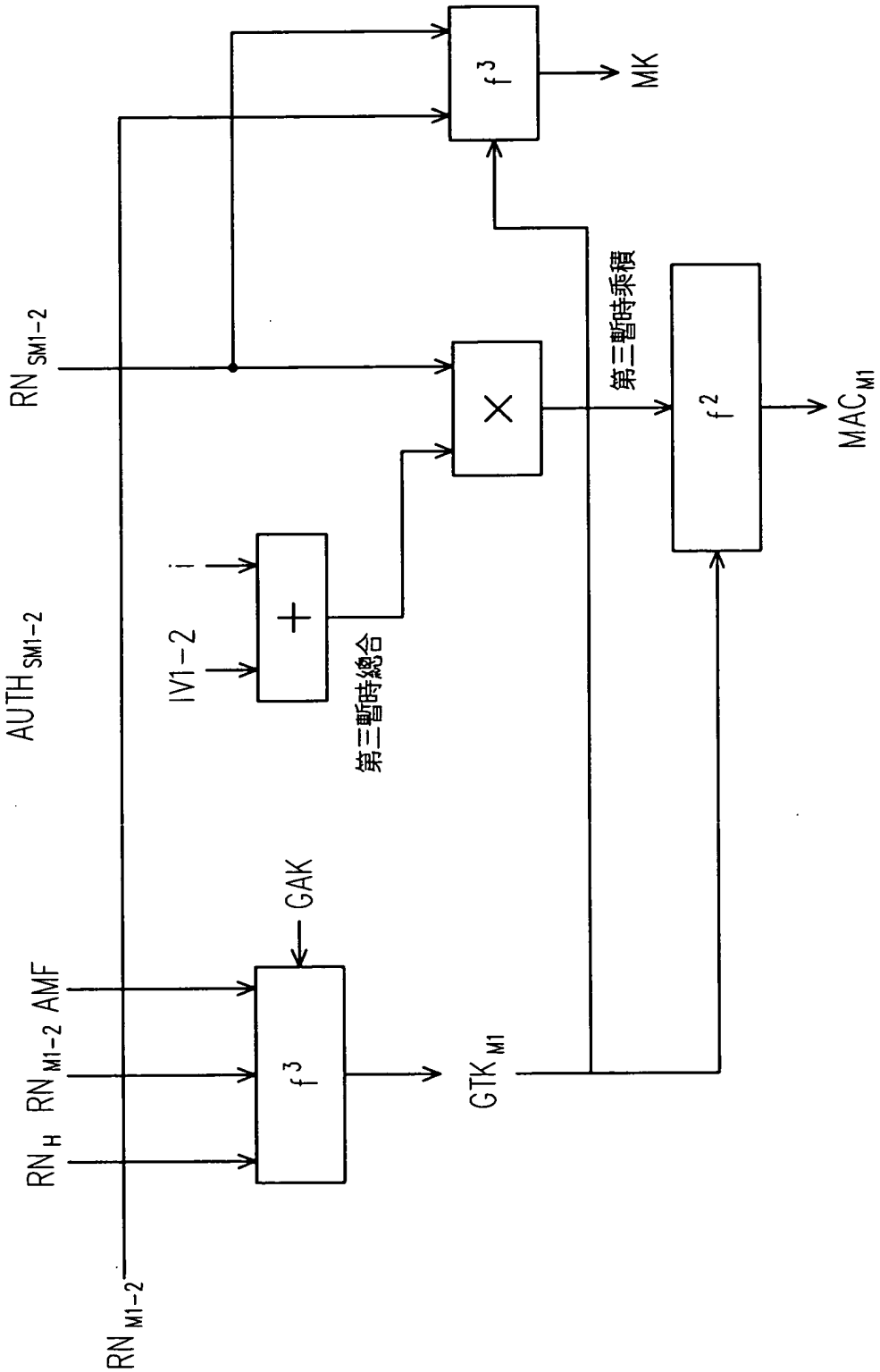
RN SM1-2
AUTH SM1-2
IV1-2
i
第三暫時總合
GAK
RN H
RN M1-2
AMF
RN M1-2
GTK M1
第三暫時乘積
MK
MAC M1
f 3
f 2

圖 21

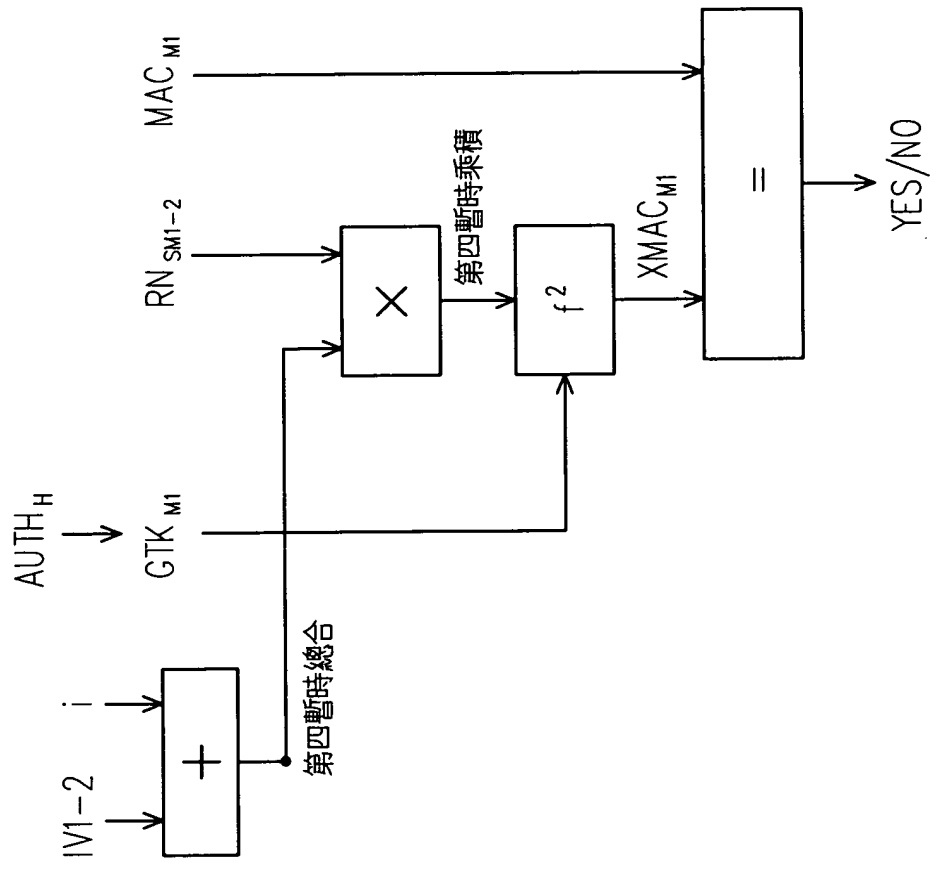

圖 22

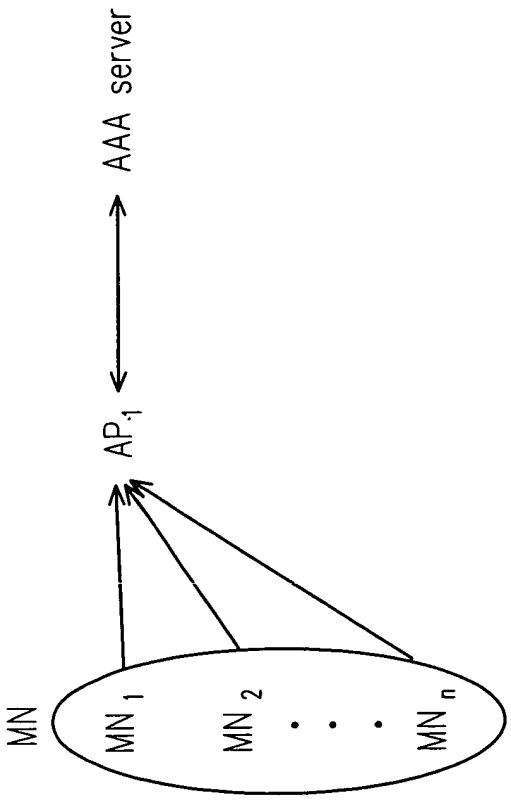

圖23

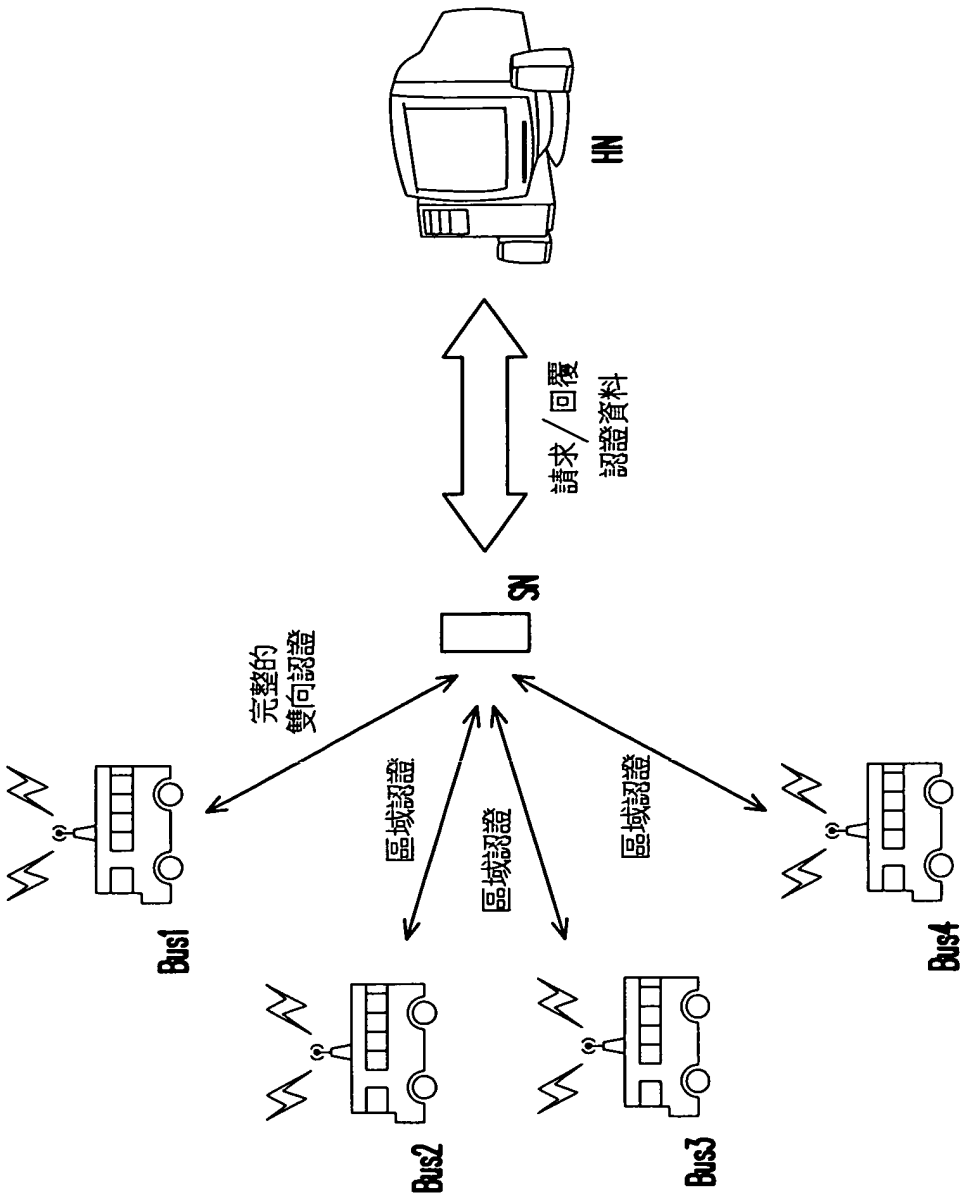

圖 24