



(19) 中華民國智慧財產局

(12) 發明說明書公告本

(11) 證書號數：TW I737702 B

(45) 公告日：中華民國 110 (2021) 年 09 月 01 日

(21) 申請案號：106109848

(22) 申請日：中華民國 106 (2017) 年 03 月 24 日

(51) Int. Cl. : E05B45/06 (2006.01)

E05B47/00 (2006.01)

(30) 優先權：2016/03/24 美國

62/312,709

(71) 申請人：美商品譜公司 (美國) SPECTRUM BRANDS, INC. (US)

美國

(72) 發明人：布朗 特洛伊 BROWN, TROY (US)；布依 覃 BUI, TAM (US)

(74) 代理人：陳長文

(56) 參考文獻：

TW 201538833A

EP 1612742A2

US 2014/0223557A1

US 2015/0281404A1

審查人員：蔡宗澤

申請專利範圍項數：20 項 圖式數：6 共 25 頁

(54) 名稱

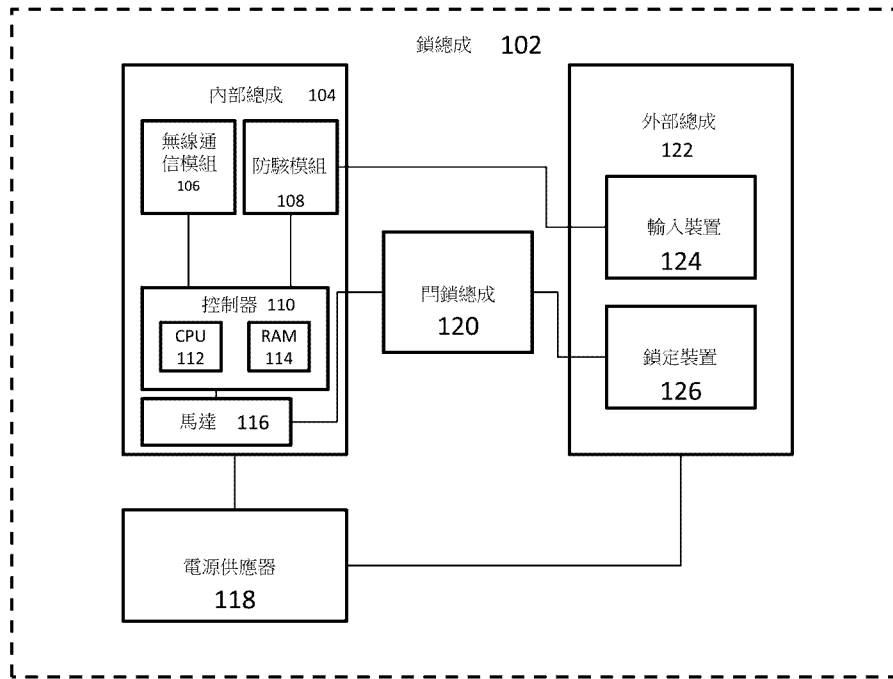
具有防駭特徵之無線鎖具

(57) 摘要

本文描述一種具有經整合之防駭方法之一無線鎖具。該無線鎖具中之該經整合之防駭方法允許偵測由一或多個個人未經授權之存取。該經整合之防駭方法可基於一命令發佈裝置之 MAC 位址來偵測關於無線命令序列號、所接收之命令之時序或洪泛攻擊之一異常及/或未經授權之存取。在偵測到一入侵嘗試後，該無線鎖具即執行一或多個動作。

A wireless lockset with integrated anti-hacking methods is described herein. The integrated anti-hacking methods in the wireless lockset allows the detection of unauthorized access by one or more individuals. The integrated anti-hacking methods can detect an anomaly regarding wireless command sequence numbers, timing of received commands or flooding attack, and/or unauthorized access based on the MAC address of a command-issuing device. Upon detection of a hacking attempt, the wireless lockset performs one or more actions.

指定代表圖：



【圖1】

符號簡單說明：

- 100 . . . 防駭電路
- 102 . . . 鎖總成
- 104 . . . 內部總成
- 106 . . . 無線通信模
組
- 108 . . . 防駭模組
- 110 . . . 控制器
- 112 . . . 處理單元
(「CPU」)
- 114 . . . 記憶體
(「RAM」)
- 116 . . . 馬達
- 118 . . . 電源供應器
- 120 . . . 門鎖總成
- 122 . . . 外部總成
- 124 . . . 輸入裝置
- 126 . . . 鎖定裝置



I737702

【發明摘要】

公告本

【中文發明名稱】

具有防駭特徵之無線鎖具

【英文發明名稱】

WIRELESS LOCKSET WITH ANTI-HACKING FEATURE

【中文】

本文描述一種具有經整合之防駭方法之一無線鎖具。該無線鎖具中之該經整合之防駭方法允許偵測由一或多個個人未經授權之存取。該經整合之防駭方法可基於一命令發佈裝置之MAC位址來偵測關於無線命令序列號、所接收之命令之時序或洪泛攻擊之一異常及/或未經授權之存取。在偵測到一入侵嘗試後，該無線鎖具即執行一或多個動作。

【英文】

A wireless lockset with integrated anti-hacking methods is described herein. The integrated anti-hacking methods in the wireless lockset allows the detection of unauthorized access by one or more individuals. The integrated anti-hacking methods can detect an anomaly regarding wireless command sequence numbers, timing of received commands or flooding attack, and/or unauthorized access based on the MAC address of a command-issuing device. Upon detection of a hacking attempt, the wireless lockset performs one or more actions.

【指定代表圖】

圖1

【代表圖之符號簡單說明】

- 100 防駭電路
- 102 鎖總成
- 104 內部總成
- 106 無線通信模組
- 108 防駭模組
- 110 控制器
- 112 處理單元(「CPU」)
- 114 記憶體(「RAM」)
- 116 馬達
- 118 電源供應器
- 120 門鎖總成
- 122 外部總成
- 124 輸入裝置
- 126 鎖定裝置

【發明說明書】

【中文發明名稱】

具有防駭特徵之無線鎖具

【英文發明名稱】

WIRELESS LOCKSET WITH ANTI-HACKING FEATURE

【技術領域】

本發明大體上係關於鎖；特定言之，本發明係關於一種具有經整合之防駭程序之無線鎖。

【先前技術】

安全系統在住宅及商業市場中廣泛使用。此等裝置藉由要求某些授權認證來控制穿過門進入安全區域，諸如一建築物或其他安全空間。現有安全系統可能受到近年來出現之不同類型之入侵攻擊。例如，一未經授權之人員可能會在一短時間段內嘗試用諸多命令來洪泛一個安全系統。在一些情況下，一未經授權之人員可能會嘗試藉由發送待在其他命令之前執行之高訊框號之命令來混淆安全系統。此等及彼等嘗試係由未經授權之人員做出以獲得存取安全系統之機會。在門鎖具中需要更多智慧係必要的，以最小化一入侵攻擊之風險，並且肯定防止對安全區域之未經授權之存取。

【發明內容】

根據一個態樣，本發明提供具有偵測潛在入侵嘗試之能力之一無線鎖具。例如，在一些實施例中，鎖可偵測發出至鎖及周圍無線存取控制裝置之特定命令之數量及時序。鎖可偵測正被發送至其(洪泛攻擊)之命令數目中之異常及此外時序(快於一般請求)何時已發生。在一些情況下，鎖亦能夠識別及追蹤無線命令序列號，並將在序列號發生一異常時進行回

應。例如，當接收具有一無序序列號之一命令時，該鎖可將此異常偵測為一潛在入侵嘗試。根據情況，鎖可能亦能夠追蹤存取控制面板/集線器之身份，並且辨別其何時自不同於最初指派之一控制面板/集線器發送命令。在偵測到任何此等潛在駭異常後，鎖即可採取某些措施，其包含(但不限於)：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及/或自動鎖定/解鎖動作。

【圖式簡單說明】

詳細描述參考附圖，其中：

圖1係根據本發明之一實施例之一鎖總成之一簡化方塊圖；

圖2係根據本發明之一實施例之一防駭模組之一簡化方塊圖；

圖3係根據本發明之一實施例之一電子鎖之一側視圖，其安裝在一門上並且門以虛線展示；

圖4係根據本發明之一實施例之用於偵測一失序命令之一例示性方法之一流程圖；

圖5係根據本發明之一實施例之用於偵測一洪泛攻擊之一例示性方法之一流程圖；及

圖6係根據本發明之一實施例之用於偵測一裝置之一有效MAC位址之一例示性方法之一流程圖。

【實施方式】

本申請案主張2016年3月24日申請之序號為62/312,709之美國臨時申請案之權益，該案之全文特此以引用的方式併入本文中。

本文提供之圖式及描述可被簡化以繪示與本文所描述之裝置、系統及方法之一清楚理解相關之態樣，同時為清楚起見消除可在典型裝置、系

統及方法中找到之其他態樣。一般技術者可認識到，其他元件及/或操作可能係實施本文所描述之裝置、系統及方法所期望及/或必需的。因為此等元件及操作在此項技術中係眾所周知的，並且因為其不利於更好地理解本發明，所以本文可能不提供對此等元件及操作之一討論。然而，本發明被視為本質上包含將為一般技術者已知之所描述之態樣之所有此等元件、變動及修改。

說明書中對「一個實施例」、「一實施例」，「一繪示性實施例」等之參考指出所描述之實施例可包含一特定特徵、結構或特性，但每一個施例可能或可能不必然包含特定特徵、結構或特性。此外，此等片語不一定指代同一實施例。此外，當結合一實施例描述一特定特徵、結構或特性時，認為在熟習此項技術者之知識範圍內，結合不管是否明確描述之其他實施例影響此特徵、結構或特性。另外，應瞭解，一清單中依「至少一個A、B及C」之形式包含之項目可意謂(A)；(B)；(C)；(A及B)；(A及C)；(B及C)；或(A、B及C)。類似地，依「A、B或C之至少一者」之形式列出之項目可意謂(A)；(B)；(C)；(A及B)；(A及C)；(B及C)；或(A、B及C)。

在附圖中，可依具體之配置及/或排序展示一些結構或方法特徵。然而，應瞭解，可能不需要此等具體配置及/或排序。實情係，在一些實施例中，此等特徵可依與繪示性圖式中所示之一不同之方式及/或順序配置。另外，在一特定圖式中包含之一結構或方法特徵並非意謂在所有實施例中皆需要此特徵，並且在一些實施例中可不包含此特徵或者可與其他特徵組合。

在一些實施例中，本發明係關於偵測已開發並整合至一鎖具(例如一無線鎖具)中之特定類型之入侵攻擊之方法。參考圖1，展示具有一防駭特

徵之一實例性無線鎖，其繪示性地展示為一防駭電路100。儘管術語「電路」被繪示性地用於描述防駭特徵，但在一些情況下，所揭示之實施例可在硬體、韌體、軟體或其等之任何組合中實施。所揭示之實施例亦可被實施為由可由一或多個處理器讀取及執行之一暫時或非暫時性機器可讀(例如，電腦可讀)儲存媒體所攜載或儲存於其上之指令。一機器可讀儲存媒體可體現為用於依由一機器(例如，一揮發性或非揮發性記憶體、一媒體盤或其他媒體裝置)可讀之一形式儲存或傳輸資訊之任何儲存裝置、機構或其他實體結構。

在所展示之實例中，電路100包含一鎖總成102，其包含分別通常安裝在一門之內側及外側之一內部總成104及一外部總成122。如所展示，電路100包含用於為電路100供電之一電源供應器118，電路100可為電池、一太陽能電池或其他電源。在所示之實施例中，電路100包含一門鎖總成120，其通常可諸如由馬達116手動地或電子式地在鎖定位置及解鎖位置之間移動。內部總成104可包含一無線通信模組106、一防駭模組108及一控制器。控制器110亦可包含一處理單元(「CPU」) 112及一記憶體(「RAM」)114。外部總成122可包含諸如用於輸入一驗證碼之一鍵台之一輸入裝置124及一鎖定裝置126。控制器110可包含一無線通信模組106，其促進與一閘道(未展示)、一使用者之行動裝置(未展示)或用於警示、遠端命令及/或與電路100之其他發訊息之其他連接裝置之無線通信，其可為透過任何一或多個相關聯無線通信協定(例如，Bluetooth®、Wi-Fi®、WiMAX、Zigbee®、Z-Wave®等)。

鎖總成102之防駭模組108可體現為硬體、韌體、軟體或其等之一組合。因而，在一些實施例中，防駭模組可體現為電裝置之電路或一集合

(例如，封包檢測電路、時序攻擊偵測器電路，洪泛攻擊偵測器電路等)。應瞭解，在此等實施例中，電路之一或多者可形成鎖定總成之處理器、記憶體及/或其他電組件之一部分。

參考圖2，展示用於本發明之至少一個實施例之防駭模組108之一實例性方塊圖200。在所示之實例中，防駭模組108可包含一封包檢測引擎204、一洪泛攻擊偵測器206、一無線命令計數器208、一時序攻擊偵測器210及一入侵攻擊通知引擎212。在一些實施例中，封包檢測引擎204檢測由無線通信模組106接收之封包。此等封包可被提供給洪泛攻擊偵測器206，以判定封包是否為一洪泛攻擊之一部分，其可基於關於由無線命令計數器208接收之命令之一數目的資料。封包亦可被提供給時序攻擊偵測器210，以判定封包是否為一時序攻擊之部分。時序攻擊偵測器210可與一資料庫214進一步通信以儲存無線命令時間資料。若洪泛攻擊偵測器206及/或時序攻擊偵測器210判定一封包可為一攻擊之部分，則一訊息將被提供給入侵攻擊通知引擎，該入侵攻擊通知引擎將向此攻擊提供一警示。取決於一期望之組態，可以硬體及/或軟體之一組合來實現之防駭模組中描繪之一系列引擎及偵測器可如由適當箭頭所繪示般彼此通信。應注意，此組態僅僅係出於例示性目的，並且可根據需要重新配置。

圖3展示根據本發明之實施例之安裝至一門302之一例示性電子鎖300。在所示之實例中，電子鎖300包含具有一電池固持器306之一內部總成304、一轉向件308、一鎖門310、一撞擊件312、一使用者輸入314、一外部總成316、一機械鎖定總成318及一鑰匙320。在一些情況下，認證及/或命令可無線地提供給電子鎖300，諸如2014年2月25日申請之針對一「Electronic Deadbolt」之美國專利申請號2014/0250956中所揭示的，其

特此以引用的方式併入本文中。在另一實例中，電子鎖可經配備以經由觸摸啟動接收使用者認證，諸如在美國專利號9,024,759中揭示的，其特此以引用的方式併入本文中。

圖4係展示使用防駭模組108來偵測具有一無序訊框計數之一命令之一無線鎖具300之一實例性防駭方法之一簡化流程圖。在此實例中，方法400自方塊402開始，其中判定一計數器變數。該計數器變數可為一序列號。該計數器變數可儲存在一典型儲存裝置或一資料庫中。在鎖具處接收各無線命令時，存在與各命令相關聯之一序列號。此確保在一鎖具處接收之命令依序執行。當各命令執行時，一計數器變數可累加，並且防止具有低於計數器變數值之一序列號之命令被執行或(換言之)不依序執行。

回至圖4，在判定計數器變數之後，程序進行至步驟404，且無線鎖具接收一命令。然後基於與所接收之命令相關聯之序列號，做出一決策406以偵測一異常。若序列號顯著高於計數器變數達一預定量，則程序進行至步驟410，並執行一特殊動作。該特殊動作可包含(但不限於)超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及一自動鎖定/解鎖動作或類似者。在命令序列號不被認為顯著更高之情況下，程序進行至步驟408，並繼續命令之正常處理。在此實例性案例中，執行命令並累加計數器變數。一典型命令可為鎖具之一鎖定命令或鎖具之一解鎖命令。圖4之異常偵測係針對無序訊框計數之偵測。在此實例中，駭客可能會嘗試發出一錯誤命令，並程式化該錯誤命令以具有一非常高之序列號。

圖5係展示使用防駭模組108來偵測一洪泛攻擊之一無線鎖具300之一實例性防駭方法之一簡化流程圖。在此實例中，方法500自步驟502開

始，以追蹤所接收之命令之間之時間。例如，所追蹤之時間變數可儲存在例如一儲存裝置或一資料庫中。在步驟504中，可判定命令之間之平均時間並將其儲存為一變數，例如一Delta變數。在決策方塊506中，基於在一特定時間段內所接收之命令之數量或所接收之命令之間之經判定之平均時間或兩者之一組合來判定一異常存在。在一個實施例中，例如，最近所接收之命令可包含在過去30秒或30分鐘內所接收之所有命令。替代地，例如，最近所接收之命令可包含一特定量之命令，諸如最後五個所接收之命令。若命令之間之平均時間被認為係低於正規平均時間之一預定量，則認為異常被偵測到，並且程序進行至步驟510，並且可執行一特殊動作。特殊動作可包含(但不限於)超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及一自動鎖定/解鎖動作或類似者。在未偵測到異常之情況下，該程序進行至步驟508並執行命令。

圖6係展示使用防駭模組108之一無線鎖具300之一實例性防駭方法之一簡化流程圖。在此實例中，在步驟602，方法600開始於在鎖具300處自一使用者裝置接收一命令。該命令包含使用者裝置之一識別符。在一個實施例中，識別符可為使用者裝置之一媒體存取控制(media access control, MAC)位址。在決策方塊604，鎖具300判定識別符是否被辨識。例如，可將識別符與可信或有效識別符之一表進行比較。繼續上述實例，該表可包括被判定為與一可信使用者裝置相關聯之有效MAC位址之一清單。在識別符被辨識且因此未偵測到異常之情況下，程序進行至步驟606並且執行命令。在識別符未被辨識且因此偵測到一異常之情況下，程序進行至步驟608，並且可執行一特殊動作。該特殊動作可包含(但不限於)超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及一自動鎖定/解鎖動作或類似者。

實例

以下提供本文揭示之鎖具之繪示性實例。鎖具之一實施例可包含下文描述之實例之一或多者以及其等之任何組合。

實例1係一鎖具，其包含一門鎖總成、一控制器、一內部總成及一外部總成。該門鎖總成具有可在一延伸位置與一縮回位置之間移動之一鎖門。該控制器經組態以電子地控制該鎖門在延伸位置及縮回位置之間之移動。該內部總成包含用於在延伸位置與縮回位置之間手動地致動鎖門之一轉動件。該外部總成包含一機構門鎖總成，其經組態以在延伸位置與縮回位置之間手動地移動鎖門。該控制器經組態以判定一命令序列號，接收至少一個命令，將該命令序列號和與所接收之命令相關聯之一序列號進行比較以識別一異常，回應於一異常未被識別而執行命令，並回應於一異常被識別而執行一特殊動作。

在實例2中，實例1之標的進一步經組態使得命令序列號回應於所接收之命令被執行而累加。

在實例3中，實例1之標的進一步經組態使得命令在被執行時致使鎖門移動至延伸位置或縮回位置中。

在實例4中，實例1之標的進一步經組態使得該特殊動作包含下列之至少一者：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及該鎖具之一自動鎖定/解鎖。

在實例5中，實例1之標的進一步經組態使得在所接收之命令序列號顯著大於命令序列號時識別異常。

在實例6中，實例1之標的進一步經組態使得在所接收之命令序列號與命令序列號之間之一差異超過一預定量時識別異常。

實例7係一鎖具，其包含一門鎖總成、一控制器、一內部總成及一外部總成。該門鎖總成包含可在一延伸位置與一縮回位置之間移動之一鎖門。該控制器經組態以電子地控制該鎖門在該延伸位置與該縮回位置之間之移動。該內部總成包含用於在該延伸位置與該縮回位置之間手動地致動該鎖門之一轉動件。該外部總成包含經組態以在該延伸位置與該縮回位置之間手動地移動該鎖門之一機械鎖總成。該控制器經組態以追蹤在該控制器處接收之一系列命令，回應於基於該系列命令之一數量及/或一時序來判定尚未偵測到一異常而執行該系列命令之至少一者，以及回應於基於該系列命令之一數量及/或一時序來判定已偵測到一異常而執行一特殊動作。

在實例8中，實例7之標的進一步經組態使得時序係基於所接收之命令之間之一平均時間。

在實例9中，實例7之標的進一步經組態使得該量係基於在一預定時段內所接收之一特定量之命令。

在實例10中，實例7之標的進一步經組態使得特殊動作包含下列之至少一者：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及該鎖具之一自動鎖定/解鎖。

在實例11中，實例7之標的進一步經組態使得該命令在被執行時致使該鎖門移動至該延伸位置或該縮回位置中。

實例12係一鎖具，其包含一門鎖總成、一控制器、一內部總成及一外部總成。該門鎖總成包含可在一延伸位置與一縮回位置之間移動之一鎖門。該控制器經組態以電子地控制該鎖門在該延伸位置與該縮回位置之間之移動。該內部總成包含用於在該延伸位置與該縮回位置之間手動地致動

該鎖門之一轉動件。該外部總成包含經組態以在該延伸位置與該縮回位置之間手動地移動該鎖門之一機械鎖總成。該控制器進一步經組態以自一裝置接收至少一個命令，其中該至少一個命令包括與該裝置相關聯之一識別符，判定該識別符是否被辨識，回應於該識別符被辨識而執行該命令；及回應於該識別符未被辨識而執行一特殊動作。

在實例13中，實例12之標的進一步經組態使得將識別符與已知識別符之一清單進行比較，以判定識別符是否被辨識。

在實例14中，實例12之標的進一步經組態使得識別符係一MAC位址。

在實例15中，實例12之標的進一步經組態使得特殊動作包含下列之至少一者：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及該鎖具之一自動鎖定/解鎖。

在實例16中，實例12之標的進一步經組態使得該命令在被執行時致使該鎖門移動至該延伸位置或該縮回位置中。

雖然鑑於以上描述已參考特定手段、材料及實施例描述本發明，但熟習此項技術者可容易地確定本發明之基本特徵，並且可進行各種改變及修改以適應各種用途及特徵，而不背離如隨附申請專利範圍中闡述之本發明之精神及範疇。

【符號說明】

- 100 防駭電路
- 102 鎖總成
- 104 內部總成
- 106 無線通信模組

- 108 防駭模組
- 110 控制器
- 112 處理單元(「CPU」)
- 114 記憶體(「RAM」)
- 116 馬達
- 118 電源供應器
- 120 門鎖總成
- 122 外部總成
- 124 輸入裝置
- 126 鎖定裝置
- 200 實例性方塊圖
- 204 封包檢測引擎
- 206 洪泛攻擊偵測器
- 208 無線命令計數器
- 210 時序攻擊偵測器
- 212 入侵攻擊通知引擎
- 214 資料庫
- 300 電子鎖/無線鎖具
- 302 門
- 304 內部總成
- 306 電池固持器
- 308 轉向件
- 310 鎖門

- 312 撞擊件
- 314 使用者輸入
- 316 外部總成
- 318 機械鎖定總成
- 320 鑰匙
- 400 方法
- 402 步驟
- 404 步驟
- 406 步驟
- 408 步驟
- 410 步驟
- 500 方法
- 502 步驟
- 504 步驟
- 506 步驟
- 508 步驟
- 510 步驟
- 600 方法
- 602 步驟
- 604 步驟
- 606 步驟
- 608 步驟

【發明申請專利範圍】

【第1項】

一種鎖具，其包括：

一門鎖總成，其包含可在一延伸位置與一縮回位置之間移動之一鎖門；

一控制器，其經組態以電子地控制該鎖門在該延伸位置與該縮回位置之間之移動；

一無線通信介面，其可通信連接至該控制器；

一內部總成，其包含用於在該延伸位置與該縮回位置之間手動地致動該鎖門之一轉動件；

一外部總成，其包含經組態以在該延伸位置與該縮回位置之間手動地移動該鎖門之一機械鎖總成；

其中該控制器進一步經組態以：

判定一命令序列號；

通過該無線通信介面接收至少一個命令；

將該命令序列號與與該所接收之命令相關聯之一序列號進行比較以識別一異常，其中該異常係為一潛在入侵嘗試；

回應於未被識別之一異常而執行該至少一命令；及

回應於被識別之一異常而執行一特殊動作，其中該特殊動作不同於該至少一命令。

【第2項】

如請求項1之鎖具，其中該命令序列號回應於正被執行之該所接收之命令而累加。

【第3項】

如請求項1之鎖具，其中該至少一命令在被執行時致使該鎖門移動至該延伸位置或該縮回位置中。

【第4項】

如請求項1之鎖具，其中該特殊動作包含下列之至少一者：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及該鎖具之一自動鎖定/解鎖。

【第5項】

如請求項1之鎖具，其中在該所接收之命令序列號顯著大於該命令序列號時識別該異常。

【第6項】

如請求項1之鎖具，其中在該所接收之命令序列號與該命令序列號之間之一差異超過一預定量時識別該異常。

【第7項】

如請求項1之鎖具，其中該無線通信介面經組態以與一行動裝置通信。

【第8項】

如請求項1之鎖具，其中該特殊動作包含在一預定時間內停用該無線通信介面。

【第9項】

如請求項8之鎖具，其中該特殊動作包含產生至少一無線警報。

【第10項】

一種鎖具，其包括：

一門鎖總成，其包含可在一延伸位置與一縮回位置之間移動之一鎖門；

一控制器，其經組態以電子地控制該鎖門在該延伸位置與該縮回位置之間之移動；

一無線通信介面，其可通信連接至該控制器；

一內部總成，其包含用於在該延伸位置與該縮回位置之間手動地致動該鎖門之一轉動件；

一外部總成，其包含經組態以在該延伸位置與該縮回位置之間手動地移動該鎖門之一機械鎖總成；

其中該控制器進一步經組態以：

追蹤在該無線通信介面處接收之一系列命令；

回應於基於該系列命令之一數量及/或一時序來判定尚未偵測到一異常而執行該系列命令之至少一者，其中該異常係為一潛在入侵嘗試；及

回應於基於該系列命令之一數量及/或一時序來判定已偵測到一異常而執行一特殊動作，其中該特殊動作不同於該至少一命令。

【第11項】

如請求項10之鎖具，其中該時序係基於所接收之命令之間之一平均時間。

【第12項】

如請求項10之鎖具，其中該量係基於在一預定時段內所接收之一特定量之命令。

【第13項】

如請求項10之鎖具，其中該特殊動作包含下列之至少一者：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及該鎖具之一自動鎖定/解鎖。

【第14項】

如請求項10之鎖具，其中該系列命令在被執行時致使該鎖門移動至該延伸位置或該縮回位置中。

【第15項】

一種鎖具，其包含：

一門鎖總成，其包含可在一延伸位置與一縮回位置之間移動之一鎖門；

一控制器，其經組態以電子地控制該鎖門在該延伸位置與該縮回位置之間之移動；

一無線通信介面，其可通信連接至該控制器；

一內部總成，其包含用於在該延伸位置與該縮回位置之間手動地致動該鎖門之一轉動件；

一外部總成，其包含經組態以在該延伸位置與該縮回位置之間手動地移動該鎖門之一機械鎖總成；

其中該控制器進一步經組態以：

通過該無線通信介面自一裝置接收至少一個命令，其中該至少一個命令包括與該裝置相關聯之一識別符；

判定該識別符是否被辨識；

回應於該識別符被辨識而執行該至少一命令；及

回應於該識別符未被辨識而執行一特殊動作，其中該特殊動作不

同於該至少一命令。

【第16項】

如請求項15之鎖具，其中將該識別符與已知識別符之一清單進行比較，以判定該識別符是否被辨識。

【第17項】

如請求項15之鎖具，其中該識別符係將該至少一命令傳輸至該鎖具之該裝置之一媒體存取控制(MAC)位址。

【第18項】

如請求項15之鎖具，其中該特殊動作包含下列之至少一者：超時、鍵台停用、無線停用、通知、聲訊警報、無線警報、LED指示燈及該鎖具之一自動鎖定/解鎖。

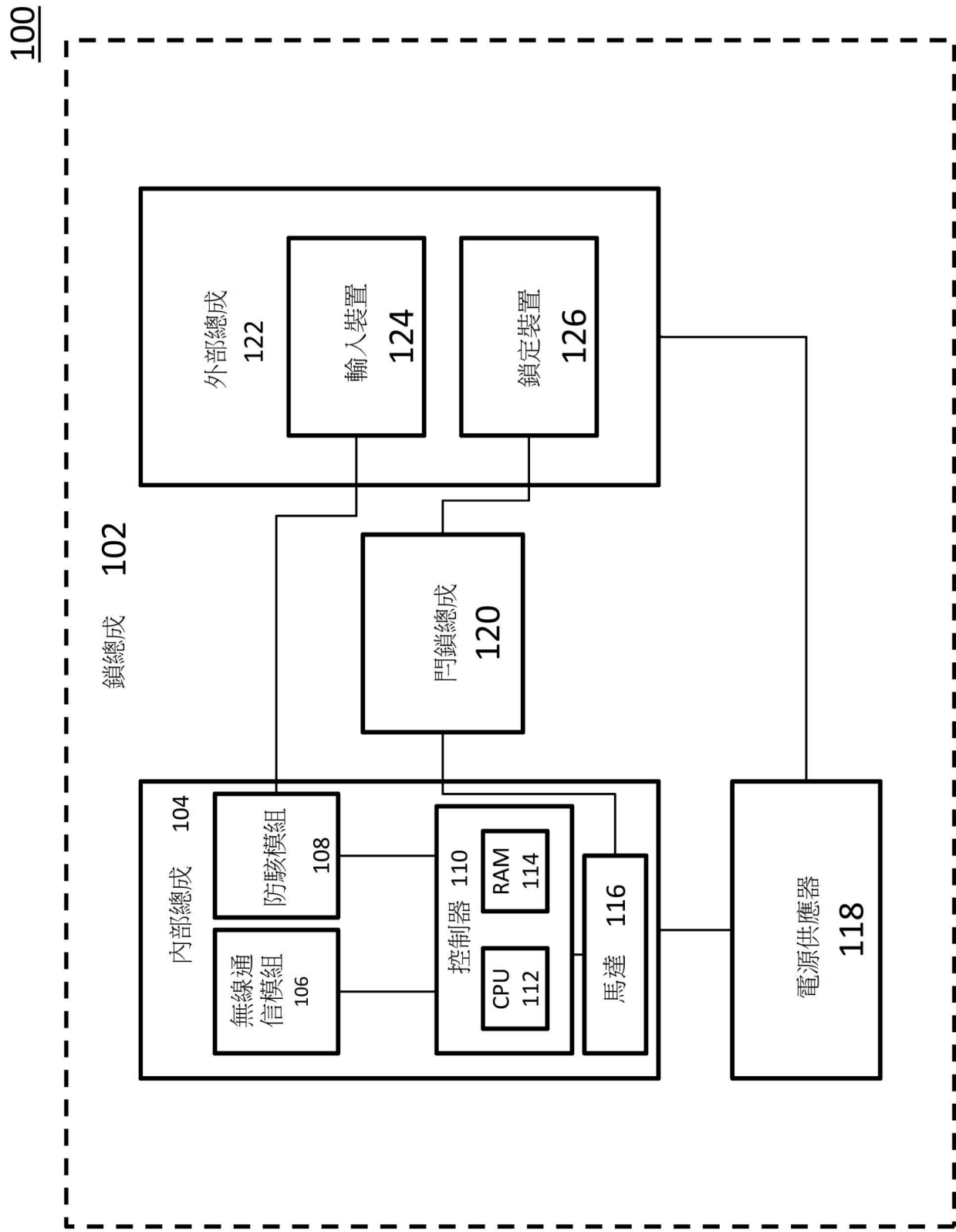
【第19項】

如請求項15之鎖具，其中該至少一命令在被執行時致使該鎖門移動至該延伸位置或該縮回位置中。

【第20項】

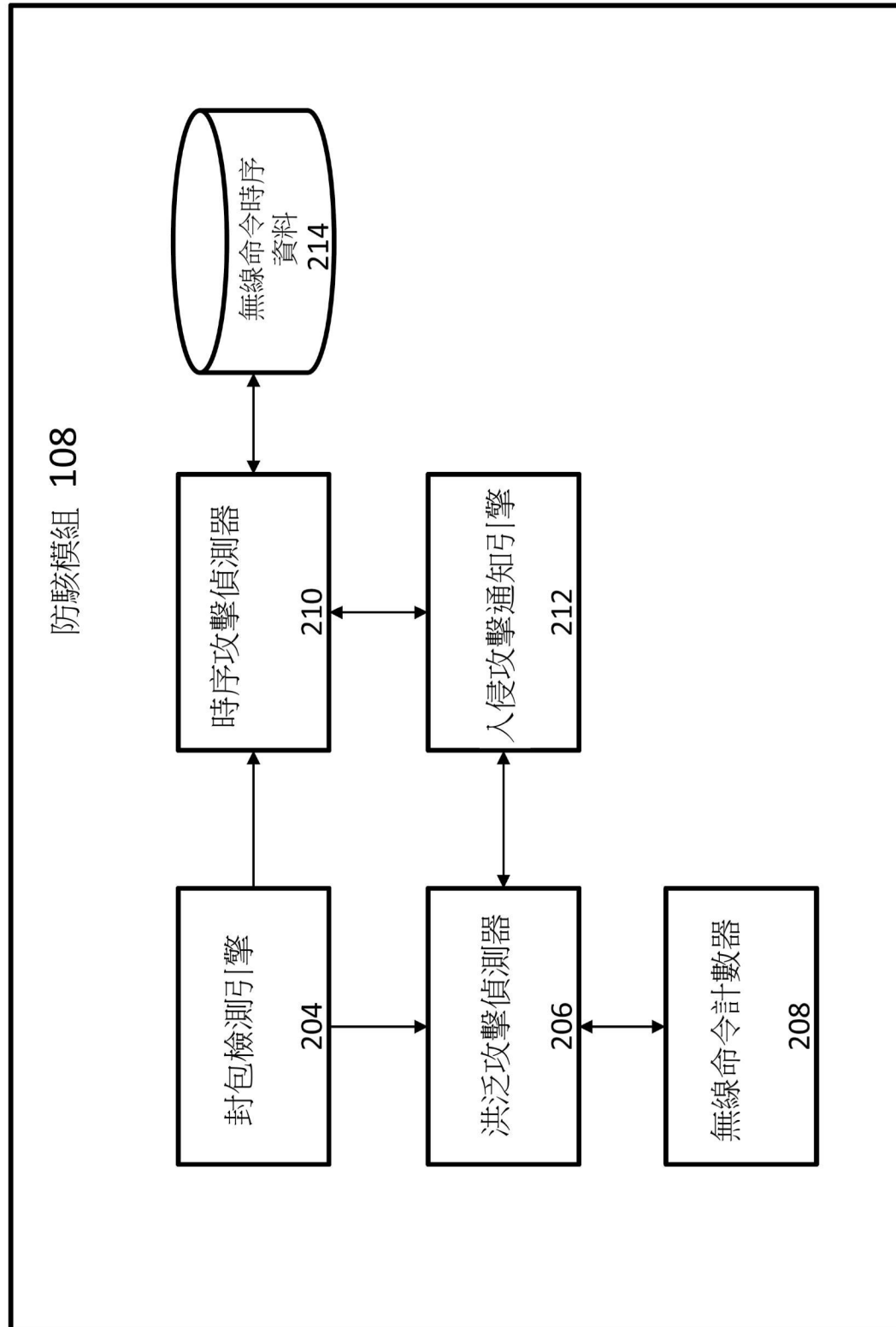
如請求項17之鎖具，其中該裝置之該MAC位址與有效MAC位址之一清單進行比較，有效MAC位址之該清單之各者與一可信使用者裝置相關聯。

【發明圖式】

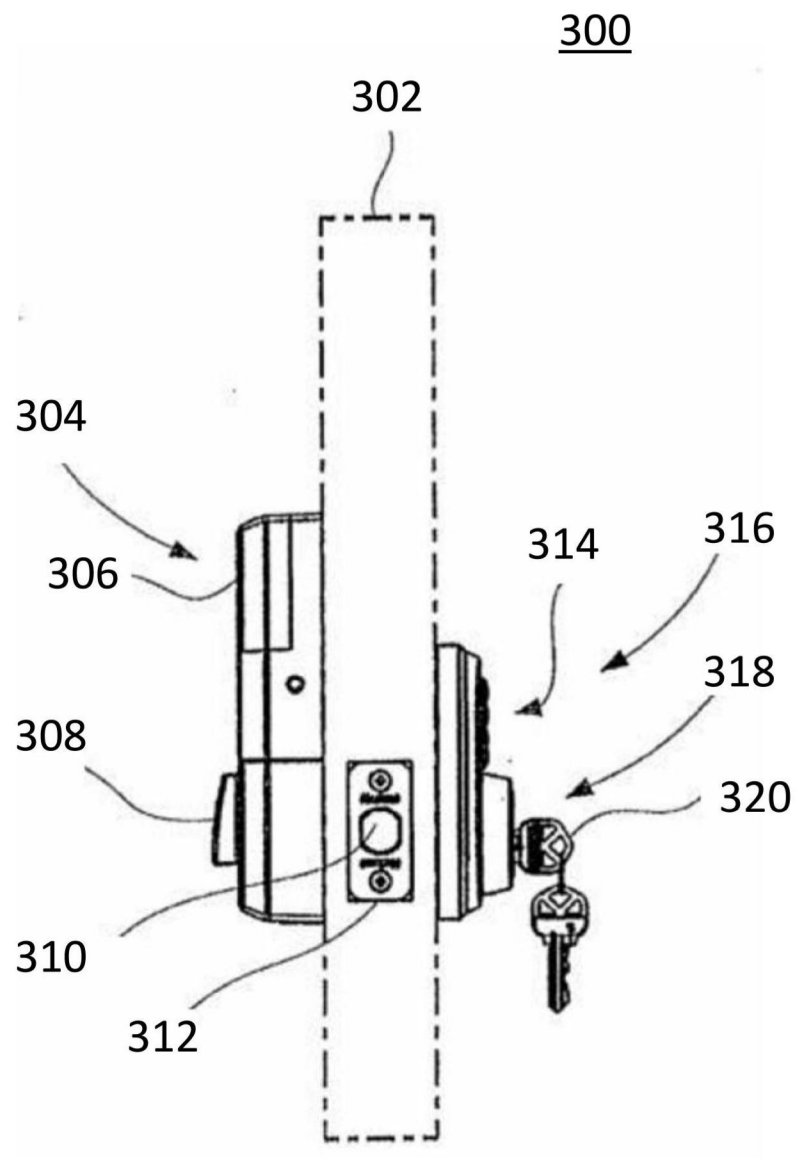


【圖1】

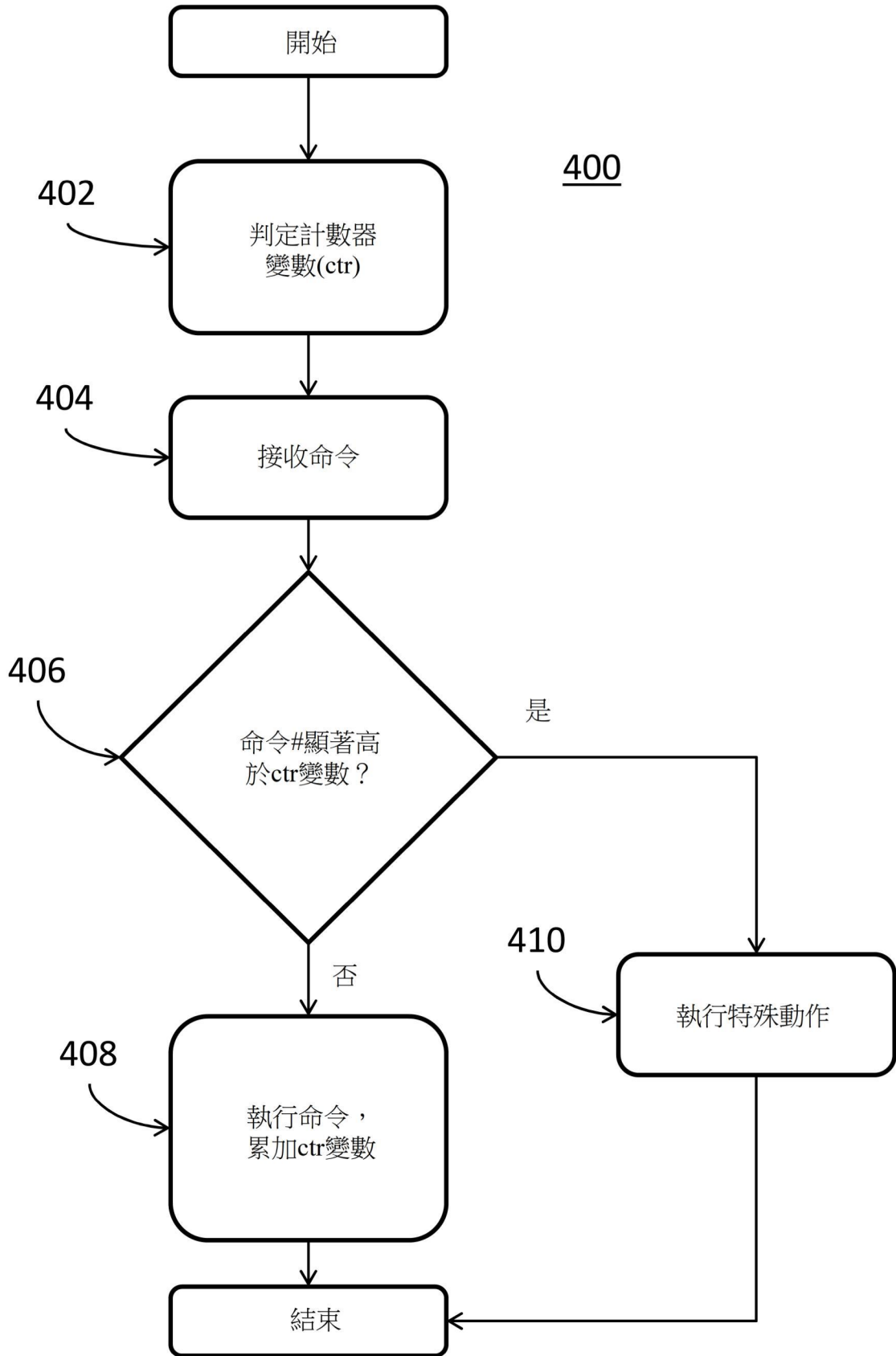
200



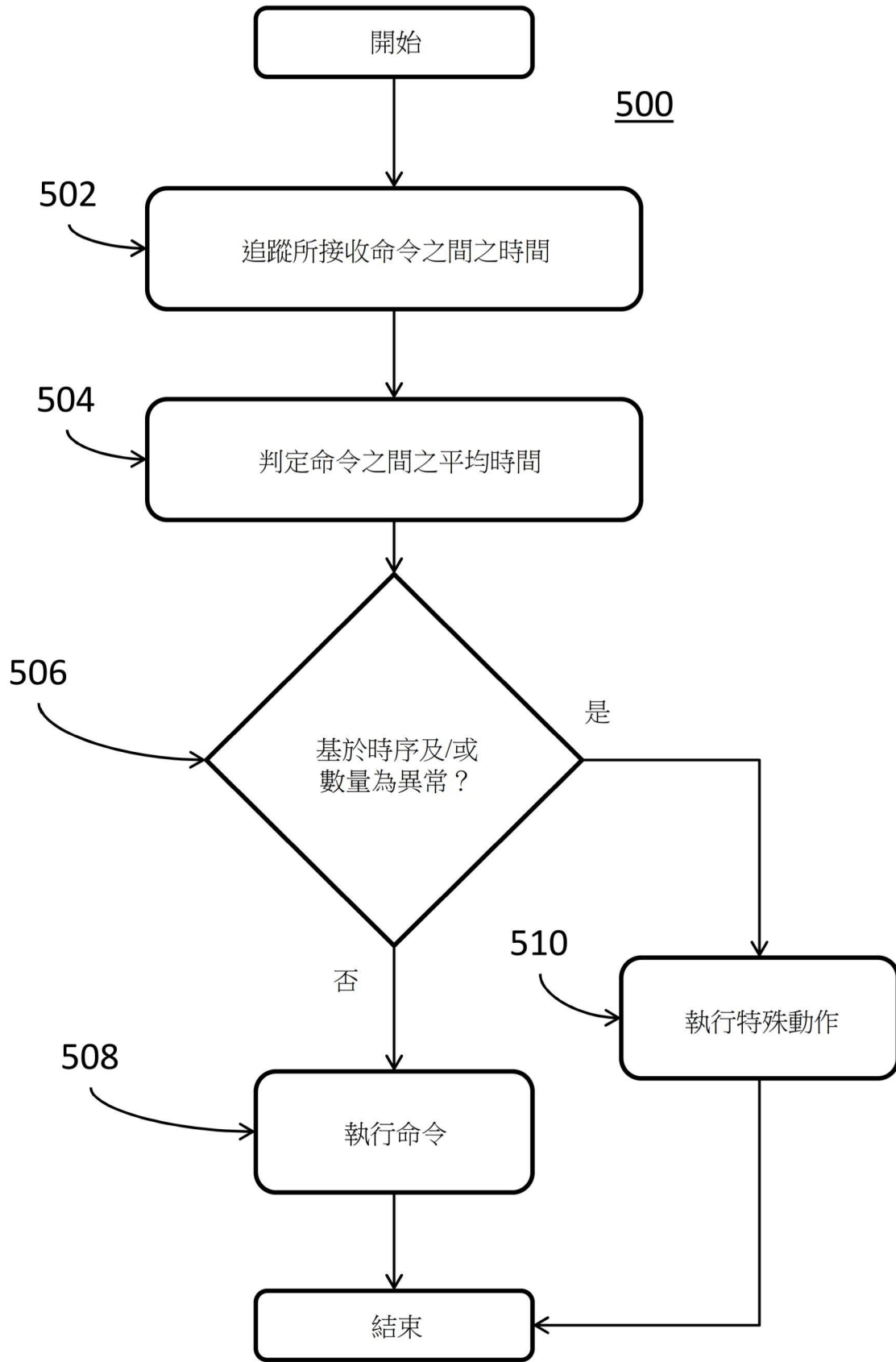
【圖2】



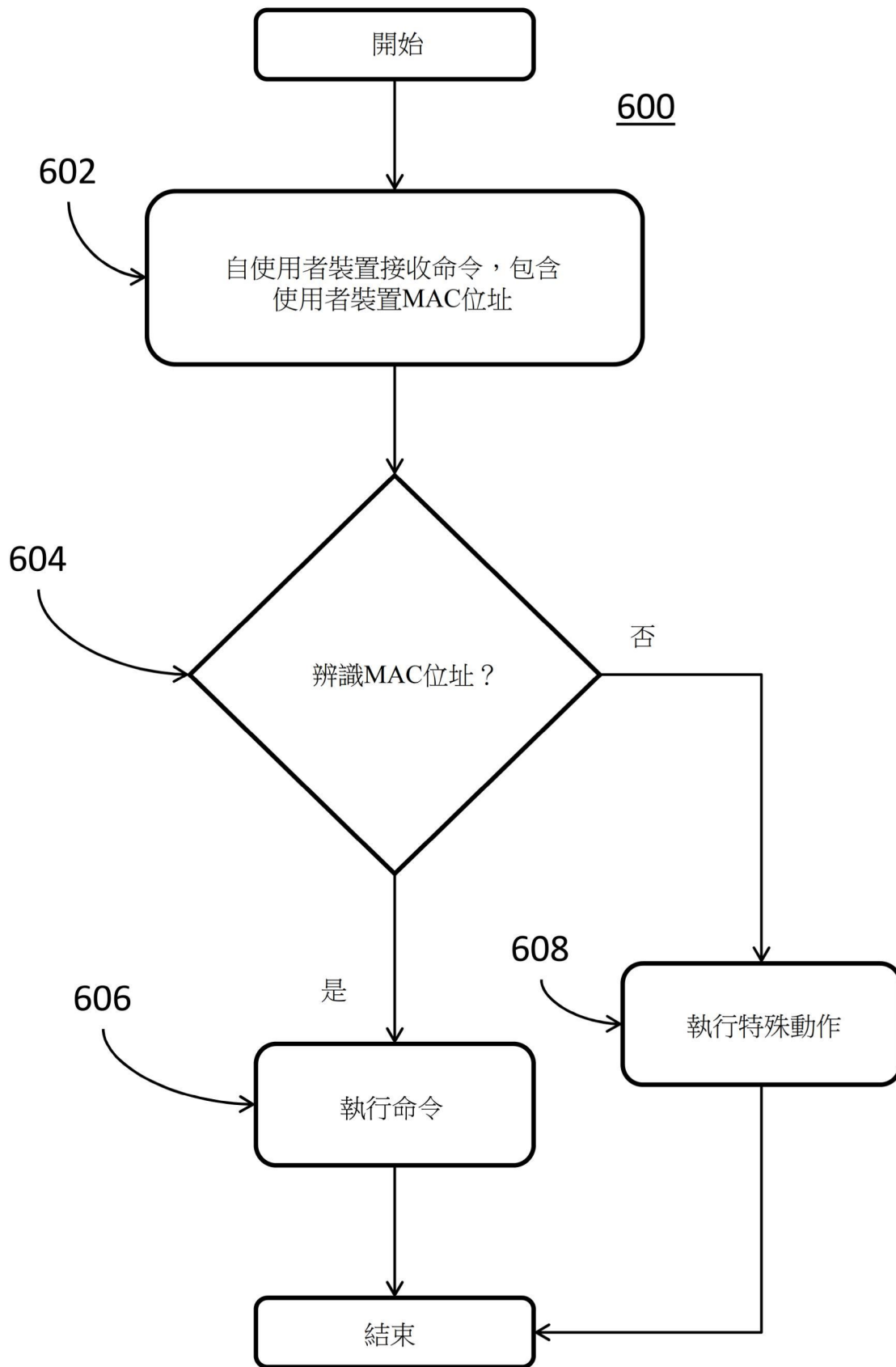
【圖3】



【圖4】



【圖5】



【圖6】