



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201642613 A

(43)公開日：中華民國 105 (2016) 年 12 月 01 日

(21)申請案號：105111515

(22)申請日：中華民國 105 (2016) 年 04 月 13 日

(51)Int. Cl. : H04L1/00 (2006.01) H04L5/00 (2006.01)

H04L12/26 (2006.01) H04L1/12 (2006.01)

(30)優先權：2015/05/29 美國 62/168,579

2015/12/16 美國 14/971,723

(71)申請人：高通公司(美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：希爾藍約翰 HILLAN, JOHN (GB)；歐唐諾古傑洛米羅賓克里斯多福 O'DONOGHUE,

JEREMY ROBIN CHRIS (GB)；法蘭克朗史蒂芬 FRANKLAND, STEPHEN (GB)

(74)代理人：李世章

申請實體審查：無 申請專利範圍項數：49 項 圖式數：9 共 62 頁

(54)名稱

用於決定設備之間的距離的上界的系統和方法

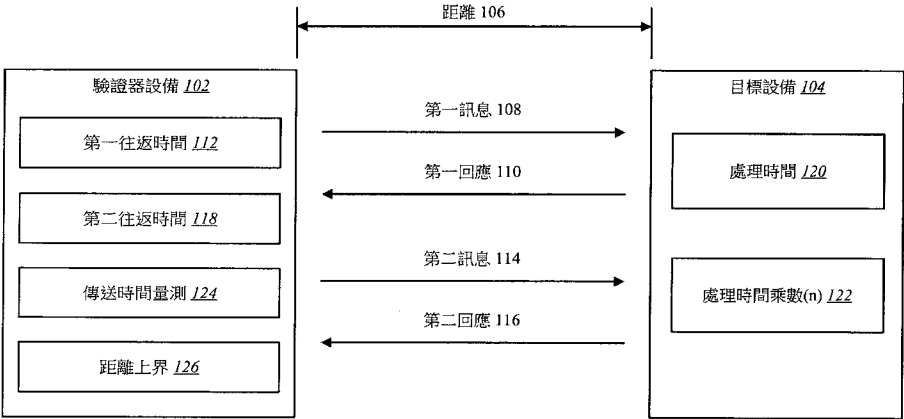
SYSTEMS AND METHODS FOR DETERMINING AN UPPER BOUND ON THE DISTANCE
BETWEEN DEVICES

(57)摘要

描述了一種用於由驗證器設備決定距離上界的方法。該方法包括量測從目標設備接收對應於發送給該目標設備的第一訊息的第一回應的第一往返時間。該方法亦包括量測從目標設備接收對應於發送給該目標設備的第二訊息的第二回應的第二往返時間，第二回應經由處理時間乘數來延遲。該方法進一步包括基於第一往返時間、第二往返時間和處理時間乘數來決定傳送時間量測。該方法附加地包括基於傳送時間量測來決定距離上界。

A method for determining a distance upper bound by a verifier device is described. The method includes measuring a first round-trip time to receive a first response from a target device corresponding to a first message sent to the target device. The method also includes measuring a second round-trip time to receive a second response from the target device corresponding to a second message sent to the target device, the second response being delayed by a processing time multiplier. The method further includes determining a transit time measurement based on the first round-trip time, the second round-trip time and the processing time multiplier. The method additionally includes determining the distance upper bound based on the transit time measurement.

指定代表圖：



符號簡單說明：

- 102 . . . 驗證器設備
- 104 . . . 目標設備
- 106 . . . 距離
- 108 . . . 第一訊息
- 110 . . . 第一回應
- 112 . . . 第一往返時間
- 114 . . . 第二訊息
- 116 . . . 第二回應
- 118 . . . 第二往返時間
- 120 . . . 處理時間
- 122 . . . 處理時間乘數
- 124 . . . 時間量測
- 126 . . . 距離上界

201642613

【發明摘要】

【中文發明名稱】用於決定設備之間的距離的上界的系統和方法 $H04L\frac{1}{2}$ (2006.01)【英文發明名稱】SYSTEMS AND METHODS FOR DETERMINING AN
UPPER BOUND ON THE DISTANCE BETWEEN DEVICES

【中文】

描述了一種用於由驗證器設備決定距離上界的方法。該方法包括量測從目標設備接收對應於發送給該目標設備的第一訊息的第一回應的第一往返時間。該方法亦包括量測從目標設備接收對應於發送給該目標設備的第二訊息的第二回應的第二往返時間，第二回應經由處理時間乘數來延遲。該方法進一步包括基於第一往返時間、第二往返時間和處理時間乘數來決定傳送時間量測。該方法附加地包括基於傳送時間量測來決定距離上界。

【英文】

A method for determining a distance upper bound by a verifier device is described. The method includes measuring a first round-trip time to receive a first response from a target device corresponding to a first message sent to the target device. The method also includes measuring a second round-trip time to receive a second response from the target device corresponding to a second message sent to the target device, the second response being delayed by a processing time multiplier. The method further includes determining a transit time measurement based on the first round-trip time, the second round-trip time and the processing time multiplier.

The method additionally includes determining the distance upper bound based on the transit time measurement.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

1 0 2 驗 證 器 設 備

1 0 4 目 標 設 備

1 0 6 距 離

1 0 8 第 一 訊 息

1 1 0 第 一 回 應

1 1 2 第 一 往 返 時 間

1 1 4 第 二 訊 息

1 1 6 第 二 回 應

1 1 8 第 二 往 返 時 間

1 2 0 處 理 時 間

1 2 2 處 理 時 間 乘 數

1 2 4 時 間 量 測

1 2 6 距 離 上 界

【特徵化學式】

無

【發明說明書】

【中文發明名稱】用於決定設備之間的距離的上界的系統和方法

【英文發明名稱】SYSTEMS AND METHODS FOR DETERMINING AN UPPER BOUND ON THE DISTANCE BETWEEN DEVICES

【相關申請】

【0001】 本案與2015年5月29日提出申請的題為「SYSTEMS AND METHODS FOR DETERMINING AN UPPER BOUND ON THE DISTANCE BETWEEN DEVICES（用於決定設備之間的距離的上界的系統和方法）」的美國臨時專利申請S/N. 62/168,579相關並要求其優先權。

【技術領域】

【0002】 本案一般涉及通訊。更具體地，本案涉及用於準確地決定設備之間的距離的上界的系統和方法。

【先前技術】

【0003】 技術進步已導致越來越小且越來越強大的個人計算設備。例如，當前存在各種各樣的可攜式個人計算設備，包括無線計算設備，諸如各自較小、輕量且可被使用者易於攜帶的可攜式無線電話、個人數位助理（PDA），以及傳呼設備。更具體而言，例如，可攜式無線電話進一步包括經由無線網路來傳達語音和資料封包的蜂巢式電話。許多此種蜂巢式電話被製造成在計算能力方面具有相對較大增長，並且由此，正變得相當於小型個人電腦和掌上型PDA。進一步，此類設備正被製

造成使得能夠使用各種有線和無線通訊技術來進行通訊。例如，設備可執行蜂巢通訊、無線區域網路(WLAN)通訊、近場通訊(NFC)、光纖通訊等等。

【0004】 在一些情景中，驗證器設備與目標設備之間的通訊可依賴於設備之間的距離。例如，若知曉設備之間的距離的準確上界，則安全性可得到增強。可實現關於決定設備之間的距離上界的益處。

【發明內容】

【0005】 描述了一種用於由驗證器設備決定距離上界的方法。該方法包括量測從目標設備接收對應於發送給該目標設備的第一訊息的第一回應的第一往返時間。該方法亦包括量測從目標設備接收對應於發送給該目標設備的第二訊息的第二回應的第二往返時間，第二回應經由處理時間乘數延遲。該方法進一步包括基於第一往返時間、第二往返時間和處理時間乘數來決定傳送時間量測。該方法附加地包括基於傳送時間量測來決定距離上界。

【0006】 處理時間乘數可指示目標設備延遲對由驗證器設備發送的訊息進行回應的時間量。在接收到第二訊息之際，目標設備可在對第二訊息進行回應之前將處理時間縮放處理時間乘數。處理時間乘數可被驗證器設備和目標設備知曉。

【0007】 處理時間乘數可以是固定值。處理時間乘數可以基於被發送給目標設備的第二訊息的內容來決定。

【0008】傳送時間量測可根據 $T_f = (n \cdot T_{round,1} - T_{round,2}) / 2(n-1)$ 來決定，其中 T_f 是傳送時間， n 是處理時間乘數， $T_{round,1}$ 是第一往返時間並且 $T_{round,2}$ 是第二往返時間。

【0009】決定距離上界可包括將傳送時間量測乘以光速。距離上界可以是驗證器設備與目標設備之間的距離的上界。

【0010】距離上界可基於至少一個附加傳送時間量測來決定，其中目標設備根據處理時間乘數來延遲回應。處理時間乘數可包括值序列，該等值之一被應用於給定的往返時間量測。

【0011】該方法亦可包括量測至少一個附加往返時間。可使用該至少一個附加往返時間來決定至少一個附加傳送時間量測。可決定平均傳送時間量測。可基於平均傳送時間量測來決定距離上界。

【0012】驗證器設備可以是讀取器設備，並且目標設備可以是監聽設備。第一訊息和第二訊息可包括被發送給監聽設備的質詢訊息。

【0013】驗證器設備可以是監聽設備，並且目標設備可以是讀取器設備。第一訊息和第二訊息可包括對接收自讀取器設備的質詢的回應。

【0014】亦描述了一種被配置成決定距離上界的驗證器設備。驗證器設備包括處理器、與該處理器處於通訊的記憶體，以及儲存在該記憶體中的指令。該等指令可

被處理器執行以量測從目標設備接收對應於發送給該目標設備的第一訊息的第一回應的第一往返時間。該等指令亦可被執行以量測從目標設備接收對應於發送給該目標設備的第二訊息的第二回應的第二往返時間，第二回應經由處理時間乘數來延遲。該等指令進一步可被執行以基於第一往返時間、第二往返時間和處理時間乘數來決定傳送時間量測。該等指令附加地可被執行以基於傳送時間量測來決定距離上界。

【0015】亦描述了一種被配置成決定距離上界的裝備。該裝備包括用於量測從目標設備接收對應於發送給該目標設備的第一訊息的第一回應的第一往返時間的構件。該裝備亦包括用於量測從目標設備接收對應於發送給該目標設備的第二訊息的第二回應的第二往返時間的構件，第二回應經由處理時間乘數來延遲。該裝備進一步包括用於基於第一往返時間、第二往返時間和處理時間乘數來決定傳送時間量測的構件。該裝備附加地包括用於基於傳送時間量測來決定距離上界的構件。

【0016】亦描述了一種用於決定距離上界的電腦程式產品。該電腦程式產品包括其上具有指令的非瞬態電腦可讀取媒體。該等指令包括用於使驗證器設備量測從目標設備接收對應於發送給該目標設備的第一訊息的第一回應的第一往返時間的代碼。該等指令亦包括用於使驗證器設備量測從目標設備接收對應於發送給該目標設備的第二訊息的第二回應的第二往返時間的代碼，第二回

應經由處理時間乘數來延遲。該等指令進一步包括用於使驗證器設備基於第一往返時間、第二往返時間和處理時間乘數來決定傳送時間量測的代碼。該等指令附加地包括用於使驗證器設備基於傳送時間量測來決定距離上界的代碼。

【0017】亦描述了一種用於決定何時延遲發送回應以用於距離上界決定操作的方法。該方法包括由目標設備向驗證器設備發送對應於從驗證器設備接收到的第一訊息的第一回應。該方法亦包括由目標設備向驗證器設備發送經由處理時間乘數延遲的第二回應，第二回應對應於從驗證器設備接收到的第二訊息。驗證器設備基於第一往返時間、第二往返時間和處理時間乘數來決定距離上界。

【0018】亦描述了一種被配置成決定何時延遲發送回應以用於距離上界決定操作的目標設備。該目標設備包括處理器、與該處理器處於通訊的記憶體，以及儲存在該記憶體中的指令。該等指令可由處理器執行以向驗證器設備發送對應於從驗證器設備接收到的第一訊息的第一回應。該等指令亦可被執行以向驗證器設備發送經由處理時間乘數延遲的第二回應，第二回應對應於從驗證器設備接收到的第二訊息。驗證器設備基於第一往返時間、第二往返時間和處理時間乘數來決定距離上界。

【0019】亦描述了一種被配置成決定何時延遲發送回應以用於距離上界決定操作的裝備。該裝備包括用於向

驗證器設備發送對應於從驗證器設備接收到的第一訊息的第一回應的構件。該裝備亦包括用於向驗證器設備發送經由處理時間乘數延遲的第二回應的構件，第二回應對應於從驗證器設備接收到的第二訊息。驗證器設備基於第一往返時間、第二往返時間和處理時間乘數來決定距離上界。

【0020】亦描述了一種用於決定何時延遲發送回應以用於距離上界決定操作的電腦程式產品。該電腦程式產品包括其上具有指令的非瞬態電腦可讀取媒體。該等指令包括用於使目標設備向驗證器設備發送對應於從驗證器設備接收到的第一訊息的第一回應的代碼。該等指令亦包括用於使目標設備向驗證器設備發送經由處理時間乘數延遲的第二回應的代碼，第二回應對應於從驗證器設備接收到的第二訊息。驗證器設備基於第一往返時間、第二往返時間和處理時間乘數來決定距離上界。

【圖式簡單說明】

【0021】圖1是圖示用於決定設備之間的距離上界的通訊系統的一種配置的方塊圖；

【0022】圖2是圖示用於決定距離上界的方法的流程圖；

【0023】圖3是圖示用於決定距離上界的另一方法的流程圖；

【0024】圖4是圖示中繼攻擊的實例的方塊圖；

【0025】 圖5是圖示一種由驗證器設備計算傳送時間的辦法的序列圖；

【0026】 圖6是圖示根據所描述的系統和方法的一種用於計算傳送時間的辦法的序列圖；

【0027】 圖7是圖示根據所描述的系統和方法的用於計算傳送時間的另一辦法的序列圖；

【0028】 圖8是圖示根據所描述的系統和方法的免除距離哄騙的序列圖；及

【0029】 圖9圖示了可被包括在電子設備內的某些元件。

【實施方式】

【0030】 在某些情況下，設備能夠決定至另一設備的距離的上界是有利的。例如，查明建築物存取徽章實體上靠近門禁讀取器在安全性上下文中會是有益的。信號強度量測趨向於具有寬的變動，此使得難以實現準確的距離決定，並且經由操縱發射器，惡意設備假裝成比實際間隔更靠近是有可能的。

【0031】 根據本文所描述的系統和方法，驗證器設備可使用信號的往返延遲來量測信號的傳送時間。根據傳送時間量測，驗證器設備可決定與目標設備的距離的上界。由於沒有什麼能比光速行進得更快，因此信號（例如，無線電信號）能可靠地被用來施加與目標設備的距離的上界。目標設備可能更靠近，但其無法更遠離。

【0032】 應當注意，一些通訊設備可以無線地通訊及/或可以使用有線連接或鏈路來通訊。例如，一些通訊設備可以使用乙太網路協定來與其他設備通訊。本文揭示的系統和方法可以應用於無線地通訊及/或使用有線連接或鏈路來通訊的通訊設備。在一種配置中，本文所揭示的系統和方法可以應用於使用近場通訊（NFC）來與另一設備進行通訊的通訊設備。

【0033】 下文結合附圖闡述的詳細描述意欲作為對本案的示例性實現的描述，而非意欲代表可在其中實踐本案的僅有實現。貫穿本描述使用的術語「示例性」意指「用作示例、實例或圖示」，並且不應當一定要解釋成優於或勝過其他示例性實現。本詳細描述包括具體細節以提供對本案的示例性實現的透徹理解。在某些實例中，某些設備以方塊圖形式圖示。

【0034】 儘管為使解釋簡單化將該等方法體系圖示並描述為一系列動作，但是應當理解該等方法體系不受動作的次序所限，因為根據一或多個態樣，一些動作可按不同次序發生及/或與來自本文中圖示和描述的其他動作併發地發生。例如，本領域技藝人士將理解和領會，方法體系可被替換地表示為一系列相互關聯的狀態或事件，諸如在狀態圖中一般。不僅如此，並非所有圖示的動作皆為實現根據一或多個態樣的方法體系所必要的。

【0035】 現在參照附圖來描述各種配置，其中相同的元件符號可指示功能上類似的元件。本文一般性地描述

的和在附圖中圖示的系統和方法可以廣泛地以各種不同配置來安排和設計。因此，對如附圖中表示的若干配置的以下更詳細的描述無意限定所要求保護的範圍，而是僅僅代表該等系統和方法。

【0036】 圖1是圖示用於決定設備之間的距離上界126的通訊系統100的一種配置的方塊圖。通訊系統100可包括驗證器設備102和目標設備104。驗證器設備102或目標設備104亦可被稱為電子通訊設備、行動設備、行動站、用戶站、客戶端、客戶站、使用者裝備（UE）、遠端站、存取終端、行動終端、終端、使用者終端、用戶單元等。設備的實例包括膝上型或桌上型電腦、讀卡器、蜂巢式電話、智慧型電話、無線數據機、電子閱讀器、平板設備、遊戲系統等。該等設備中的一些可根據一或多個工業標準來操作。

【0037】 驗證器設備102和目標設備104可使用一或多個通訊技術來通訊。該等通訊技術可包括有線通訊技術和無線通訊技術。

【0038】 驗證器設備102和目標設備104可使用以光速操作的一或多個通訊技術來通訊。該等技術可包括但不限於射頻（RF）、可見光（「LiFi」）、微波，以及紅外通訊。

【0039】 在一種配置中，驗證器設備102和目標設備104可使用感應耦合通訊來進行通訊。在感應耦合通訊的實現中，驗證器設備102和目標設備104可使用近場

通訊（NFC）。在另一實現中，驗證器設備102和目標設備104可使用射頻標識（RFID）。

【0040】 在另一配置中，驗證器設備102和目標設備104可根據某些行業標準來操作，諸如第三代夥伴項目（3GPP）長期進化（LTE）標準。通訊設備可遵循的標準的其他實例包括電氣和電子工程師協會（IEEE）802.11a、802.11b、802.11g、802.11n及/或802.11ac（例如，無線保真或「Wi-Fi」）標準，藍芽，IEEE 802.16（例如，全球互通微波存取性或「WiMAX」）標準，分碼多工存取（CDMA）2000 1x（本文稱為「1x」，亦可被稱為IS-2000或1xRTT）標準，進化資料最佳化（EVDO）標準，臨時標準95（IS-95），高資料率（HDR），高速率封包資料（HRPD），進化型高速率封包資料（eHRPD），無線電標準，以及其他。WWAN亦可包括無線都會區網路（WMAN）標準和高速下行鏈路封包存取（HSDPA）標準。儘管本文中所揭示的一些系統和方法可能是根據一或多個標準來描述的，但此不應限制本案的範圍，因為該等系統和方法可適用於許多系統及/或標準。

【0041】 驗證器設備102和目標設備104可被分開一距離106。在某些情況下，能夠決定從驗證器設備102到目標設備104的距離上界126會是有利的。在嘗試驗證正被呈現給一設備（亦即，驗證器設備102）以進行

交易的另一設備（亦即，目標設備104）實體上靠近以便抵制中繼攻擊時，此變得尤為重要。

【0042】 正常安全性協定（諸如用於建築物存取或支付）僅驗證正被呈現的設備能夠正確地對一或多個質詢進行回應。然而，有可能經由將質詢中繼給真實設備、隨後將回應中繼回攻擊下的設備來規避該驗證。在考慮到將會需要的全部是具有執行該中繼的惡意程式的一對設備（例如，智慧型電話）時，攻擊的潛在數目是龐大的。圖4圖示了中繼攻擊的實例。

【0043】 若攻擊下的設備（例如，驗證器設備102）能夠決定正被呈現的設備（例如，目標設備104）實體上靠近，則此種類型的攻擊變得困難得多。已提議了數種辦法，但該等辦法皆遭受缺陷。在一種辦法中，可基於信號強度量測來決定距離。然而，信號強度量測趨向於具有寬的變動，此使得難以實現準確的距離決定。此外，經由操縱發射器，有可能假裝比實際間隔更靠近。

【0044】 另一種辦法是使用信號的往返延遲（亦即，傳送時間）。如本文所使用的，「傳送時間」代表信號在兩點之間行進的時間量。例如，由驗證器設備102向目標設備104發送的信號的傳送時間是在驗證器設備102傳送該信號之際該信號抵達目標設備104的時間量。傳送時間亦可被稱為傳送時間、飛行時間、時間間隔或其他等同術語。

【0045】 由於沒有什麼能比光速行進得更快，因此信號（例如，無線電或光信號）能可靠地被用來對從驗證器設備102到目標設備104的距離106施加上界（亦即，距離上界126）。目標設備104可能更靠近，但其無法比距離上界126更遠離。

【0046】 該辦法的主要缺陷在於通訊傳送時間是極短的，尤其在嘗試建立到人類尺寸的定位時。即使1奈秒（ns）的往返行程亦對應於15釐米（cm）的間隔。此意味著遠端設備中的任何處理延遲可快速地壓倒傳送時間並導致距離上界126量測的巨大不確定性。圖5圖示該情景。

【0047】 本文所描述的系統和方法允許在執行距離上界126決定操作時消除遠端設備中的處理延遲的影響。此可允許更為準確的距離量測。

【0048】 在一種配置中，驗證器設備102可以是讀取器/寫入器，並且目標設備104可以是監聽設備。例如，驗證器設備102可以是NFC讀取器/寫入器，並且目標設備104可以是NFC卡。

【0049】 驗證器設備102可部分地基於經由處理時間乘數122延遲的往返時間量測來決定距離上界126。處理時間乘數122指示目標設備104延遲對由驗證器設備102發送的訊息進行回應的時間量。

【0050】 驗證器設備102可量測第一往返時間112。第一往返時間112可包括用於向目標設備104發送第一

訊息 108 的傳送時間、目標設備 104 作出的處理時間 120，以及從目標設備 104 接收第一回應 110 的傳送時間。

【0051】處理時間 120 可以是目標設備 104 處理從驗證器設備 102 接收到的訊息所花費的時間量。處理時間 120 亦可被稱為處理延遲。例如，若第一訊息 108 是質詢，則處理時間 120 是目標設備 104 處理質詢、產生回應和發送回應所花費的時間量。第一往返時間 112 可根據式 (1) 來表達。

$$T_{round,1} = T_{proc} + 2 \cdot T_f \quad (1)$$

【0052】在式 (1) 中， $T_{round,1}$ 是第一往返時間 112， T_{proc} 是目標設備 104 處理第一訊息 108 的處理時間 120，並且 T_f 是傳送時間，該傳送時間因驗證器設備 102 發送第一訊息 108 和接收第一回應 110 而被乘以 2。

【0053】在第二訊息/回應交換中，目標設備 104 可根據處理時間乘數 122 來延遲回應。在該交換中，驗證器設備 102 可量測第二往返時間 118，第二往返時間 118 包括用於向目標設備 104 發送第二訊息 114 的傳送時間、目標設備 104 應用的處理時間乘數 122 (n)，以及從目標設備 104 接收第二回應 116 的傳送時間。

【0054】處理時間乘數 122 指示目標設備 104 延遲對由驗證器設備 102 發送的訊息進行回應的時間量。在接收到第二訊息 114 之際，目標設備 104 可在對第二訊息

114 進行回應之前將處理時間 120 縮放處理時間乘數 122。第二往返時間 118 可根據式 (2) 來表達。

$$T_{round,n} = n \cdot T_{proc} + 2 \cdot T_f \quad (2)$$

【0055】 在式 (2) 中， $T_{round,n}$ 是第二往返時間 118，並且 n 是目標設備 104 處理第二訊息 114 的處理時間乘數 122。再一次，傳送時間 T_f 因驗證器設備 102 發送第二訊息 114 和接收第二回應 116 而被乘以 2。

【0056】 驗證器設備 102 可基於第一往返時間 112、第二往返時間 118 和處理時間乘數 122 (n) 來決定傳送時間量測 124。由於處理時間乘數 122 (n) 表示供目標設備 104 (例如，卡) 在其處理時間 120 延遲中使用的縮放因數，因此傳送時間量測 124 T_f 可以根據下式來決定。將第一往返時間 112 乘以處理時間乘數 122 (n) 得到

$$n \cdot T_{round,1} = n \cdot T_{proc} + 2n \cdot T_f \quad (3)$$

$$\begin{aligned} n \cdot T_{round,1} - T_{round,n} &= n \cdot T_{proc} + 2n \cdot T_f - n \cdot T_{proc} - 2 \cdot T_f \\ &= 2n \cdot T_f - 2 \cdot T_f \\ &= 2T_f(n-1) \end{aligned} \quad (4)$$

$$T_f = \frac{n \cdot T_{round,1} - T_{round,n}}{2(n-1)} \quad (5)$$

【0057】 應注意，根據式 (5)，驗證器設備 102 (例如，讀取器/寫入器) 可獨立於目標設備 104 的實際處理時間 120 來計算傳送時間。換言之，驗證器設備 102 無需知曉目標設備 104 的處理時間 120 來決定傳送時間量測 124。儘管目標設備 104 必須能夠準確地縮放其處理

時間 120，但該辦法不依賴於此處理時間 120 較短。圖 6 圖示了處理時間乘數 122 (n) 為 2 的實例。

【0058】 驗證器設備 102 可基於傳送時間量測 124 來決定驗證器設備 102 與目標設備 104 之間的距離上界 126。一旦傳送時間量測 124 T_f 被決定為期望的準確度，驗證器 102 就可經由將傳送時間量測 124 乘以光速 (c) 來決定距離上界 126。距離上界 126 可表達為 $T_f \cdot c$ 。

【0059】 該距離上界 126 可以是驗證器設備 102 與目標設備 104 之間的距離 106 (或間隔) 的量測的上界。因此，驗證器設備 102 和目標設備 104 可以比距離上界 126 更靠近，但驗證器設備 102 和目標設備 104 不能更遠離。

【0060】 應注意，根據式 (1)–(5)，假定傳出時間和傳回時間相等。因此， $2 \cdot T_f$ 是總傳送時間。若目標設備 104 的處理時間 120 較大，則有可能驗證器設備 102 和目標設備 104 可能已相對於彼此移動。假定實際的處理時間 120，該場景對於正被使用者握持的設備將不會是實際問題。然而，即使在目標設備 104 處理時間 120 很慢並且驗證器設備 102 與目標設備 104 之間的距離 106 快速改變的極端情形中，驗證器設備 102 亦將決定設備間隔的平均。在該情形中，時間量測將圖示距離 106 在改變。此可用作拒絕與目標設備 104 進行通訊的另一準則。

【0061】亦應注意，經由將往返時間量測重複多次，處理延遲的微小波動可被平均掉，由此進一步改進了傳送時間量測124的準確性。因此，在一實現中，驗證器設備102可基於至少一個附加傳送時間量測124來決定距離上界126，其中目標設備124根據處理時間乘數122來延遲其回應。

【0062】在該實現中，驗證器設備102可量測接收來自目標設備104的回應的至少一個附加往返時間。來自目標設備104的回應可以或者可以不經由處理時間乘數122來延遲。此外，一或多個往返時間量測中所使用的處理時間乘數122可以是相同值，或者可以是不同值。換言之，在該實現中，處理時間乘數122可以是被應用於給定往返時間量測的值序列。例如，在一個往返時間量測中，處理時間乘數122可以為2，而在另一往返時間量測中，處理時間乘數122可以為3。

【0063】驗證器設備102隨後可使用至少一個附加往返時間來決定至少一個附加傳送時間量測124。對於每個往返時間量測，驗證器設備102可根據式(5)來決定傳送時間量測124。驗證器設備102可使用多個傳送時間量測124中的每一個來決定平均傳送時間量測124。驗證器設備102可經由將平均傳送時間量測124乘以光速來決定距離上界126。

【0064】處理時間乘數122可以被驗證器設備102和目標設備104知曉，但不被其他設備知曉。用於決定應

用於給定回應的處理時間乘數 1 2 2 的方式可被選擇以適應於特定應用的需求。在一個實現中，對於距離上界 1 2 6 量測的簡單的非安全建立，可使用處理時間乘數 1 2 2 (n) 的固定序列，諸如 2 - 2 - 2 - 2 或 2 - 3 - 4 - 2 - 3 - 4。在期望的情況下，附加的單處理延遲回應（亦即， $n = 1$ ）可被包括在任何預定位置處。

【0 0 6 5】 在另一實現中，可經由取決於由驗證器設備 1 0 2 發送的訊息的內容來產生處理時間乘數 1 2 2 (n) 的方式引入更多的複雜化。例如，若此是單個位元，則 1 可遞增經商定的處理時間乘數 1 2 2 (n)，並且 0 可遞減 n 。亦可實現此兩種機制的組合。

【0 0 6 6】 在又一實現中，給定充足數目的往返時間量測，即使處理時間乘數 1 2 2 (n) 的序列不是決定性的，驗證器設備 1 0 2 亦可決定傳送時間。驗證器設備 1 0 2 知曉對於給定處理時間乘數 1 2 2 (n)，式 (2) 提供了 $T_{round,n} = n \cdot T_{proc} + 2 \cdot T_f$ 。因此，驗證器設備 1 0 2 可將時間陣列與處理時間乘數 1 2 2 (n) 的各個可能值進行比對。

【0 0 6 7】 在一些情景中，被呈現以供存取或支付的設備自身是智慧設備。例如，智慧型電話可以是接收來自讀取器設備的質詢的監聽設備。監聽設備亦驗證與讀取器設備的距離會是有益的。在該情形中，角色可被反轉，並且監聽設備可充當驗證器設備 1 0 2，而讀取器設備可充當目標設備 1 0 4。此可經由以上提供的辦法的簡單擴展來完成，如圖 7 中所示。作為實例，監聽設備（例如，

智慧型電話) 的存取或支付應用可要求關於潛在讀取器在實體上靠近的檢查，隨後其將允許其自己被存取。

【0068】 監聽設備決定與讀取器設備的距離上界126的機制可以與用於反方向的機制相同。換言之，監聽設備可根據式(5)來決定傳送時間。與讀取器設備的距離上界126可經由將傳送時間乘以光速來決定。

【0069】 惡意設備經由調整其處理時間來假裝比其實際上更靠近來擊敗該辦法是極為困難的。此是因為為了使回應在正確時間抵達驗證器設備102(例如，讀取器/寫入器)，縮放處理時間並不是簡單地加倍。由於惡意設備不知曉與驗證器設備102的距離106，其不知曉 T_f ，因此其不能決定其需要用來假裝處於較短距離處所必需的處理時間120或處理時間乘數122。該場景結合圖8來描述。

【0070】 圖2是圖示用於決定距離上界126的方法200的流程圖。方法200可由與目標設備104處於通訊的驗證器設備102執行。在一種配置中，驗證器設備102可以是讀取器設備(例如，讀取器/寫入器)，並且目標設備104可以是監聽設備(例如，卡)。在另一配置中，驗證器設備102可以是監聽設備(例如，卡)，並且目標設備104可以是讀取器設備(例如，讀取器/寫入器)。在一實現中，驗證器設備102可以是NFC設備。驗證器設備102可使用NFC操作來與目標設備104通訊。

【0071】 驗證器設備102可量測(202)從目標設備104接收對應於發送給目標設備104的第一訊息108的第一回應110的第一往返時間112。第一往返時間112包括用於向目標設備104發送第一訊息108的傳送時間、目標設備104作出的處理時間120，以及從目標設備104接收第一回應110的傳送時間。第一往返時間112可根據式(1)來表達。

【0072】 在驗證器設備102是讀取器設備(例如，讀取器/寫入器)的配置中，第一訊息108可以是驗證器設備102向目標設備104發送的質詢訊息。在該配置中，驗證器設備102可量測(202)從目標設備104接收對質詢的回應所花費的時間量。

【0073】 在驗證器設備102是監聽設備(例如，卡)的配置中，第一訊息108可以是對質詢訊息的回應。驗證器設備102可向目標設備104發送回應。在該配置中，驗證器設備102可量測(202)從目標設備104接收另一質詢訊息所花費的時間量。

【0074】 驗證器設備102可量測(204)從目標設備104接收對應於發送給目標設備104的第二訊息114的第二回應116的第二往返時間118，第二回應經由處理時間乘數122來延遲。處理時間乘數122指示目標設備104延遲對由驗證器設備102發送的訊息進行回應的時間量。

【0075】 在接收到第二訊息114之際，目標設備104可在對第二訊息114進行回應之前將處理時間120縮放處理時間乘數122。第二往返時間118可根據式(2)來表達。第二往返時間118包括用於向目標設備104發送第二訊息114的傳送時間、經由處理時間乘數122縮放的處理時間120，以及從目標設備104接收第二回應116的傳送時間。

【0076】 在一個實現中，處理時間乘數122是固定值。在另一實現中，處理時間乘數122基於被發送給目標設備104的第二訊息114的內容來決定。

【0077】 在驗證器設備102是讀取器設備（例如，讀取器/寫入器）的配置中，第二訊息114可以是驗證器設備102向目標設備104發送的第二質詢訊息。在該配置中，驗證器設備102可量測(204)從目標設備104接收對該第二質詢的回應所花費的時間量。

【0078】 在驗證器設備102是監聽設備（例如，卡）的配置中，第二訊息114可以是對第二質詢訊息的第二回應。驗證器設備102可向目標設備104發送第二回應。在該配置中，驗證器設備102可量測(204)目標設備104發送另一質詢訊息所花費的時間量。

【0079】 驗證器設備102可基於第一往返時間112、第二往返時間118和處理時間乘數122來決定(206)傳送時間量測124。此可根據式(5)來完成。

【0080】 驗證器設備102可基於傳送時間量測124來決定(208)距離上界126。在一實現中，驗證器設備102可將傳送時間量測124乘以光速以決定距離上界126。

【0081】 應注意，所描述的系統和方法亦可按比光速慢的通訊速度來實現。然而，此可引入弱點。例如，考慮超聲波的使用。此比光慢許多，因此惡意設備將資訊轉換成無線電/光形式，並在相同時間量中將其在遠得多的距離上進行傳送將是可能的。因此，距離上界126對於小於光速的速度可能較不可靠。

【0082】 圖3是圖示用於決定何時延遲發送回應以用於距離上界126決定操作的另一方法300的流程圖。方法300可由與驗證器設備102處於通訊的目標設備104執行。在一實現中，目標設備104可以是NFC設備。目標設備104可使用NFC操作來與驗證器設備102通訊。

【0083】 在一配置中，目標設備104可以是監聽設備(例如，卡)，並且驗證器設備102可以是讀取器設備(例如，讀取器/寫入器)。在另一配置中，目標設備102可以是讀取器設備(例如，讀取器/寫入器)，並且目標設備104可以是監聽設備(例如，卡)。

【0084】 目標設備104可向驗證器設備102發送(302)對應於從驗證器設備102接收到的第一訊息108的第一回應110。第一訊息108可以作為由驗證器設備102進行的第一往返時間112量測操作的一部分來

接收，如結合圖1所描述的。在處理接收到的第一訊息108之後，目標設備104可發送(302)第一回應110。處理時間120可以是目標設備104處理從驗證器設備102接收到的第一訊息108所花費的時間量。

【0085】 目標設備104可向驗證器設備102發送(304)經由處理時間乘數122延遲的第二回應116。第二回應116可對應於從驗證器設備102接收到的第二訊息114。第二訊息114可以作為由驗證器設備102進行的第二往返時間118量測操作的一部分來接收，如結合圖1所描述的。

【0086】 處理時間乘數122可指示目標設備104延遲對由驗證器設備102發送的訊息進行回應的時間量。在接收到第二訊息114之際，目標設備104可在對第二訊息114進行回應之前將處理時間120縮放處理時間乘數122。

【0087】 驗證器設備102可基於第一往返時間112、第二往返時間118和處理時間乘數122來決定距離上界126。此可以如結合圖1所描述的一般來完成。

【0088】 圖4是圖示中繼攻擊的實例的方塊圖。第一惡意設備428a可緊鄰驗證器設備402。第二惡意設備428b可緊鄰目標設備404。

【0089】 驗證器設備402可以是讀取器/寫入器設備。例如，驗證器設備102是銷售點(POS)終端。目標設備404可以是監聽設備。例如，目標設備404可以

是被用來在讀取器/寫入器（亦即，POS終端）處進行支付的非接觸式支付卡。第一惡意設備428a和第二惡意設備428b可以是智慧型電話。

【0090】 驗證器設備402和目標設備404可被分開足以使其無法彼此直接通訊的距離。例如，若驗證器設備402和目標設備404使用NFC或RFID進行通訊，則通訊可被限於數釐米。

【0091】 在該實例中，目標設備404可被用於建築物存取或支付。目標設備404所使用的安全性協定僅可驗證正被呈現的設備能夠正確地對數個質詢進行回應。第一惡意設備428a和第二惡意設備428b可規避該等安全性協定。

【0092】 第一惡意設備428a可將來自驗證器設備402的質詢中繼到第二惡意設備428b。第二惡意設備428b可隨後向目標設備404中繼質詢。目標設備404可經由將回應發送回（經由第一惡意設備428a和第二惡意設備428b）攻擊下的驗證器設備402來對該質詢進行回應。

【0093】 該攻擊使用支付卡的真實加密功能和真實授權。此回到驗證器設備402並且作出欺詐交易。就驗證器設備402而言，其發送質詢並且其接收到正確的回應，此滿足了安全性協定。

【0094】 若攻擊下的設備（例如，驗證器設備402）能夠決定正被呈現的設備（例如，目標設備404）實體

上靠近，則此種類型的攻擊變得困難得多。因此，驗證器設備 402 可決定距離上界 126，如結合圖 1 所描述的。若距離上界 126 指示目標設備 404 比所允許距離更遠離，則驗證器設備 402 可拒絕授權交易。

【0095】圖 5 是圖示驗證器設備 502 計算傳送時間 530 的一種辦法的序列圖。在該實例中，驗證器設備 502（例如，讀取器/寫入器）與目標設備 504（例如，卡）進行通訊。驗證器設備 502 可以根據圖 1 的驗證器設備 102 來實現。目標設備 504 可以根據圖 1 的目標設備 104 來實現。

【0096】驗證器設備 502 可向目標設備 504 發送（501）質詢。信號在驗證器設備 502 與目標設備 504 之間行進的時間量是傳送時間 530 (T_f) 。因此，質詢抵達目標設備 504 的時間量是傳送時間 530 a (T_f) 。

【0097】目標設備 504 可處理（503）質詢。處理質詢和產生回應的時間量是處理時間 520 (T_{proc}) 。目標設備 504 可將回應發送（505）回驗證器設備 502。回應抵達驗證器設備 502 的時間量是傳送時間 530 b (T_f) 。假定驗證器設備 502 與目標設備 504 之間的距離尚未改變，則質詢的傳送時間 530 a (T_f) 和回應的傳送時間 530 b (T_f) 相同。

【0098】質詢/回應交換的往返時間 512 $(T_{round,1})$ 可根據上式（1）來表達。在該實例中，驗證器設備 502 可量測質詢/回應交換的從質詢被發送的時間到回應被接收

的 時 間 的 往 返 時 間 5 1 2 ($T_{round,1}$)。換 言 之， $T_{round,1} = T_{proc} + 2 \cdot T_f$ 。然 而，由 於 驗 證 器 設 備 5 0 2 通 常 不 知 曉 處 理 時 間 5 2 0 (T_{proc})，因 此 驗 證 器 設 備 5 0 2 無 法 準 確 地 決 定 傳 送 時 間 5 3 0 (T_f)，以 及 由 此 與 目 標 設 備 5 0 4 的 距 離。

【0099】圖 6 是 圖 示 根 據 所 描 述 的 系 統 和 方 法 的 用 於 計 算 傳 送 時 間 6 3 0 的 一 種 辦 法 的 序 列 圖。在 該 實 例 中，驗 證 器 設 備 6 0 2 與 目 標 設 備 6 0 4 進 行 通 訊。驗 證 器 設 備 6 0 2 可 以 根 據 圖 1 的 驗 證 器 設 備 1 0 2 來 實 現。目 標 設 備 6 0 4 可 以 根 據 圖 1 的 目 標 設 備 1 0 4 來 實 現。驗 證 器 設 備 6 0 2 可 以 是 讀 取 器 設 備（例 如，讀 取 器 / 寫 入 器），目 標 設 備 6 0 4 可 以 是 監 聽 設 備（例 如，卡）。

【0100】驗 證 器 設 備 6 0 2 可 量 測 第 一 質 詢（例 如，第 一 訊 息 1 0 8）和 第 一 回 應 1 1 0 的 交 換 的 第 一 往 返 時 間 6 1 2 ($T_{round,1}$)。驗 證 器 設 備 6 0 2 可 向 目 標 設 備 6 0 4 發 送（6 0 1）第 一 質 詢。第 一 訊 息 1 0 8 抵 達 目 標 設 備 6 0 4 的 時 間 量 是 傳 送 時 間 6 3 0 a (T_f)。

【0101】目 標 設 備 6 0 4 可 開 始 處 理（6 0 3）質 詢。處 理 質 詢 和 產 生 回 應 的 時 間 量 是 處 理 時 間 6 2 0 (T_{proc})。目 標 設 備 6 0 4 可 將 第 一 回 應 發 送（6 0 5）回 驗 證 器 設 備 6 0 2。第 一 回 應 1 1 0 抵 達 驗 證 器 設 備 6 0 2 的 時 間 量 是 傳 送 時 間 6 3 0 b (T_f)。

【0102】驗 證 器 設 備 6 0 2 可 量 測 第 二 質 詢（例 如，第 二 訊 息 1 1 4）和 第 二 回 應 1 1 6 的 交 換 的 第 二 往 返 時 間 6 1 8 ($T_{round,2}$)。驗 證 器 設 備 6 0 2 可 向 目 標 設 備 6 0 4 發 送

(607) 第二質詢。第二質詢抵達目標設備604的時間量是傳送時間630c (T_f)。

【0103】 目標設備604可基於處理時間乘數122 (n) 來延遲(609)處理第二訊息114。在該實例中，處理時間乘數122 (n) 等於2。因此，目標設備604在對第二訊息114進行回應之前將處理時間620縮放倍數2。換言之，目標設備604將其回應延遲達其內部處理延遲的兩倍。

【0104】 在該處理延遲之後，目標設備604可向驗證器設備602發送(611)第二回應116。第二回應116抵達驗證器設備602的時間量是傳送時間630d (T_f)。

【0105】 再一次，假定驗證器設備602與目標設備604之間的距離尚未改變，則傳送時間630a-d (T_f)相同。

【0106】 驗證器設備602現在具有兩個不同的往返時間。驗證器設備602可根據式(5)來決定傳送時間量測124。在該情形中，處理時間乘數122 (n) 為2。應注意，傳送時間量測124不要求驗證器設備602知曉目標設備604的實際處理實際620。

【0107】 在該實例中， $T_{round,1} = T_{proc} + 2 \cdot T_f$ 且 $T_{round,2} = 2 \cdot T_{proc} + 2 \cdot T_f$ 。因此 $2 \cdot T_{round,1} = 2 \cdot T_{proc} + 4 \cdot T_f$ 。因此， $2 \cdot T_{round,1} - T_{round,2} = 2T_f$ 。此提供了 $T_f = (2 \cdot T_{round,1} - T_{round,2}) / 2$ 。

【0108】 圖7是圖示根據所描述的系統和方法的用於計算傳送時間730的另一辦法的序列圖。在該實例中，

驗證器設備 702 與目標設備 704 進行通訊。驗證器設備 702 可以根據圖 1 的驗證器設備 102 來實現。目標設備 704 可以根據圖 1 的目標設備 104 來實現。

【0109】 在該辦法中，驗證器設備 702 是監聽設備。例如，驗證器設備 702 可以是智慧型電話或另一智慧監聽設備。目標設備 704 是讀取器設備（例如，讀取器/寫入器）。

【0110】 目標設備 704 可發送（701）第一質詢。第一質詢抵達驗證器設備 702 的時間量是傳送時間 730 a (T_f)。

【0111】 驗證器設備 702 可發送（703）對第一質詢的第一回應。驗證器設備 702 可量測第一回應和第二質詢的交換的第一往返時間 712 ($T_{round,1}$)。第一回應抵達目標設備 704 的時間量是傳送時間 730 b (T_f)。

【0112】 目標設備 704 可開始處理（705）回應。讀取器/寫入器處理回應和產生第二質詢的時間量是處理時間 720 ($T_{proc,rw}$)。目標設備 704 可將第二質詢發送（707）回驗證器設備 702。第二質詢抵達驗證器設備 702 的時間量是傳送時間 730 c (T_f)。

【0113】 驗證器設備 702 可發送（709）對第二質詢的第二回應。驗證器設備 702 可量測第二回應和第三質詢的交換的第二往返時間 718 ($T_{round,2}$)。第二回應抵達目標設備 704 的時間量是傳送時間 730 d (T_f)。

【0114】 目標設備704可基於處理時間乘數122 (n)來延遲(711)處理第二回應。在該實例中，處理時間乘數122 (n)等於2。因此，目標設備704在發送(713)第三質詢之前將處理時間720縮放倍數2。在該辦法中，讀取器/寫入器可具有以下約束：其以其處理延遲的固定倍數來發送質詢。第三質詢抵達驗證器設備702的時間量是傳送時間730e (T_f)。

【0115】 再一次，假定驗證器設備702與目標設備704之間的距離尚未改變，則傳送時間730a-e (T_f)相同。驗證器設備702現在具有兩個不同的往返時間。驗證器設備702可根據式(5)來決定傳送時間量測124。

【0116】 重要的是，若使用此類對稱性辦法，則從交換的開始作出定時量測。如以上所提及的，惡意設備328在其知曉正被交換的信號的傳送時間730的情況下可假裝比其的靠近程度更靠近。如圖7圖示的，監聽設備(亦即，驗證器設備702)必須在其能計算傳送時間730之前發送其第二回應116，因此讀取器/寫入器仍可認出聲稱比其實際上更靠近的設備。

【0117】 圖8是圖示根據所描述的系統和方法的免除距離哄騙的序列圖。在該實例中，驗證器設備802(例如，讀取器/寫入器)與惡意設備828進行通訊。驗證器設備802可以根據圖1的驗證器設備102來實現。惡意設備828可與驗證器設備802分隔開實際距離806a，但可

嘗試指示其處於比實際距離 806 a 更靠近的聲稱距離 806 b。因此，惡意設備 828 正聲稱比其實際上更靠近。

【0118】 在該實例中，處理時間乘數 122 (n) 為 2。因此，聲稱距離 806 b 的預計處理時間 820 延遲為處理時間 820 的兩倍。

【0119】 驗證器設備 802 可向惡意設備 828 發送 (801) 第一訊息 108 (例如，質詢)。第一訊息 108 抵達惡意設備 828 的時間量是傳送時間 830 a (T_f)。

【0120】 惡意設備 828 可開始處理 (803) 第一質詢。為了嘗試哄騙聲稱距離 806 b，惡意設備 828 可使用偽造處理時間 832 ($T_{fake,1}$)。偽造處理時間 832 可以是任何值。惡意設備 828 可將第一回應發送 (805) 回驗證器設備 802。第一回應抵達驗證器設備 802 的時間量是傳送時間 830 b (T_f)。

【0121】 驗證器設備 802 可向惡意設備 828 發送 (807) 第二質詢。第二質詢抵達惡意設備 828 的時間量是傳送時間 830 c (T_f)。

【0122】 惡意設備 828 可在發送 (811) 第二回應之前經由應用偽造處理延遲 834 ($T_{fake,2}$) 來延遲處理 (809) 第二質詢以嘗試哄騙聲稱距離 806 b。第二回應 116 抵達驗證器設備 802 的時間量是傳送時間 830 d (T_f)。

【0123】 即使惡意設備 828 知曉或者猜到處理時間乘數 122 (n) 來計算處理延遲 834 ($T_{fake,2}$)，惡意設備 828 亦將需要知曉對於聲稱距離 806 b 而言到驗證器設備

802 的傳送時間 830。如所提及的，處理時間乘數 122 (n) 等於 2。然而，惡意設備 828 不能經由將其偽造處理時間 832 加倍來哄騙聲稱距離 806b，此是因為其必須縮放的量不是因數 2。此是因為往返行程現在在實際距離 806a 處較長。惡意設備 828 將必須知曉其離驗證器設備 802 有多遠以能夠縮放其偽造處理時間 832，並且其無法使用所描述的系統和方法來做到此點。

【0124】 因此，驗證器設備 802 可偵測到惡意設備 828 作出的攻擊。若惡意設備 828 的確使其偽造處理時間 832 加倍，則驗證器設備 802 將看到聲稱距離 806b 與傳送時間 830 之間的關係不正確。

【0125】 圖 9 圖示了可被包括在電子設備 936 內的某些元件。電子設備 936 可以是存取終端、行動站、使用者裝備 (UE) 等。例如，電子設備 936 可以是圖 1 的驗證器設備 102 或目標設備 104。

【0126】 電子設備 936 包括處理器 903。處理器 903 可以是通用單晶片或多晶片微處理器 (例如，高級 RISC (精簡指令集電腦) 機器 (ARM))、專用微處理器 (例如，數位訊號處理器 (DSP))、微控制器、可程式設計閘陣列等。處理器 903 可被稱為中央處理單元 (CPU)。儘管在圖 9 的電子設備 936 中僅圖示單個處理器 903，但在替換配置中，可以使用處理器的組合 (例如，ARM 和 DSP)。

【0127】 電子設備936亦包括與處理器處於電子通訊的記憶體905（亦即，處理器可從記憶體讀資訊及/或向記憶體寫資訊）。記憶體905可以是能夠儲存電子資訊的任何電子元件。記憶體905可被配置為隨機存取記憶體（RAM）、唯讀記憶體（ROM）、磁碟儲存媒體、光學儲存媒體、RAM中的快閃記憶體設備、隨處理器包括的板載記憶體、EPROM記憶體、EEPROM記憶體、暫存器等等，包括其組合。

【0128】 資料907a和指令909a可被儲存在記憶體905中。指令可包括一或多個程式、常式、子常式、函數、程序、代碼等。指令可包括單條電腦可讀取語句或許多電腦可讀取語句。指令909a可由處理器903執行以實現本文揭示的方法。執行指令909a可涉及使用儲存在記憶體905中的資料907a。當處理器903執行指令909時，指令909b的各個部分可被載入到處理器903上，並且資料907b的各個片段可被載入到處理器903上。

【0129】 電子設備936亦可包括發射器911和接收器913，以允許經由天線917向電子設備936傳送信號以及從其接收信號。發射器911和接收器913可被合稱為收發機915。電子設備936亦可包括（未圖示的）多個發射器、多個天線、多個接收器，及/或多個收發機。

【0130】 電子設備936可包括數位訊號處理器（DSP）921。電子設備936亦可包括通訊介面923。通訊介面923可允許使用者能與電子設備936互動。

【0131】 電子設備936的各種元件可由一或多條匯流排耦合在一起，匯流排可包括電源匯流排、控制信號匯流排、狀態信號匯流排、資料匯流排等。為清楚起見，各種匯流排在圖9中被圖示為匯流排系統919。

【0132】 在以上描述中，有時結合各種術語使用了元件符號。在結合元件符號使用術語的場合，此可以意欲引述在附圖中的一幅或更多幅圖中圖示的特定元件。在不帶元件符號地使用術語的場合，此可以意欲泛指該術語而不限於任何特定附圖。

【0133】 術語「決定」廣泛涵蓋各種各樣的動作，並且因此「決定」可包括演算、計算、處理、推導、調研、檢視（例如，在表、資料庫或其他資料結構中檢視）、探明和類似動作。另外，「決定」亦可包括接收（例如，接收資訊）、存取（例如，存取記憶體中的資料）和類似動作。另外，「決定」可包括解析、選擇、選取、建立和類似動作等等。

【0134】 除非明確另行指出，否則短語「基於」並非意味著「僅基於」。換言之，短語「基於」描述「僅基於」和「至少基於」兩者。

【0135】 術語「處理器」應被寬泛地解讀為涵蓋通用處理器、中央處理單元（CPU）、微處理器、數位訊號處理器（DSP）、控制器、微控制器、狀態機，等等。在某些情況下，「處理器」可以是指特殊應用積體電路（ASIC）、可程式設計邏輯裝置（PLD）、現場可程

式設計閘陣列（FPGA）等。術語「處理器」可以是指處理設備的組合，例如數位訊號處理器（DSP）與微處理器的組合、多個微處理器、與數位訊號處理器（DSP）核心協調的一或多個微處理器，或任何其他此類配置。

【0136】術語「記憶體」應被寬泛地解讀為涵蓋能夠儲存電子資訊的任何電子元件。術語記憶體可以是指各種類型的處理器可讀取媒體，諸如隨機存取記憶體（RAM）、唯讀記憶體（ROM）、非揮發性隨機存取記憶體（NVRAM）、可程式設計唯讀記憶體（PROM）、可抹除可程式設計唯讀記憶體（EPROM）、電可抹除PROM（EEPROM）、快閃記憶體、磁或光學資料儲存、暫存器等等。若處理器能從記憶體讀資訊及/或向記憶體寫資訊，則認為該記憶體與該處理器正處於電子通訊中。整合到處理器的記憶體與該處理器處於電子通訊中。

【0137】術語「指令」和「代碼」應被寬泛地解讀為包括任何類型的電腦可讀取語句。例如，術語「指令」和「代碼」可以是指一或多個程式、常式、子常式、函數、程序等。「指令」和「代碼」可包括單條電腦可讀取語句或許多條電腦可讀取語句。

【0138】本文中所描述的功能可以在正由硬體執行的軟體或韌體中實現。各功能可以作為一或多數指令儲存在電腦可讀取媒體上。術語「電腦可讀取媒體」或「電腦程式產品」是指能被電腦或處理器存取的任何有形儲

存媒體。作為示例而非限定，電腦可讀取媒體可包括 R A M、R O M、E E P R O M、C D - R O M 或其他光碟儲存、磁碟儲存或其他磁儲存設備，或任何其他能夠用於攜帶或儲存指令或資料結構形式的期望程式碼且能由電腦存取的媒體。如本文中所使用的盤（disk）和碟（disc）包括壓縮光碟（CD）、鐳射光碟、光碟、數位多功能光碟（DVD）、軟碟和藍光®光碟，其中盤常常磁性地再現資料而碟用鐳射來光學地再現資料。應注意，電腦可讀取媒體可以是有形且非瞬態的。術語「電腦程式產品」是指計算設備或處理器結合可由該計算設備或處理器執行、處理或計算的代碼或指令（例如，「程式」）。如本文中所使用的，術語「代碼」可以是指可由計算設備或處理器執行的軟體、指令、代碼或資料。

【0139】軟體或指令亦可以在傳輸媒體上傳送。例如，若軟體是使用同軸電纜、光纖電纜、雙絞線、數位使用者線（DSL），或諸如紅外、無線電以及微波等無線技術從web網站、伺服器或其他遠端源傳送而來的，則該同軸電纜、光纖電纜、雙絞線、DSL，或諸如紅外、無線電以及微波等無線技術就被包括在傳輸媒體的定義裡。

【0140】本文所揭示的方法包括用於實現所描述的方法的一或多個步驟或動作。該等方法步驟及/或動作可以彼此互換而不會脫離請求項的範圍。換言之，除非所描述的方法的正確操作要求步驟或動作的特定次序，否則

便可改動具體步驟及 / 或動作的次序及 / 或使用而不會脫離請求項的範圍。

【0141】 此外，應領會，用於執行本文中所描述的（諸如圖2和3所圖示的彼等）方法和技術的模組及 / 或其他合適裝置可以由設備下載及 / 或以其他方式獲得。例如，可以將設備耦合至伺服器以便於轉送用於執行本文中所描述的方法的裝置。替換地，本文中所描述的各種方法可經由儲存裝置（例如，隨機存取記憶體（RAM）、唯讀記憶體（ROM）、諸如壓縮光碟（CD）或軟碟等實體儲存媒體）來提供，以使得一旦將該儲存裝置耦合至或提供給設備，該設備就可獲得各種方法。此外，可利用適於向設備提供本文所描述的方法和技術的任何其他合適的技術。

【0142】 將理解，請求項並不被限定於以上所圖示的精確配置和元件。可在本文中所描述的系統、方法和裝置的佈局、操作及細節上作出各種改動、變化和變型而不會脫離請求項的範圍。

【符號說明】

【0143】

102 驗證器設備

104 目標設備

106 距離

108 第一訊息

110 第一回應

1 1 2 第一往返時間
1 1 4 第二訊息
1 1 6 第二回應
1 1 8 第二往返時間
1 2 0 處理時間
1 2 2 處理時間乘數
1 2 4 時間量測
1 2 6 距離上界
2 0 0 方法
2 0 2 步驟
2 0 4 步驟
2 0 6 步驟
2 0 8 步驟
3 0 0 方法
3 0 2 步驟
3 0 4 步驟
4 0 2 驗證器設備
4 0 4 目標設備
4 2 8 a 第一惡意設備
4 2 8 b 第二惡意設備
5 0 1 步驟
5 0 2 驗證器設備
5 0 3 步驟
5 0 4 目標設備

5 0 5 步 驟

5 1 2 往 返 時 間

5 2 0 處 理 時 間

5 3 0 a 傳 送 時 間

5 3 0 b 傳 送 時 間

6 0 1 步 驟

6 0 2 驗 證 器 設 備

6 0 3 步 驟

6 0 4 目 標 設 備

6 0 5 步 驟

6 0 7 步 驟

6 0 9 步 驟

6 1 1 步 驟

6 1 2 第 一 往 返 時 間

6 1 8 第 二 往 返 時 間

6 2 0 處 理 時 間

6 3 0 a 傳 送 時 間

6 3 0 b 傳 送 時 間

6 3 0 c 傳 送 時 間

6 3 0 d 傳 送 時 間

7 0 1 步 驟

7 0 2 驗 證 器 設 備

7 0 3 步 驟

7 0 4 目 標 設 備

7 0 5 步 驟

7 0 7 步 驟

7 0 9 步 驟

7 1 1 步 驟

7 1 2 第 一 往 返 時 間

7 1 3 步 驟

7 1 8 第 二 往 返 時 間

7 2 0 處 理 時 間

7 3 0 a 傳 送 時 間

7 3 0 b 傳 送 時 間

7 3 0 c 傳 送 時 間

7 3 0 d 傳 送 時 間

7 3 0 e 傳 送 時 間

8 0 1 步 驟

8 0 2 驗 證 器 設 備

8 0 3 步 驟

8 0 5 步 驟

8 0 6 a 實 際 距 離

8 0 6 b 聲 稱 距 離

8 0 7 步 驟

8 0 9 步 驟

8 1 1 步 驟

8 2 0 預 計 處 理 時 間

8 2 8 惡 意 設 備

8 3 0 a 傳送時間

8 3 0 b 傳送時間

8 3 0 c 傳送時間

8 3 0 d 傳送時間

8 3 2 偽造處理時間

8 3 4 偽造處理延遲

9 0 3 處理器

9 0 5 記憶體

9 0 7 a 資料

9 0 7 b 資料

9 0 9 a 指令

9 0 9 b 指令

9 1 1 發射器

9 1 3 接收器

9 1 5 收發機

9 1 7 天線

9 1 9 匯流排系統

9 2 1 數位訊號處理器

9 2 3 通訊介面

9 3 6 電子設備

【生物材料寄存】

【 0 1 4 4 】 國內寄存資訊(請依寄存機構、日期、號碼順序註記)

無

【 0 1 4 5 】 國外寄存資訊(請依寄存國家、機構、日期、號碼順序註
記)
無

【序列表】(請換頁單獨記載)

無

【發明申請專利範圍】

【第 1 項】 一種用於由一驗證器設備決定一距離上界的方法，包括以下步驟：

量測從一目標設備接收對應於發送給該目標設備的一第一訊息的一第一回應的一第一往返時間；

量測從該目標設備接收對應於發送給該目標設備的一第二訊息的一第二回應的一第二往返時間，該第二回應經由一處理時間乘數來延遲；

基於該第一往返時間、該第二往返時間和該處理時間乘數來決定一傳送時間量測；及

基於該傳送時間量測來決定該距離上界。

【第 2 項】 如請求項 1 所述之方法，其中該處理時間乘數指示該目標設備延遲對由該驗證器設備發送的一訊息進行回應的一時間量。

【第 3 項】 如請求項 1 所述之方法，其中在接收到該第二訊息之際，該目標設備在對該第二訊息進行回應之前將一處理時間縮放該處理時間乘數。

【第 4 項】 如請求項 1 所述之方法，其中該處理時間乘數被該驗證器設備和該目標設備知曉。

【第 5 項】 如請求項 1 所述之方法，其中該處理時間乘數是一固定值。

【第 6 項】 如請求項 1 所述之方法，其中該處理時間乘

數基於被發送給該目標設備的該第二訊息的內容來決定。

【第7項】 如請求項1所述之方法，其中該傳送時間量測根據 $T_f = (n \cdot T_{round,1} - T_{round,2}) / 2(n-1)$ 來決定，其中 T_f 是該傳送時間， n 是該處理時間乘數， $T_{round,1}$ 是該第一往返時間並且 $T_{round,2}$ 是該第二往返時間。

【第8項】 如請求項1所述之方法，其中決定該距離上界包括將該傳送時間量測乘以光速。

【第9項】 如請求項1所述之方法，其中該距離上界包括該驗證器設備與該目標設備之間的一距離的一上界。

【第10項】 如請求項1所述之方法，其中該距離上界基於至少一個附加傳送時間量測來決定，其中該目標設備根據該處理時間乘數來延遲回應。

【第11項】 如請求項10所述之方法，其中該處理時間乘數包括一值序列，該等值之一被應用於一給定往返時間量測。

【第12項】 如請求項1所述之方法，進一步包括以下步驟：

量測至少一個附加往返時間；

使用該至少一個附加往返時間來決定至少一個附加傳送時間量測；

決定一平均傳送時間量測；及

基於該平均傳送時間量測來決定該距離上界。

【第13項】 如請求項1所述之方法，其中該驗證器設備是一讀取器設備，該目標設備是一監聽設備，並且該第一訊息和該第二訊息包括發送給該監聽設備的質詢訊息。

【第14項】 如請求項1所述之方法，其中該驗證器設備是一監聽設備，該目標設備是一讀取器設備，並且該第一訊息和該第二訊息包括對接收自該讀取器設備的質詢的回應。

【第15項】 一種被配置成決定一距離上界的驗證器設備，包括：

一處理器；

與該處理器處於通訊的一記憶體；及

儲存在該記憶體中的指令，該等指令能由該處理器執行以：

量測從一目標設備接收對應於發送給該目標設備的一第一訊息的一第一回應的一第一往返時間；

量測從該目標設備接收對應於發送給該目標設備的一第二訊息的一第二回應的一第二往返時間，該第二回應經由一處理時間乘數來延遲；

基於該第一往返時間、該第二往返時間和該處理

時間乘數來決定一傳送時間量測；及

基於該傳送時間量測來決定該距離上界。

【第16項】 如請求項15所述之驗證器設備，其中該處理時間乘數指示該目標設備延遲對由該驗證器設備發送的一訊息進行回應的一時間量。

【第17項】 如請求項15所述之驗證器設備，其中該處理時間乘數被該驗證器設備和該目標設備知曉。

【第18項】 如請求項15所述之驗證器設備，其中該處理時間乘數是一固定值。

【第19項】 如請求項15所述之驗證器設備，其中該處理時間乘數基於被發送給該目標設備的該第二訊息的內容來決定。

【第20項】 如請求項15所述之驗證器設備，其中該傳送時間量測根據 $T_f = (n \cdot T_{round,1} - T_{round,2}) / 2(n-1)$ 來決定，其中 T_f 是該傳送時間， n 是該處理時間乘數， $T_{round,1}$ 是該第一往返時間並且 $T_{round,2}$ 是該第二往返時間。

【第21項】 如請求項15所述之驗證器設備，其中該距離上界基於至少一個附加傳送時間量測來決定，其中該目標設備根據該處理時間乘數來延遲回應。

【第22項】 一種被配置成決定一距離上界的裝備，包括：

用於量測從一目標設備接收對應於發送給該目標

設備的一第一訊息的一第一回應的一第一往返時間的構件；

用於量測從該目標設備接收對應於發送給該目標設備的一第二訊息的一第二回應的一第二往返時間的構件，該第二回應經由一處理時間乘數來延遲；

用於基於該第一往返時間、該第二往返時間和該處理時間乘數來決定一傳送時間量測的構件；及

用於基於該傳送時間量測來決定該距離上界的構件。

【第23項】 如請求項22所述之裝備，其中該處理時間乘數指示該目標設備延遲對由該裝備發送的一訊息進行回應的一時間量。

【第24項】 如請求項22所述之裝備，其中該處理時間乘數被該裝備和該目標設備知曉。

【第25項】 如請求項22所述之裝備，其中該處理時間乘數是一固定值。

【第26項】 如請求項22所述之裝備，其中該處理時間乘數基於被發送給該目標設備的該第二訊息的內容來決定。

【第27項】 如請求項22所述之裝備，其中該傳送時間量測根據 $T_f = (n \cdot T_{round,1} - T_{round,2}) / 2(n-1)$ 來決定，其中 T_f 是該傳送時間， n 是該處理時間乘數， $T_{round,1}$ 是該第一往

返時間並且 $T_{round,2}$ 是該第二往返時間。

【第 28 項】 如請求項 22 所述之裝備，其中該距離上界基於至少一個附加傳送時間量測來決定，其中該目標設備根據該處理時間乘數來延遲回應。

【第 29 項】 一種用於決定一距離上界的電腦程式產品，該電腦程式產品包括其上具有指令的一非瞬態電腦可讀取媒體，該等指令包括：

用於使一驗證器設備量測從一目標設備接收對應於發送給該目標設備的一第一訊息的一第一回應的一第一往返時間的代碼；

用於使該驗證器設備量測從該目標設備接收對應於發送給該目標設備的一第二訊息的一第二回應的一第二往返時間的代碼，該第二回應經由一處理時間乘數來延遲；

用於使該驗證器設備基於該第一往返時間、該第二往返時間和該處理時間乘數來決定一傳送時間量測的代碼；及

用於使該驗證器設備基於該傳送時間量測來決定該距離上界的代碼。

【第 30 項】 如請求項 29 所述之電腦程式產品，其中該處理時間乘數指示該目標設備延遲對由該驗證器設備發送的一訊息進行回應的一時間量。

【第31項】 如請求項29所述之電腦程式產品，其中該處理時間乘數被該驗證器設備和該目標設備知曉。

【第32項】 如請求項29所述之電腦程式產品，其中該處理時間乘數是一固定值。

【第33項】 如請求項29所述之電腦程式產品，其中該處理時間乘數基於被發送給該目標設備的該第二訊息的內容來決定。

【第34項】 如請求項29所述之電腦程式產品，其中該傳送時間量測根據 $T_f = (n \cdot T_{round,1} - T_{round,2}) / 2(n-1)$ 來決定，其中 T_f 是該傳送時間， n 是該處理時間乘數， $T_{round,1}$ 是該第一往返時間並且 $T_{round,2}$ 是該第二往返時間。

【第35項】 一種用於決定何時延遲發送回應以用於一距離上界決定操作的方法，包括以下步驟：

由一目標設備向一驗證器設備發送對應於從該驗證器設備接收到的一第一訊息的一第一回應；及

由該目標設備向該驗證器設備發送經由一處理時間乘數延遲的一第二回應，該第二回應對應於從該驗證器設備接收到的一第二訊息，其中該驗證器設備基於一第一往返時間、一第二往返時間和該處理時間乘數來決定該距離上界。

【第36項】 如請求項35所述之方法，其中該處理時間乘數指示該目標設備延遲對由該驗證器設備發送

的一訊息進行回應的一時間量。

【第37項】 如請求項35所述之方法，其中在接收到該第二訊息之際，該目標設備在對該第二訊息進行回應之前將一處理時間縮放該處理時間乘數。

【第38項】 如請求項35所述之方法，其中該處理時間乘數被該驗證器設備和該目標設備知曉。

【第39項】 如請求項35所述之方法，其中該處理時間乘數是一固定值。

【第40項】 如請求項35所述之方法，其中該處理時間乘數基於由該目標設備接收到的該第二訊息的內容來決定。

【第41項】 一種被配置成決定何時延遲發送一回應以用於一距離上界決定操作的目標設備，包括：

一處理器；

與該處理器處於通訊的一記憶體；及

儲存在該記憶體中的指令，該等指令能由該處理器執行以：

向一驗證器設備發送對應於從該驗證器設備接收到的一第一訊息的一第一回應；及

向該驗證器設備發送經由一處理時間乘數延遲的一第二回應，該第二回應對應於從該驗證器設備接收到的一第二訊息，其中該驗證器設備基於一第

一往返時間、一第二往返時間和該處理時間乘數來決定該距離上界。

【第42項】 如請求項41之目標設備，其中該處理時間乘數指示該目標設備延遲對由該驗證器設備發送的一訊息進行回應的一時間量。

【第43項】 如請求項1所述之目標設備，其中在接收到該第二訊息之際，該目標設備在對該第二訊息進行回應之前將一處理時間縮放該處理時間乘數。

【第44項】 一種被配置成決定何時延遲發送一回應以用於一距離上界決定操作的裝備，包括：

用於向一驗證器設備發送對應於從該驗證器設備接收到的一第一訊息的一第一回應的構件；及

用於向該驗證器設備發送經由一處理時間乘數延遲的一第二回應的構件，該第二回應對應於從該驗證器設備接收到的一第二訊息，其中該驗證器設備基於一第一往返時間、一第二往返時間和該處理時間乘數來決定該距離上界。

【第45項】 如請求項44所述之裝備，其中該處理時間乘數指示該裝備延遲對由該驗證器設備發送的一訊息進行回應的一時間量。

【第46項】 如請求項44所述之裝備，其中在接收到該第二訊息之際，該裝備在對該第二訊息進行回應之

前將一處理時間縮放該處理時間乘數。

【第47項】 一種用於決定何時延遲發送一回應以用於一距離上界決定操作的電腦程式產品，該電腦程式產品包括其上具有指令的一非瞬態電腦可讀取媒體，該等指令包括：

用於使一目標設備向一驗證器設備發送對應於從該驗證器設備接收到的一第一訊息的一第一回應的代碼；及

用於使該目標設備向該驗證器設備發送經由一處理時間乘數延遲的一第二回應的代碼，該第二回應對應於從該驗證器設備接收到的一第二訊息，其中該驗證器設備基於一第一往返時間、一第二往返時間和該處理時間乘數來決定該距離上界。

【第48項】 如請求項47所述之電腦程式產品，其中該處理時間乘數指示該目標設備延遲對由該驗證器設備發送的一訊息進行回應的一時間量。

【第49項】 如請求項47所述之電腦程式產品，其中在接收到該第二訊息之際，該目標設備在對該第二訊息進行回應之前將一處理時間縮放該處理時間乘數。

圖式

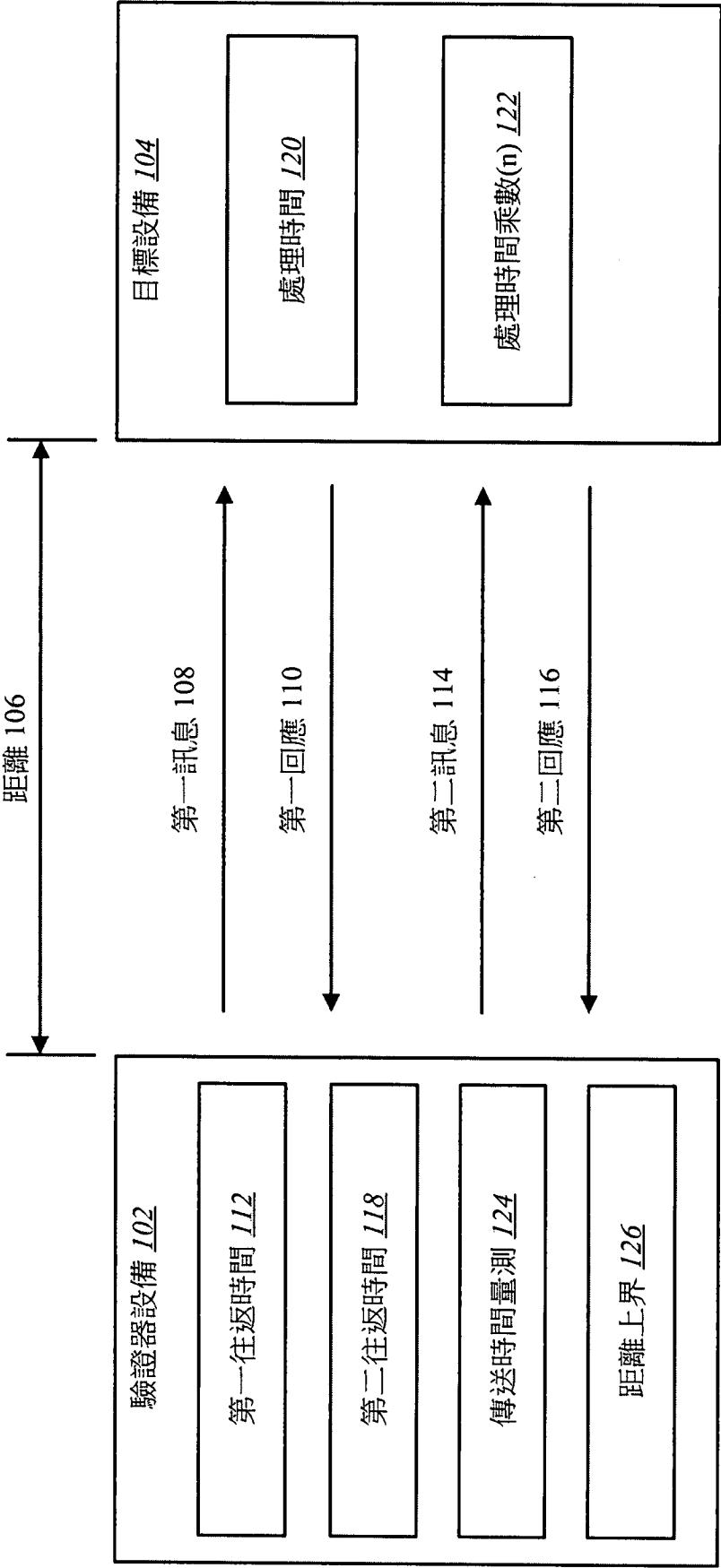


圖1

200 →

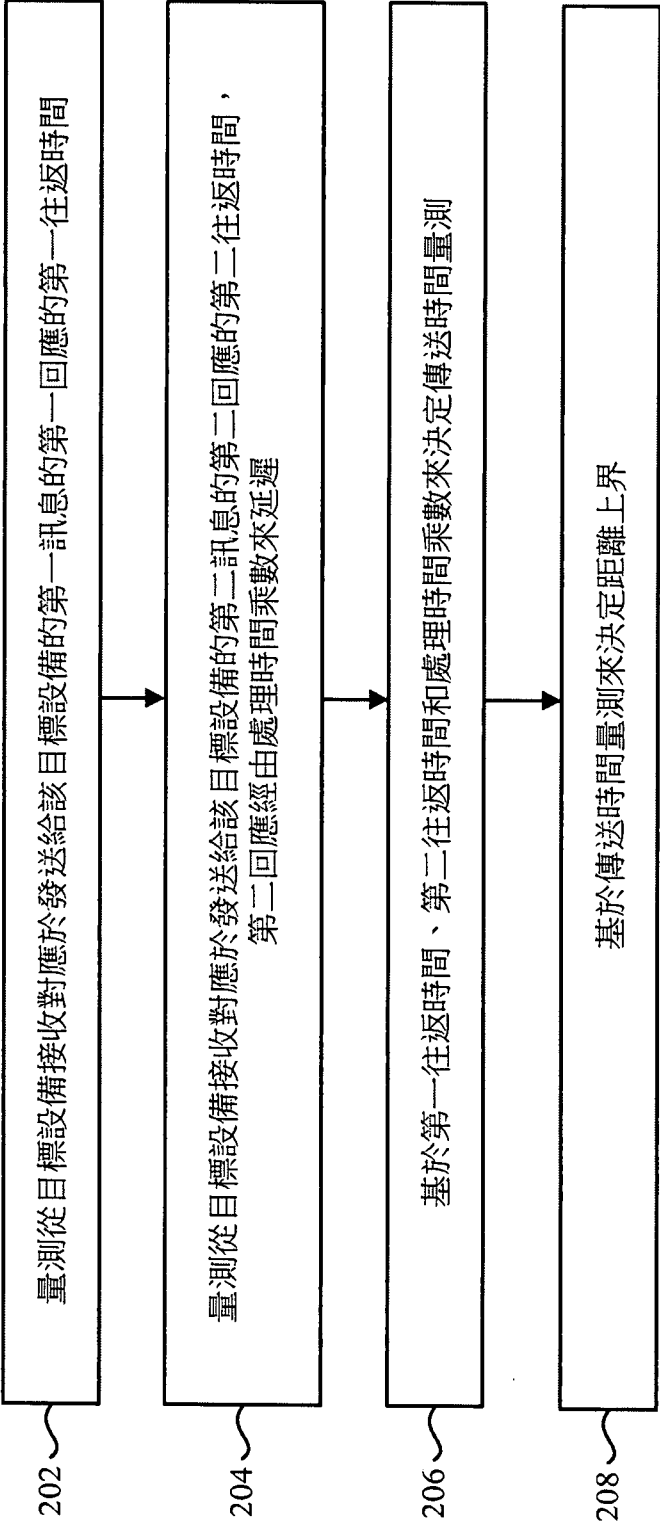


圖2

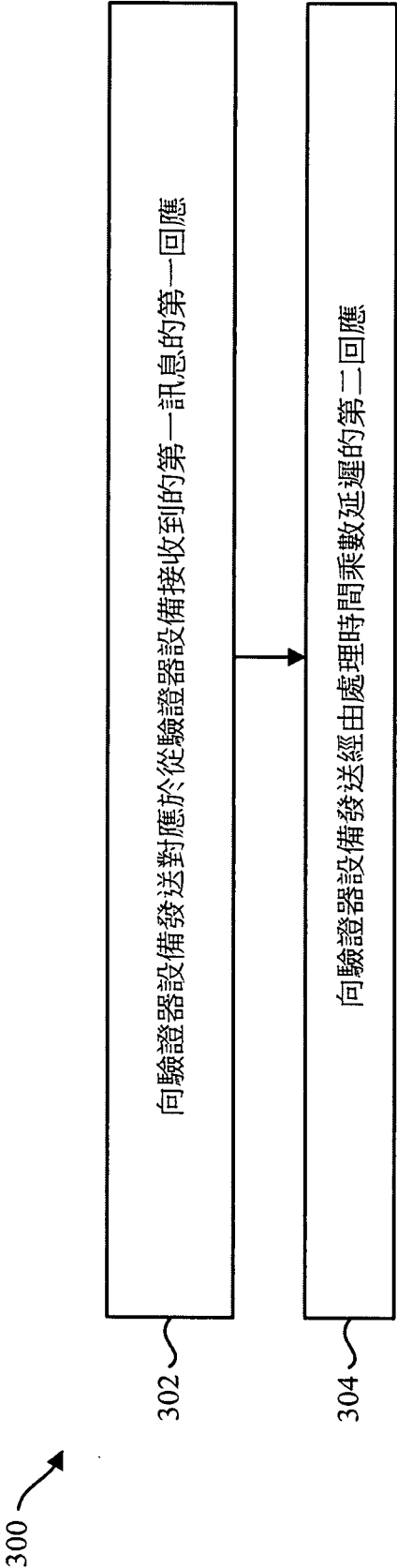


圖3

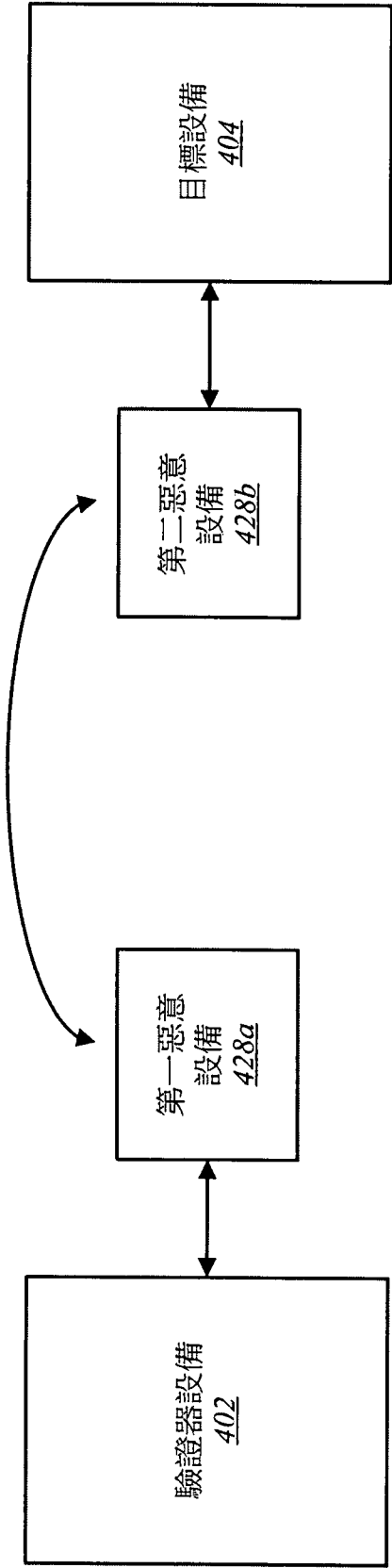


圖4

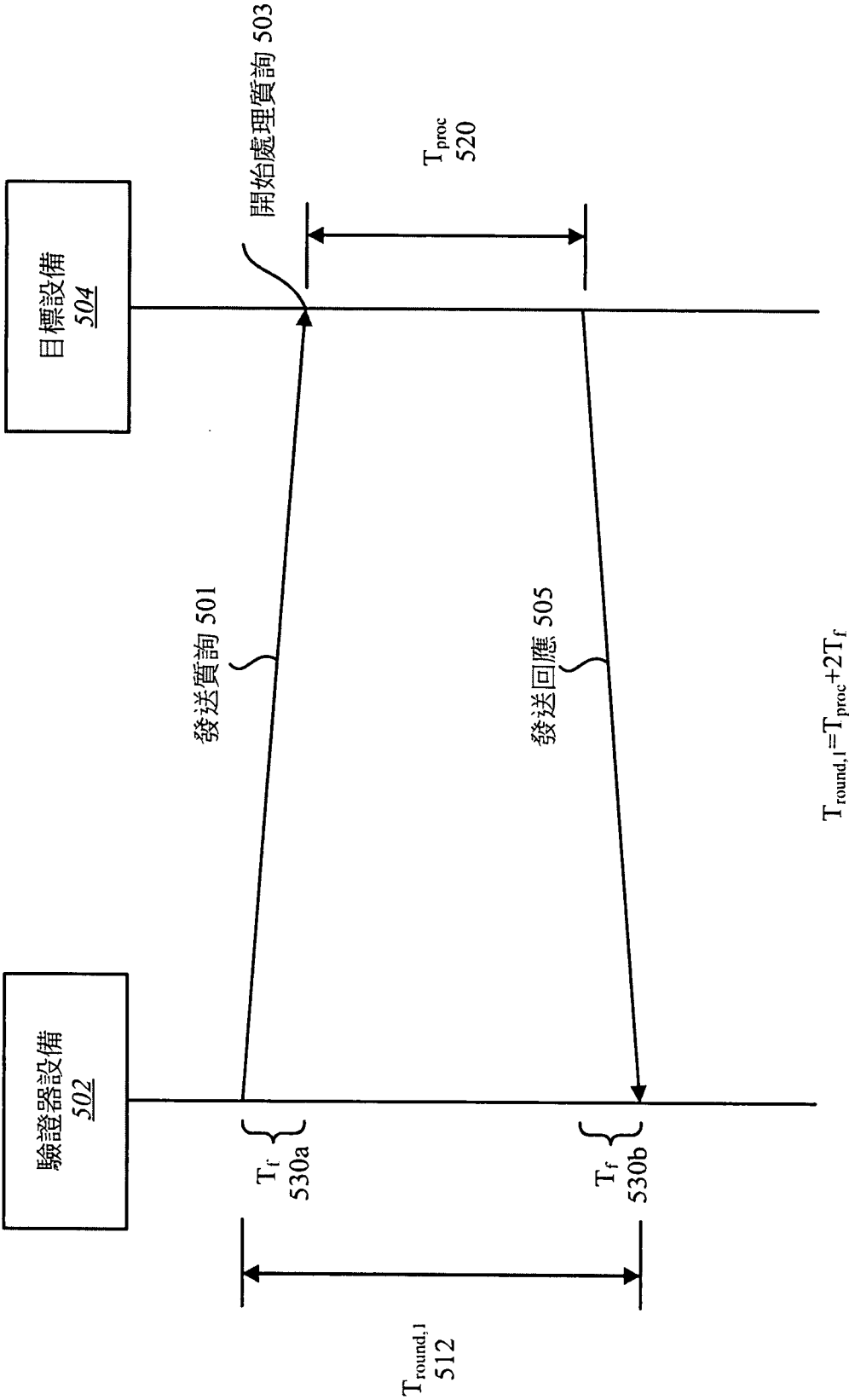


圖5

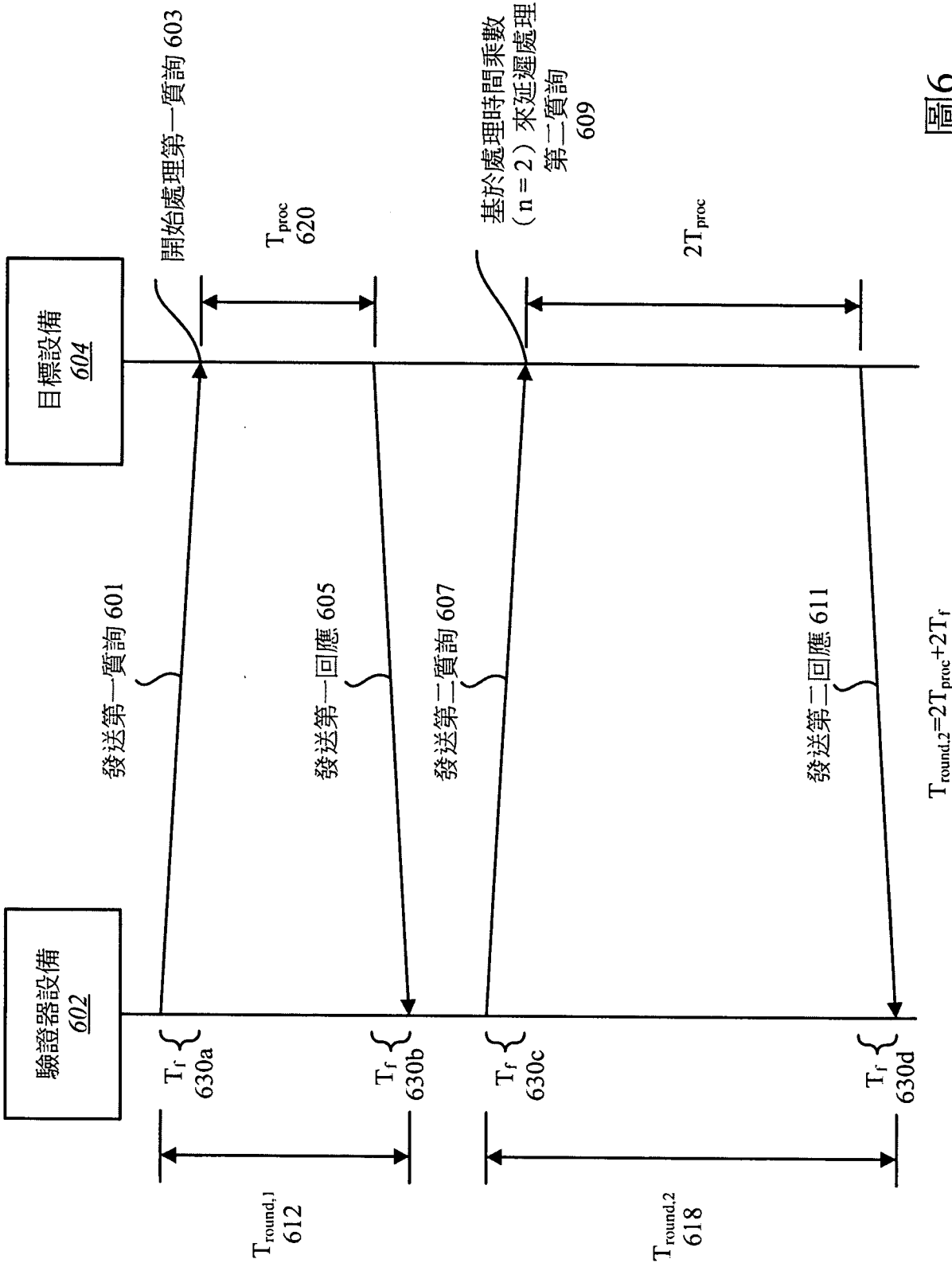


圖6

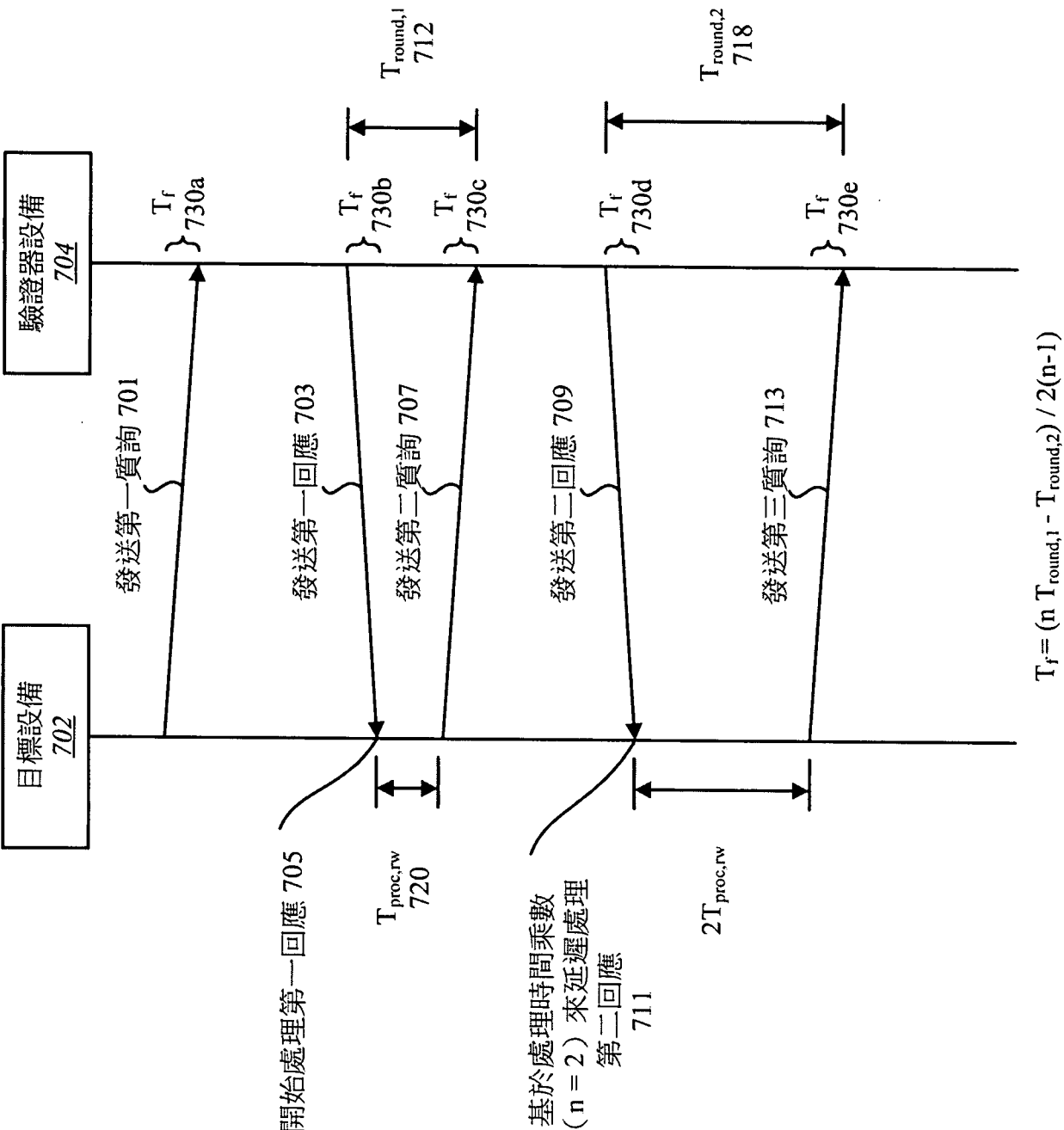


圖7

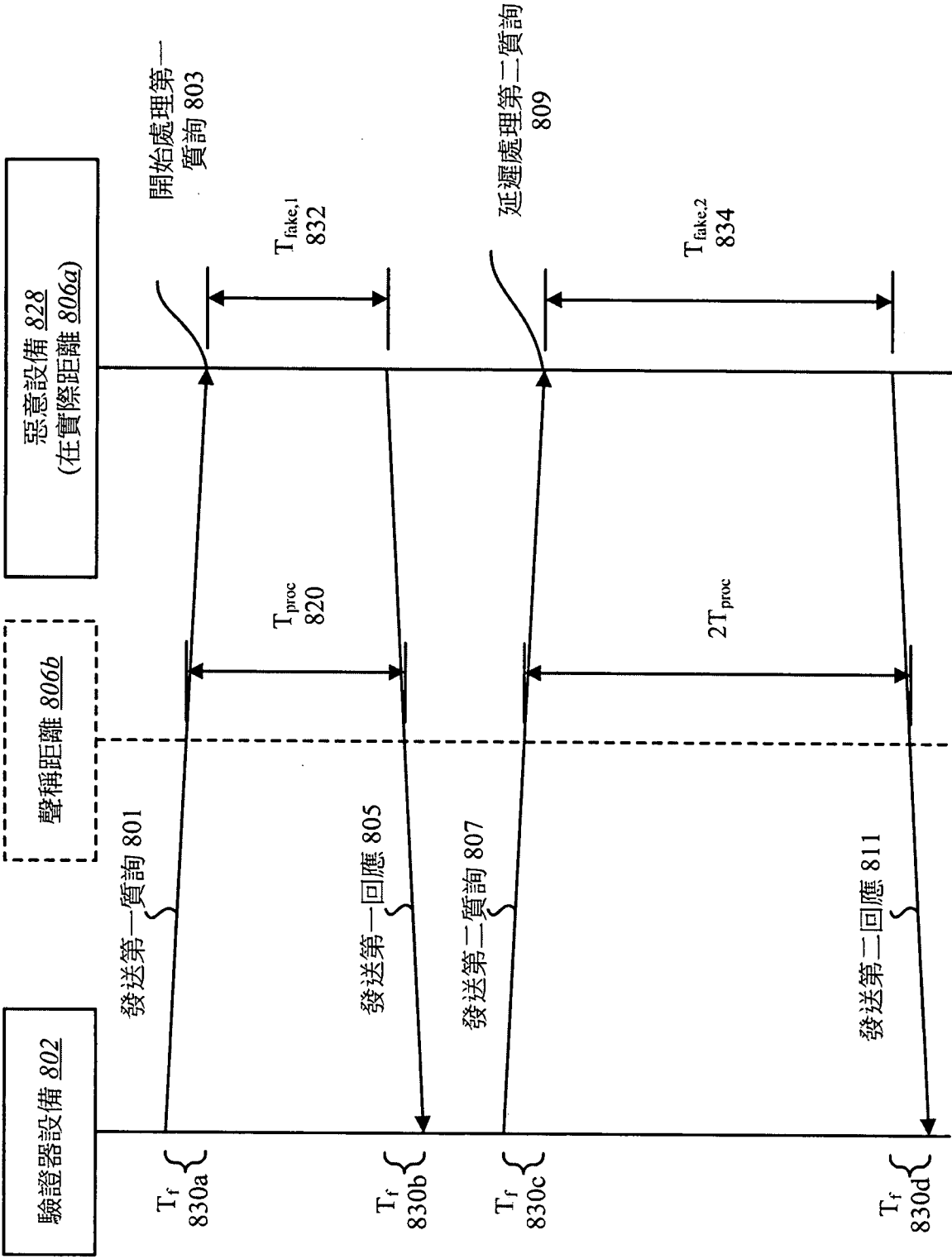


圖8

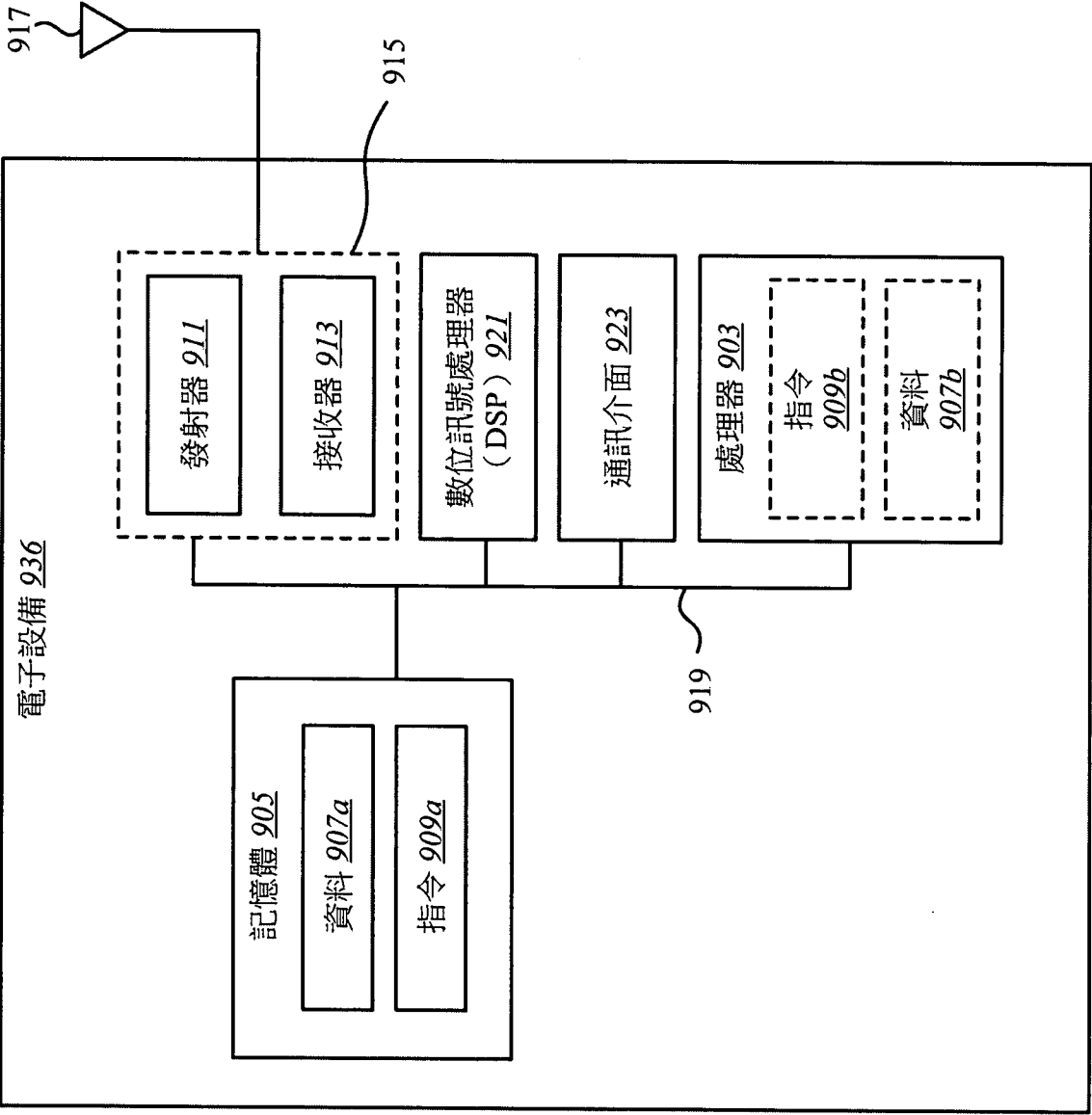


圖9