RFID 於零售業存貨管理之安全監控應用系統－TRP 的問題與改良設計

Design of an RFID-based Retail Inventory Management System using an improved Trusted Reader Protocol

陳育毅
中興大學資訊管理學系
Email:chenyuyi@nchu.edu.tw

詹進科
中興大學資訊科學與工程學系
Email:jkjan@cs.nchu.edu.tw

顧純菁
中興大學資訊科學與工程學系
Email:s9556053@cs.nchu.edu.tw

***摘要*—在流通零售業的一般作業中，商品的存貨控制一直是個重要的課題，因為良好的存貨控制才能反應實際上的銷售利潤。而實行存貨控制的方法，從傳統的人工直接盤點到商品加上條碼後進行盤點，精確性與效率都在逐漸提升。近年來 RFID 也開始應用於其中。本篇文章裡，我們討論了 Tan、Sheng & Li 三位學者所提出的 TRP 協定，對於 TRP 協定的問題點，特別是應用情境及協定限制進行了提升準確性的改良，主要是希望可以利用 RFID 在商品盤點的即時監控中，能更快速，更安全，且具有更高的精確性。**

***關鍵詞*—存貨控制、盤點、RFID、TRP。**

***Abstract*—For the regular operation of retail business, the inventory control mechanism is always a important task since the profit control can be easily estimation. Recently, the RFID had been widely apply to automatically inventory control and the accuracy and performance are thus be highly improved. In this paper, we surveyed the TRP protocol, that was proposed by Tan、Sheng & Li, and the possible accuracy enhancement and been proposed, And the accuracy of enhanced TRP protocol had been highly improved especially for the specified application situation. In the future, we hope the proposed can be widely used in inventory control and the performance, accuracy and security can thus be improved via proposed method.**

***Keywords*—inventory control、盤點、RFID、TRP。**

一、簡介

就賣場零售業者來說，從傳統的小型雜貨店，經過不斷演化，開始出現大型經營的模式，例如百貨公司、超級市場、量販店等，這一類型賣場的特點是賣場面積大並且販售的商品種類及數量繁多，營業時間也較長。對於此類型的零售商，如何施行商品的存貨控制機制就顯得十分重要。根據 NRSS 對於 2008 年零售業的相關調查結果發現[3]，全年有高達 360 億美金的損失而其中 80%導因於商品偷竊以及廠商的欺騙行為，也就是說因為商品存貨的問題，而導致業者的獲利降低。換句話說，若能對商品的存貨控制提出更有效的方法，將有助於零售業者的整體獲

利。

商品的存貨控制最基本的方法便是進行盤點，盤點的目的是要了解商品的存缺狀況以了解經營的損益，而根據存貨盤點的結果，才能反應出實際上的銷售利潤。傳統的盤點，是以人工方式執行，工作人員使用紙筆一一核對賣場商品的種類與數量，這樣的方式需花費大量的人力與時間，而準確性則是由人員的執行狀況來決定。40年代開始出現條碼[10]，而在盤點過程中使用條碼，可減少不少的人力時間，而結果也較人工方式快速並正確。

近幾年來，興起了一種新的技術—無線射頻識別系統(Radio Frequency Identification, RFID)，這個技術與條碼最大的不同點在於使用條碼盤點時，商品都必須在可以看到的範圍內，因為條碼讀取器必須對準條碼才能讀取到條碼以獲取相關商品訊息，並且一次只能讀取一個條碼，而 RFID 因為其原理使用電磁波，因此 RFID 讀取器僅需與商品在電磁波可感應到的範圍內即可，同時間可讀取多個，因此與條碼相比其效率極佳。如果在所有商品都貼上電子標籤，使用讀取器便可在一定範圍內主動獲得電子標籤所傳回的識別碼以獲取商品資訊，以這樣的方式進行盤點作業時，如此不僅能保有原先條碼盤點的準確性，更能提升盤點的效率。

零售業對於盤點，除了因科技的進步而不斷發展出使得效率更好的解決方式之外，就盤點管理來說，盤點執行的時間也是一個重要的考量。盤點作業若就盤點時間區分，可分為營業中、營業前(後)與停業盤點[1]。並且就盤點而言，準確性十分重要，因為確實掌握商品數量才能了解經營的狀況。而上述的三個盤點時間，營業中盤點是指在賣場營業時間中即進行盤點，其優點是可即時掌握商品的存貨狀況，但易受顧客影響降低準確性，營業前(後) 盤點則是在賣場開始營業前或是營業時間結束後進行盤點，雖然此時盤點不受營業中狀況影響，準確性高卻有商品損失無法及時發現的風險，而停業盤點，則是在正規營業時間中暫停營業來進行盤點，此種方式的準確性較高，然而由於零售業的商品流動性大，間隔太久進行盤點將容易造成存貨控制的問題，而時間過於密集則會影響業績及客戶的購買慾，所以同樣是有較高的商品損失風險，更多了停業的業務損失，更何況近年來 24 小時營業並且加上全年無休的營業模式興起，停業盤點與營業前(後) 盤點似乎是不可能被考慮的選項，所以唯有改善營業中盤點的準確性，才是切合未來需求的發展。

但我們所了解，營業中盤點所面臨的最大問題便是顧客購物持續進行所造成的無法精確盤點，特別是大型賣場，例如百貨公司、超級市場、量販店等，其賣場面積大並且營業時間長，因此同時進行購物的顧客數量也多，顧客購物的時間也較長，若此時進行盤點，不在貨架上的商品代表的可能是被購買、取貨尚未結帳或者是已遺失，如此一來，很難精確掌握商品的數量。

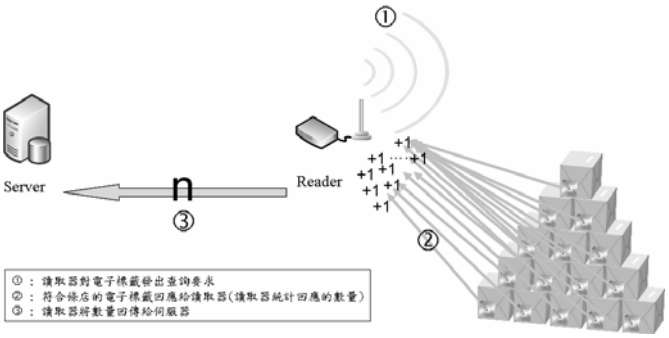
但是，若考慮 RFID 技術的引進，就可以達到短時間內完成盤點，提升盤點效率。至於如何改善營業中盤點的準確性，可採用監控模式，也就是隨時隨地監視商品狀況，並在得知商品狀況後給予適當的控制處理[8]。若營業中實施持續的監控，除了對於商品是否存在給予監視，還可以即時察覺到商品是否有異常減少現象，並適時的提出警告。這樣的方式，似乎是解決盤點問題的好方法，目前已有學者提出相關的研究[6]，實際上以監控方式的運作，做到更好的存貨控制。

因此，引進 RFID，可以發展出一套監控系統，這樣的系統除了能夠改善盤點作業的準確性及效率之外，更必須兼顧安全性。不僅能在營業中即時掌握商品動態，將顧客同時購物所可能造成的商品數量誤差考慮進來，以即時掌握營業中商品的存貨狀況，並且能夠預防內部工作人員的偷竊行為，達到安全的目的。

二、相關研究

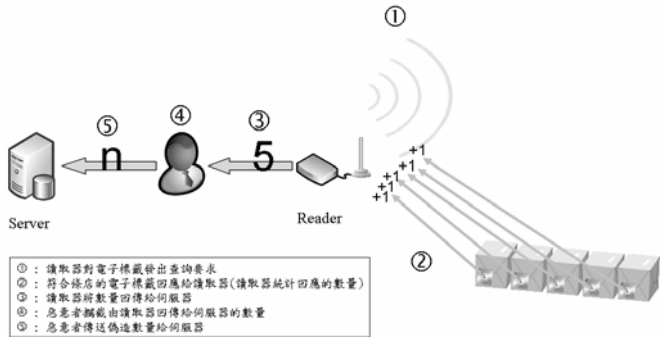
在前一節中已經了解，若從 RFID 的方向來做商品的存貨控制，那麼不應該落入舊式盤點的思維，應該以監控的方向來做應用，而這樣的監控方式應該要能夠改善效率、提升準確度並且達到安全性。接下來將對於盤點各類方式的基本演進做一個介紹及分析。

第一種是以盤點為出發點所設計的計數法(Count)。這個方式的設計最為簡單，最後只須將電子標籤數量傳回伺服器做確認。計數法的運作方式是讀取器對於需要盤點的電子標籤廣播查詢條件，電子標籤收到查詢條件後與自己所持有的資訊比對，若是符合條件，該電子標籤便回應給讀取器，接著讀取器計算有回應的電子標籤總數，再將數量回傳至伺服器(如圖一)。



圖一 計數法

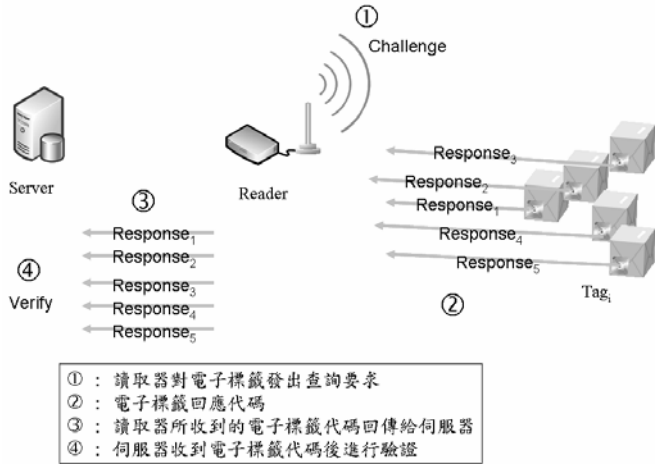
這種方式簡單，不需傳送大量資料，可以得到很好的盤點效率，也可得到精確的盤點結果，若套用於監控模式上，同樣也可以在效率與準確性上有著很好的效果。



圖二 計數法的安全漏洞

然而這樣的設計卻有著很大的安全性問題，因為若只回應數量，內部工作人員將有機會在讀取器回傳資料給伺服器的過程中進行竄改，也就是在數量傳給伺服器前將其攔截，並偽造數量回傳給伺服器，而實際上，已有部份商品遺失或遭偷竊(如圖二)。

第二種方式也是基植於盤點概念而設計出來的方法，稱為收集法(Collect All)[6]。這個方法不同於前一個計數法的方式，它並不是由讀取器統計有回應的電子標籤數量來回報給伺服器，而是讓讀取器藉由一種在設計上較為安全的方法來將電子標籤上的回應值傳回給伺服器作比對。這個方法的運作方式是由讀取器對於每一個需盤點的商品電子標籤發出查詢要求，受盤點的電子標籤收到查詢要求時需做出回應，接著讀取器將所收到的電子標籤回應值回傳至伺服器，並與伺服器中的記錄作比對，以驗證電子標籤的真確性(如圖三)。



圖三 收集法

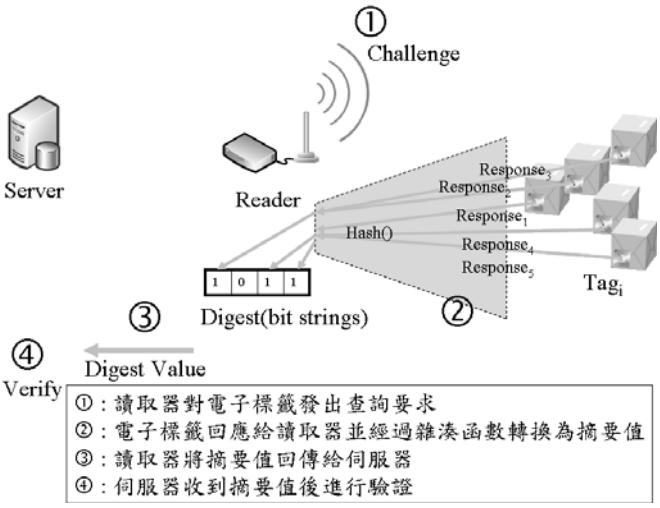
基本上此類設計要達到安全性等同於設計 RFID 的驗證(Authentication)，而 RFID 驗證的執行上，電子標籤、讀取器與伺服器三方面資料傳遞的次數與資料量都比第一個方式要大，當這個方式使用於一個較小範圍商品的盤點時，盤點效率仍可在一定的範圍之內。然而，若盤點商品數量增加，讀取器就必須對大量的商品進行查詢驗證，因此讀取器與所有電子標籤間會有大量的資訊流產生，再加上與後端商品記錄伺服器的資訊交換，系統中資料傳遞的次數與資料量都大幅增

加，商品盤點效率將大為降低。另外，電子標籤必須以其關鍵值(Key)計算出回應值，若安全設計不佳，有可能在傳遞過程中遭受重送攻擊或遭攔截竊聽並被破解關鍵值(Key)。

若將此種方法套用至監控模式中，由於監控要求的是隨時掌握商品狀況，因此必須在短時間內完成一次盤點的動作，收集法因為會對每一個電子標籤做驗證，精確度高，但也由於必需對每一個電子標籤做驗證，所以所需的時間長，因此效率不佳。至於安全性，已有多篇研究針對 RFID 的安全設計做研究討論，例如 2005 年 Lee 等學者提出的 LCAP(low-cost authentication protocol)[4]，主要是用相互任證來達到安全性，若將 LCAP 套用至收集法，是可以達到監控中的安全性要求。當然也有一些 RFID 研究想要做到安全的設計，然而並未考慮周全，若使用此類方式套用至收集法，則可能使得監控作業中遭受到攻擊[7][2][5]。

第三種方式已不單用盤點為思考中心，而是發揮 RFID 的特性來做監控模式的設計。2008 年，Tan、Sheng & Li 提出了 TRP(Trusted Reader Protocol)協定，就是屬於這樣的方法。這個方法中讀取器與電子標籤之間的互動是以 Challenge-Response 的精神來做設計，以類似收集法的方式來著手，但是讀取器最後將資料回傳給伺服器時又不希望回傳大量資料，而為了降低傳遞資料量並維持可驗證電子標籤的特性，讀取器需收集所有的電子標籤的資訊後轉換為可驗證的摘要值傳回伺服器，所以讀取器與電子標籤間的溝通中，巧妙的融入雜湊函數，利用雜湊函數可摘要出資料又可驗證的特性達到監控目的。

TRP 的主要概念是使用雜湊(Hash)方法，首先由伺服器決定種子(seed)並將種子傳送給讀取器，接著讀取器廣播種子給所有電子標籤，每個電子標籤利用所收到的種子與自己的關鍵值來計算各自的雜湊值，讀取器再依序發出查詢，電子標籤則依據查詢回應 0 或 1 給讀取器，整個查詢過程完成即彙整成位元字串傳回給伺服器。所以最後回傳給伺服器的不是電子標籤數量，也不是每個電子標籤的回應值，而是一個可驗證的位元字串，是一個由每個電子標籤的回應值經由雜湊函數轉換過後所摘要出來的摘要值(如圖四)。



圖四 TRP 法

由於 TRP 是使用雜湊方法，而雜湊方法是由種子來決定計算出來的值，每次發出查詢需求時都由伺服器決定種子，種子的不同則每次計算出來的雜湊值也會不同，最後依雜湊值所簡化出來的位元字串也會不同，因此每一次的查詢過程中讀取器收集所得的位元字串若與伺服器計算之結果不同，很容易發現到電子標籤遺失或是資訊遭到竄改。

使用 TRP 方式的優點在於若電子標籤的雜湊值沒有發生碰撞(Collision) ，也就是沒有兩個以上的電子標籤所計算出來的雜湊值相同，其效果等同於逐一盤點，因此準確性高。也由於讀取器發出查詢後，電子標籤並不直接回應關鍵值，而是將關鍵值經過雜湊函數轉換後再回傳讀取器，因此安全性高。並且讀取器是以位元資料形式回傳給伺服器，可降低傳遞資料量，因此可達快速的目的。

從以上的討論中可以了解，TRP 提供了一個在營業中監測商品存貨的新模式，這個模式脫離傳統盤點的方法，發揮 RFID 可主動收集資訊及快速傳遞資料的特性，增加商品盤點的次數來達到可在營業中監控商品的存在狀況，藉此完成盤點的目的，然而 TRP 本身仍存在著一些問題，下一節將對 TRP 做個基本介紹並且說明其問題。

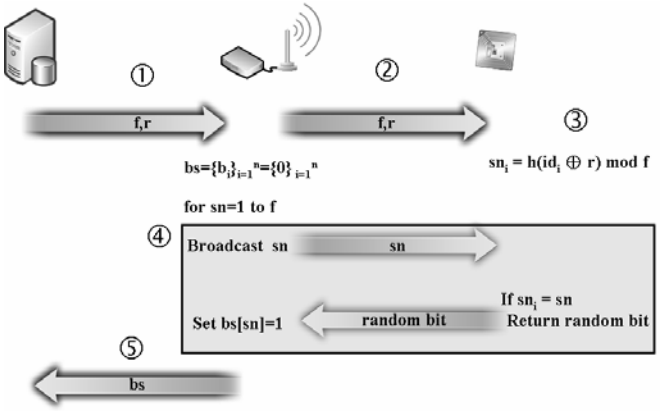
三、TRP 協定

TRP 協定是 Tan、Sheng & Li 三位學者在 2008 年所提出的，主要是以改善存貨控制為出發點，他們認為應該要精確並有效率的監控商品，才能達到良好的存貨控制，因此提出了 TRP 的協定。在詳細介紹 TRP 前，先簡單說明使用符號如表一。

表一 TRP 使用符號表

f	摘要值大小
r	亂數種子
n	電子標籤個數
m	可忍受遺失的最大電子標籤個數
α	可偵測出超過 m 個遺失狀況的成功率
$h()$	雜湊函數
sn_i	電子標籤的雜湊值
bs	長度為 f 的位元字串
id_i	電子標籤代碼

TRP 協定的主要設計概念在於由讀取器負責收集所有電子標籤資料，資料收集時不需要直接傳遞電子標籤關鍵值(Key)，收集後的結果轉換為位元字串，並且一次將位元字串傳給伺服器，而整個協定的相關參數均由伺服器決定，其運作流程可分為兩個階段(如圖五)：



圖五 TRP 法

第一個階段為準備階段：

首先步驟 1~步驟 3 是 TRP 的準備步驟，主要是要將由伺服器決定的摘要值長度及雜湊函數所需要的種子廣播給所有需要監控的電子標籤，每個電子標籤利用所收到的種子與自己的關鍵值來計算各自的雜湊值。

步驟 1. 伺服器決定摘要值長度 f、隨機產生亂數種子 r，並將(f,r)傳送給讀取器。

步驟 2. 讀取器將摘要值長度 f 及亂數值 r 廣播給所有電子標籤，並且在讀取器產生長度為 f 的位元字串，預設位元值均為 0。

步驟 3. 每個電子標籤收到(f,r)後，與自己的電子標籤代碼一起計算出雜湊值 sn_i。

$$sn_i = h(id_i \oplus r) \bmod f \qquad (1)$$

第二個階段為執行階段：

由於在前面的步驟中，所有的電子標籤已將各自的雜湊值計算好，所以接下來的步驟 4~步驟 5，讀取器依序發出查詢要求，並依照有無電子標籤回應來決定該位元應為 0 或 1，最後產生位元字串。

步驟 4. 讀取器依序廣播 1 至 f，每次廣播，完成下列動作：

步驟 4.1. 當電子標籤收到讀取器廣播的值時，便與自己先前計算出來準備好的 sn_i 值做比對，若相等則發出一個簡單回應訊息給讀取器，若不相等則該電子標籤不做任何回應。

步驟 4.2. 若讀取器收到電子標籤的回應，便將位元字串的對應位置設為 1。

步驟 5. 讀取器將位元字串回傳給伺服器驗證。

伺服器在收到由讀取器回傳的位元字串後，先將伺服器資料庫中的電子標籤記錄，依同樣函式做計算來產生另一組位元字串，接著將兩個位元字串做比對。每一次的查詢過程中，伺服器決定的摘要值長度及雜湊函數種子不同，就算是電子標籤的存在狀況無變化，也會產生不同的字串。如此即可避免惡意者對此機制實施重送攻擊，所以伺服器收到的位元字串若與其計算的結果不同，就代表電子標籤遺失或資訊遭到竄改。

至於伺服器是如何比對位元字串，在原來的研究中並沒有說明。我們推敲過最合理的比對方式，不只是比對位元為 1 的數量還必需比對位元的位置，因為可藉由位置去回查代表哪幾個電子標籤。對於比較結果相異的位元，若依據資料庫中計算的結果是 1，而讀取器回傳的是 0，則代表有電子標籤遺失，但若依據資料庫中計算的結果是 0，而讀取器回傳的是 1，則可能有假冒的電子標籤出現。

四、TRP 協定的設計缺失

依據比對結果中相異的位元再去對照伺服器資料庫中的記錄，便可以得知是哪些電子標籤遺失。然而，TRP 是應用在營業中進行商品監控，若單純以上述比對方式來看，只要位元比對時發現伺服器計算所得位元為 1，但讀取器回傳位元為 0，就表示商品遺失，如此一來，系統將會頻繁的發出警告訊息，為什麼會發生這樣的狀況呢？因為賣場在營業中，能會有消費者自貨架取下商品但尚未結帳的情況，於是盤點時就會出現伺服器中記錄與賣場中的讀取器所盤點出來的不同，因此比對的結果若有不同，並不能完全代表商品的遺失。而 TRP 的設計是有考慮到這樣的問題，其設計可以達成容許誤差，也就是說，若計算出遺失電子標籤的數目超過伺服器所設定的門檻值，才視為有遺失而發出警告。

在 TRP 的設計中，有另外兩個參數是系統可依實際運作來決定的—可容忍遺失的最大電子標籤個數 m 以及指定一個機率值 α 作為可偵測出超過 m 個遺失狀況的成功率。Tan、Sheng & Li 進一步的分析，推導出 n、f、m、α 間的關係，從機率的觀點定出機率函數 $g(n, x, f)$ ，該函數代表的是 n 個電子標籤，摘要值長度為 f 且實際遺失電子標籤數為 x 時，能偵測到遺失電子標籤的機率，並從此函數推導出 f 的最佳值是 $f = \min\{ x|g(n, m+1, x) > \alpha\}$。舉例來說，假設 n=10，m=2，α=0.95 時，f 的最佳解為 18，也就是在 f=18 時，遺失電子標籤數超過 2 以上能被偵測出來的機率是超過 0.95 的，可是在原文敘述中，可能讓我們誤解這樣的機制是很安全的，高達 0.95 的成功監控能有效做到損害控制，但實際狀況真是如此嗎？當這個機制發生了 0.05 機率的遺失電子標籤數超過 2 個以上而未偵測出來，若損失的幅度是可能遠大於 2 件商品，這樣的監控系統將無法令人安心！

接下來我們舉個例子來說明：假設有 10 個需監控的電子標籤，摘要值長度 f 設為 18，可容忍遺失的最大電子標籤個數 m 設為 2，偵測出遺失 m+1 個電子標籤的最低要求機率 α 設為 0.95，這 10 個電子標籤所計算出來的 sn_i ($sn_i = h(id_i \oplus r) \bmod f$)分別為有 5 個是 1，另外 5 個是 2，當讀取器進行查詢時可收集到的位元字串是 1100000000000000，由於發生碰撞，所以位元為 1 的部份集中在兩個位置，若 sn_i 為 1 及 2 的電子標籤各剩下一個未遺失，當讀取器進行查詢時，仍可在前兩個位置得到回應，所以收集到的位元字串仍是 1100000000000000，這個結果回傳給伺服器作比對，將與正確結果相同，不會發出警示訊息，但是實際上的遺失已達電子標籤個數的 80%。

從以上例子可以發現，可能會出現遺失電子標籤數已超過門檻值 m，但是系統卻無法發現。TRP 協定的作者們以機率方式討論出遺失 m 個電子標籤可偵測出的機率，但也說明仍有 1-α 的機率是偵測不到遺失，然而根據上述例子，並以一個可實際應用的系統來說，雖然只有 0.05 的機率會無法偵測到可容許的遺失，然而，這 0.05 的機率卻可能包含了遺失 80%電子標籤的結果，這樣的風險是否可被接受，是需要考慮的。

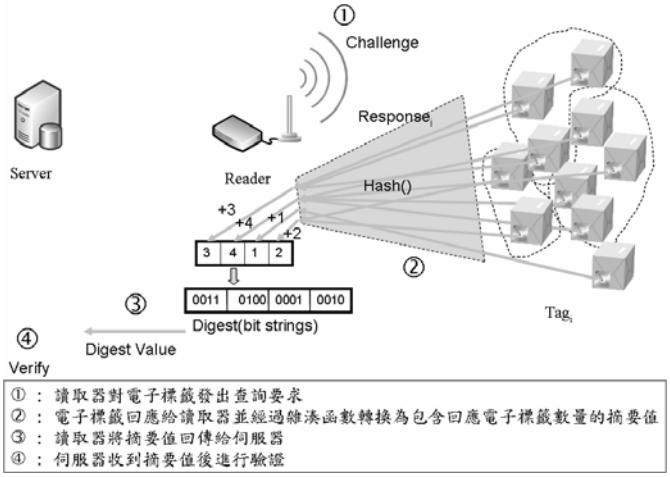
另外，一般來說，電子標籤的代碼是可公開的資訊，也就是說惡意者可經由一般的讀取器先得知電子標籤代碼，再加上竊取 TRP 協定中讀取器傳遞給電子標籤的摘要值長度與亂數種子，便可以得知讀取器在廣播查詢過程中，電子標籤在哪些時候會有回應，因此可藉由設置假電子標籤來回應給讀取器而達到竊取電子標籤的目的。

五、我們的設計

基於前一節中所提出 TRP 的兩大問題，我們提出改良的設計，首先為了避免可能被設置假電子標籤的情況，因此將整個設計中所有使用電

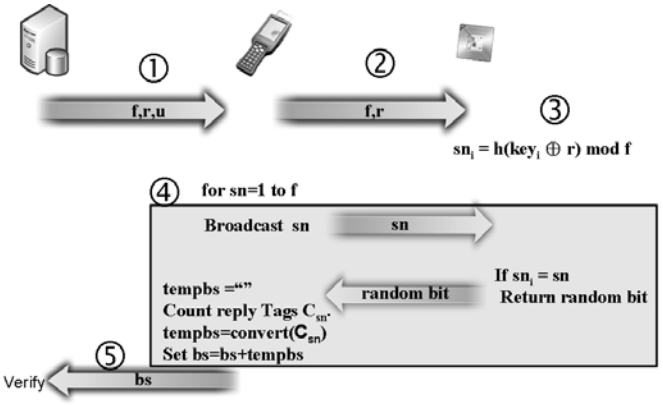
子標籤代碼的部份，改為使用電子標籤金鑰，因為電子標籤金鑰值僅為伺服器與電子標籤所共有，且不可公開，更適合用來做電子標籤識別的計算。

其次，原來的方法中，尚有 1-α的機率可能無法偵測出電子標籤的遺失而導致極大的損失。所以若能達到 100%的偵測出遺失電子標籤，則更具有應用上的價值。也就是說，若能將每次廣播時回應的電子標籤數量記錄下來，便可以準確的知道電子標籤的遺失狀況。而根據 EPC 的規格[9]，當讀取器對電子標籤進行廣播查詢時，若同時有多個電子標籤回應，讀取器可統計出此次廣播查詢所回應的電子標籤數。所以我們應用此特性，讓讀取器每次發出查詢要求時，將回應的電子標籤個數記錄下來，並且將回應的電子標籤數量同樣轉換為位元字串，最後將所有查詢結果的位元字串合併後回傳伺服器做驗證，如此一來，傳輸資料量並不會擴張太多又可達精確目的(如圖六)。



圖六 我們的設計

接下來，我們將改良方式做一個說明，整個的運作流程可分為兩個階段(如圖七)：



圖七 我們的設計

第一個階段為準備階段：

這個階段中伺服器除了決定摘要值長度及雜湊函數所需要的種子外，須多決定一個數字 u，這個數字是用來決定可表達電子標籤個數的最小位元長度，以下為此階段的執行步驟：

步驟 1. 伺服器決定摘要值長度 f、隨機產生亂數種子 r 以及表示電子標籤總數 n 所需的最小位元數 $u(=\log_2 n)$ ，並且將(f, r, u)傳送給讀取器。

步驟 2. 讀取器將摘要值長度 f 、亂數種子 r 廣播給所有電子標籤，並產生長度為 f 個單位的計數字串(其中每個計數單位大小為 u 個位元)。

步驟 3. 每個電子標籤收到(f,r)後，與自己的電子標籤金鑰一起計算出雜湊值 sn_i。

$$sn_i = h(key_i \oplus r) \bmod f \qquad (2)$$

第二個階段為執行階段：

由於在前面的步驟中，所有的電子標籤已將各自的雜湊值計算好，所以接下來的步驟 4~步驟 5，讀取器依序發出查詢要求，並且計算每次查詢回傳的電子標籤個數，最後產生計數字串。

步驟 4. 讀取器依序廣播 1 至 f，每次廣播，完成以下動作：

步驟 4.1. 當電子標籤收到讀取器廣播的值時，便與自己先前計算出來準備好的 sn_i 值做比對則發出一個簡單回應訊

息給讀取器，若不相等則該電子標籤不做任何回應。

步驟 4.2. 讀取器收到電子標籤的回應，計算所有回應的電子標籤個數，並將其計數值填入對應之計數字串位置。

步驟 5. 讀取器將計數字串回傳給伺服器驗證。

當伺服器收到由讀取器回傳的計數字串後，首先利用一開始決定的計數單位大小 u 個位元，將計數字串還原回一組讀取器執行的各次查詢所獲得回應的電子標籤個數，接著將伺服器資料庫中的電子標籤記錄，依同樣函式做計算來產生另一組電子標籤個數，將兩組電子標籤個數依序計算差值，每個差值代表的是電子標籤的遺失，所有的差值相加即代表遺失的電子標籤個數，若高於系統定義的可容忍遺失的最大電子標籤個數 m，系統就必須發出警示。

六、範例

舉例來說，假設有 10 個需監控的電子標籤，摘要值長度 f 設為 18，計數字串單位大小 u 為 4 個位元，可容忍遺失的最大電子標籤個數 m 設為 2，這 10 個電子標籤所計算出來的 sn_i ($sn_i = h(key_i \oplus r) \bmod f$)分別為有 5 個是 1，另外 5 個是 2，當讀取器進行查詢時可收集到的電子標籤個數的計數字串是 5500000000000000000，若 sn_i 為 1 及 2 的電子標籤各剩下一個未遺失，當讀取器進行查詢時，收集到的電子標籤個數的計數字串是 1100000000000000000，這個結果回傳給伺服器後，伺服器依資料庫記錄以同樣的函式計算產生的計數字串 5500000000000000000 不同，逐一計算差值可發現總共有 8 個電子標籤短少。

七、結論

我們改良 TRP 後的方法，不僅同樣承襲了 TRP 以下的優點：

(一) 讀取器不須直接收集電子標籤代碼，仍可達到精確的監控遺失電子標籤的效果。

(二) 不需公開傳遞電子標籤代碼，因此可保有電子標籤的隱私性。

(三) 不需昂貴的硬體設施也不需要在電子標籤上設計 MAC 功能。

(四) 整個設計不限制監控的電子標籤數量，更具有彈性。

並且更進一步加強了精確性，還解決了 TRP 中有 1-α 的機率所可能產生無法控制的損害。雖然就目前來說 RFID 仍有價格上的考量，若要推廣至較屬於低價的一般零售業，會有不少的困難，但是就長遠的市場來說，先以高價商品如 3C 專賣店或是精品店為現行目標，配合 RFID 的發展進程，逐漸朝向普遍性零售業來發展，應對商品的存貨控制有其實用價值。

八、參考文獻

[1] 許文誠，“行動無線通訊應用於零售業盤點作業之研究—以西點麵包零售業為例”，淡江大學，2003 年 6 月。

[2] D. Henrici and P. Müller, “Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers”, Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp.149-153, Mar, 2004.

[3] Richard Hollinger, “2008 National Retail Security Survey : Preliminary Results”, A Town Hall Meeting with Dr. Richard Hollinger, 2008

[4] S. M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim, “Efficient Authentication for Low-Cost RFID systems”, International Conference on Computational Science and its Applications - ICCSA 2005, pp.619-627, 2005.

[5] Alex X. Liu and LeRoy A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags", Computer Communications, Vol. 32, No. 7-10, pp. 1194-1199, May28, 2009.

[6] C. C. Tan, B. Sheng, and Q. Li, “How to Monitor for Missing RFID Tags”, The 28th International Conference on Distributed Computing Systems, 2008.

[7] S. Weis, S. Sarma, R. Rivest and D. Engels,

“Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, in 1st Intern. Conference on Security in Pervasive Computing (SPC), Boppard, Germany, March 12-14, 2003.

[8] Asiainfo, “分散式監控系統之概念”, http://www.asia-info.net/detail_mech.asp?id=919

[9] EPCglobal, http://www.epcglobalinc.org/standards/

[10] 維基百科,”條型碼”, http://zh.wikipedia.org/wiki/%E6%A2%9D%E7%A2%BC