感測網路的安全資料彙集機制之概觀
A Survey of Secure Data Aggregation on Sensor Networks

陳煜弦 [1] 蕭旭君 [2] 雷欽隆 [3]
國立台灣大學電機工程學系
{ [1]ethan, [2]matelda }@fractal.ee.ntu.edu.tw [3]lei@cc.ee.edu.tw

摘要

本論文提供各種無線感測網路安全彙集機制研究的概觀，歸納出安全資料彙集的共通模型，並概述幾個比較可行且著名的安全彙集機制，歸納發展趨勢。接著介紹從最早的 SIA 以及到 2006 年以前接續的各種研究，以及 Wagner 以統計方式分析彙集函數的強固性等，這些研究多受限於特定的環境條件或是使用過於繁瑣的協定，無法完整解決感測網路資料彙集所面臨的困難。最後介紹 2006 年以來 Proof sketches、CPS 與 EVIA 等更全面的方案。讀者可從中得到安全彙集機制發展的脈絡。

關鍵詞：aggregation, sensor networks,

壹、前言

無線感測網路是近年計算機科學研究的熱門焦點，其重要性不言而喻。關於感測網路的安全議題有很多層面。最基本的兩個主題是感測節點本身的防護，以及路由的安全。前者較偏向機械性的設計，通常會以 TPM 的方式來處理；後者則較為複雜。感測網路的安全性起先也多環繞在這兩個議題上，本質上這都是網路層以下至實體層的問題。隨著感測網路的技術日益成熟，應用層的安全也開始被考慮。但感測網路的應用簡言之就是資料的收集，為了節省頻寬與運算，收集資料的同時進行資料的彙集（aggregation），感測與彙集其實就是感測網路最主要的功能。2003 年[18]後，開始有學者探討感測網路中如何實現安全資料彙集，陸續有不少研究被發表。多數研究從較簡易的模型出發，例如只考慮平坦（非階層）的網路結構，或是設計繁瑣的通訊協定，因此難以沿用於真正的實作上，2006 年後才有較全方面的機制出現，但離真正強化資料彙集的安全，事實上還有一段差距。

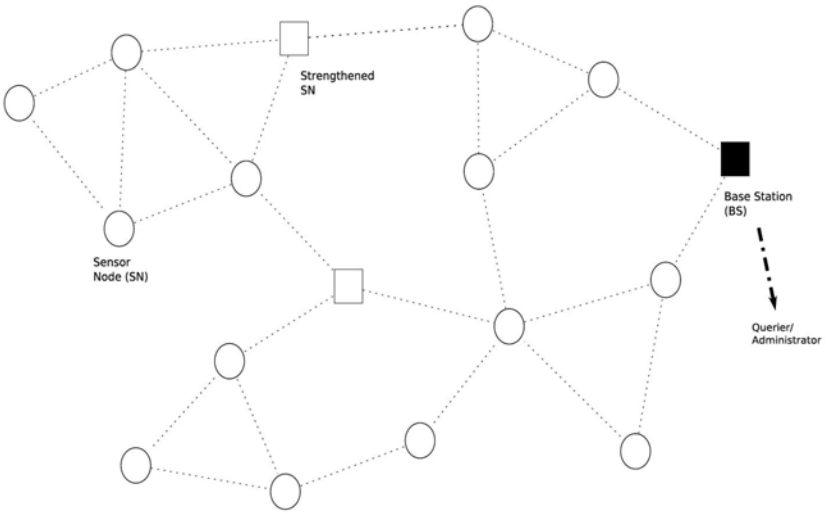
雖然這裡所提到的彙集機制是用在無線感測網路，但許多電腦網路上需要彙集功能的應用，例如路由資訊的整合等，也有沿用這些安全機制的可能，事實上，不少感測網路的安全彙集機制也是改良自主從式（server-client）應用資料彙集的方法。

本論文將整合歷年感測網路安全資料彙集的研究，先介紹這個議題的通用模型以及所面臨的問題。接著簡介歷年來主要的安全機制，提供讀者對這個問題的概觀，作為研

究與開發的參考。

貳、問題模型

一個基本的無線感測網路通常由一個或少數基地台（Base Station, BS）以及眾多感測節點（Sensor nodes）所組成，基地台擁有較完整的運算能力與電力支援，作為感測網路與後端管理者的溝通閘道；個別感測節點由電量有限的電池驅動，負責感測環境變數、傳送或遞送資料封包，少部分感測節點也許有比一般節點更多的資源，用以輔助加強網路的功能，例如許多感測網路協定內使用多個叢集頭（cluster head）強化局部網路的運算。感測網路的最主要任務就是蒐集各項環境指數，因此多數的作業是將感測到的數值傳送回基地台，經由基地台遞送回給管理者。但對資源有限的感節點而言，傳送過長的資料就必須耗損更多的電量。此外，網路中充斥越多的封包，發生錯誤的機率也就越高，更多封包必須被重送，對頻寬無疑是種浪費。圖一為一感測網路的圖例。

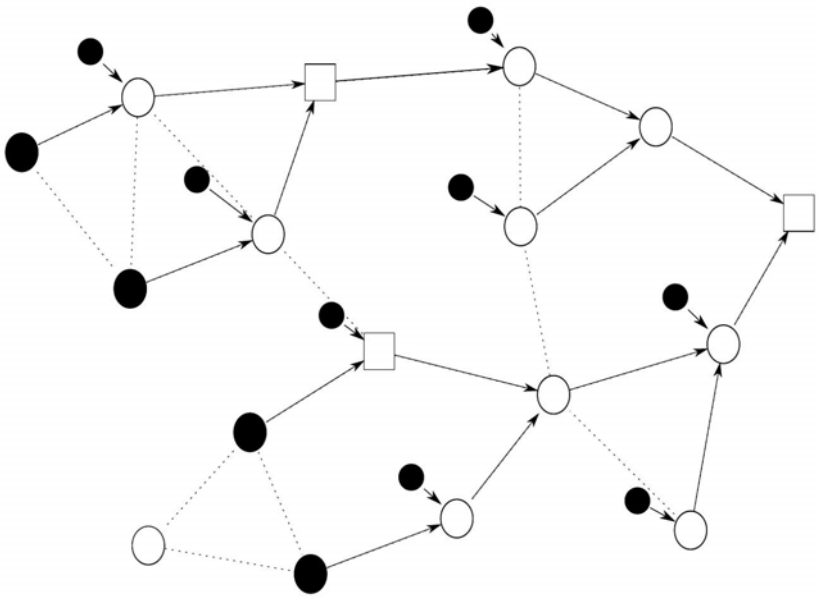


圖一：感測網路模型

感測節點所傳送的資料通常多為管理者所要求的數值讀數，一般而言管理者並不需要所有的讀值，只需要這些讀值經過函數處理後的統計結果。以資料庫的觀點而言，最基本的五種函數為 SUM、COUNT、AVERAGE、MIN、MAX，這些函數可以組合出更複雜的函數。基本上 COUNT 就是 SUM 的特例，AVERAGE 是 SUM 的延伸。以感測網路的應用而言，需求量最大的函數就是 SUM 此類。

一般而言查詢者（querier）本身即是系統管理者，而各節點的讀數如果能在傳遞繞送的過程中同步被函數處理，便可大大降低傳送的封包量以及末端的工作量。在封包傳遞路徑上執行這些函數的節點被稱為彙集者（aggregator），彙集者通常本身也是感測節

點，同時兼負感測、繞送、彙集的任務。通常資料彙集的路徑會成為在網路拓樸的樹狀子集，稱為彙集樹（aggregation tree），根就是最後的彙集者或是查詢者本身，葉子就是各感測節點，內部節點是彙集者。需要注意的是，同時兼負感測與彙集功能的節點在彙集樹上會由不同的葉與內部節點來標示其不同的機能。圖二為對應圖一的彙集樹示意圖：黑色節點表示感測機能，白色節點代表彙集者。



圖二：對應圖一的彙集樹

同樣以安全資料彙集為題，不同的研究指涉的彙集函數卻不盡相同。Huebsch[9]等人提出了三種分類方式，將彙集函數以是否為線性型（linear）、對複本遲鈍型（duplicate insensitive）、通用型（general）分門別類討論。依照他們的分類方式，安全資料彙集的研究大部份著重於線性型且 duplicate sensitive 的部份，亦即是 SUM、COUNT、AVERAGE 等函數。

在不考慮安全因素的狀況下，資料彙集的動作並不困難，只要在彙集樹上的內部節點依照所指示的函數執行彙集即可。但感測網路通常處於不確定的環境，暴露在外的感測節點遠比一般伺服器更容易被滲透或攻破。位於網路後端的管理者（或查詢者）難以察覺個別節點所遭遇的狀況，因此攻擊者可以藉著少數被瓦解的節點影響查詢的結果。尤其在彙集的功能被執行時，攻擊者可以鎖定在彙集樹上越接近根的彙集者，可對彙集結果產生更大的扭曲。因此，基本的彙集作業在無線感測網路內顯然是不完善的，為了確保查詢者可以得到正確的資訊，比須有適當的安全機制作為基礎。

特別要澄清的是，一般感測節點被捕獲與彙集者被攻破是兩種不同的情況。任何一個感測節點被捕獲，攻擊者都可藉此回覆任意偽造的讀值給查詢者，一般來說查詢者很難分辨真實的與偽造的感測資料，最後的彙集結果必然會產生偏差。這類攻擊稱為『直

接資料植入』(direct data injection):攻擊者直接由受其控制的感測節點傳送不真實讀值的攻擊。這種類型的破壞並非加諸於彙集機能上的安全機制所可以處理,因此通常不在安全彙集機制的處理範圍內。安全彙集機制所要對付的是惡意的彙集者試圖竄改或隱藏所收到的部分感測資料並上傳不真實的彙集結果。當然彙集者本身常也是一個感測節點,攻擊者大可直接竄改自身的讀值,不過學理上這屬於前述感測節點被攻破的狀況,不列入考慮。

另一個常令人混淆的狀況是阻斷式攻擊,這類型的攻擊包含破壞節點或無線訊號等,其目的是使查詢者無法正常接收查詢結果。可以達到這種目的的攻擊有很多種方式,但在感測網路的應用中通常也不列入考慮,理由是如果攻擊會導致管理者察覺攻擊的存在,那管理者自然會排斥接受不確定的資料結果,並且進行後續的系統檢查。以攻擊者的角度來看,這種結果除了擾亂系統運作外,對攻擊者並沒有進一步的好處,更可能因此暴露攻擊者的所在。

因此,在此所探討的攻擊模型限定於 Przydatek [18]等所定義的隱蔽攻擊(stealthy attack),意指誤導查詢者接受被竄改的彙集結果,被竄改的結果可能高或低於真正原始的數值,攻擊者會試著隱藏自身的存在,以利後續的攻擊。簡言之,安全的彙集機制的目標在於防止惡意的彙集者竄改其下游的資料。攻擊者除了直接資料植入外,無法藉著操控資料彙集過程來誤導查詢者接受彙集結果,則此資料彙集機制是『最佳安全(optimally secure)』的。攻擊者如果意圖提高彙集結果的數值,這種攻擊稱為『膨脹』(inflation),反之則稱為『緊縮』(deflation or suppression)。

依照驗證(verification)發生的地方不同,可以分為兩種:分散式(distributed)驗證和集中式驗證。後者的驗證程序集中在少數幾個節點(例如基地台或叢集頭),前者則是將驗證的工作分散在每個節點上。除了判斷資料是否有遭受惡意竄改,更進一步地,未來的研究將著眼於找出受到攻擊者掌控的節點並設法移除。

綜觀來看,安全彙集機制所能保護的範圍似乎有限,感測節點被攻破或是阻斷式服務攻擊都可輕易破壞彙集結果。但本質上這是不同的議題,即便有良好的機制可以防治阻斷式攻擊或攻破節點,彙集過程缺乏安全設計仍將造成系統漏洞。安全彙集機制所設定的模型乍看似乎過於理想,實際上卻是整體感測網路安全與效能不可缺的環節。

在感測網路中實現安全機制所遭遇兩大困難:其一是路由的複雜度,這是無線隨意網路所必然面臨的困境;其二是感測節點有限的運算能力,這使得不只是彙集而已其他許多和安全有關的功能都只能使用簡易的密碼學運算,不過這種狀況正在改善,稍後會再做說明。

參、早期研究

Wagner's statistical analysis

2004 年 Wagner[19]提出了各種安全彙集的數學分析，討論直接資料植入對各種匯集函數的危害程度。其模型是假定攻擊者可捕獲 n 個節點當中 k 個節點的狀況下，函數的強固性（resilience）。

aggregate (f)	error ($\mathrm{rms}(f)$)	resilience (α)	(ϵ^*)	security level
minimum	—	∞	0	insecure
maximum	—	∞	0	insecure
sum	$\sqrt{n}\cdot\sigma$	∞	0	insecure
average	$\sigma/\sqrt{n}$	∞	0	insecure
$[l,u]$-truncated average	$\sigma/\sqrt{n}$ or larger	$1+(u-l)/\sigma\cdot k/\sqrt{n}$	—	problematic
5%-trimmed average	$(1+\epsilon)\cdot\sigma/\sqrt{n}$	if $k<0.05n$: $1+6.278\,k/n$	0.05	better
		if $k>0.05n$: ∞		
median	$1.253\sigma/\sqrt{n}$	if $k<n/2$: $\sim\sqrt{1+0.101k^2}$	0.5	much better
		if $k>n/2$: ∞		
count	$\sqrt{n\theta(1-\theta)}$	$1+O(k/\sqrt{n})$	—	acceptable

表一：Wagner 對彙集函數的強固性（resilience）分析結果

Wagner 並未論及安全彙集機制，因為他所考慮的是感測節點的安全而非會集者的安全，但是提供了幾項補救措施，協助查詢者盡量排除不真實讀值對整體結果的影響。其作法有兩種：一是忽略差異過大的讀值，例如忽略超出正常感測讀值範圍的數據，或是忽略某信賴區間外的數據；二是對不同的彙集函數採用不同的估計子（estimators）以提高正確率。

SIA: Secure In-network Aggregation

Przydatek[18]等人於 2003 年提出最早用於感測網路的安全彙集機制：SIA。SIA 考慮只有單一彙集者的模型，所有的感測節點將結果傳送至該彙集者，由彙集者除了執行彙集，並以 Merkle 雜湊樹的架構將個別感測數值雜湊成一個驗證值（commitment），這個動作稱為 Commit，隨後傳送彙集結果與驗證值給查詢者。為確保資料的正確，查詢者與彙集者隨後會執行一連串的互動證明（interactive proof），在多次互動後，查詢者可確認彙集者是否依法行事。這個 aggregate-commit-proof 模型的安全度主要憑藉於統計上的機率測試，並未使用到任何複雜的計算函數。但最大的缺點在於限定只有一個彙集者的平坦架構，以感測網路的規模與佈置來說，並沒有充分利用到彙集的功能（可以想見多數的感測網路會是網狀架構），仍然會消耗許多通訊頻寬。這個方式可處理 MEDIAN、MAX、MIN 等常用的函數，不過每種函數都有個別的互動證明演算法。SIA 所使用的統計方式具有參考價值，但並不適用於通訊頻寬有限的感測網路。

以下是查詢者與彙集者稽核 MEDIAN 的演算法：

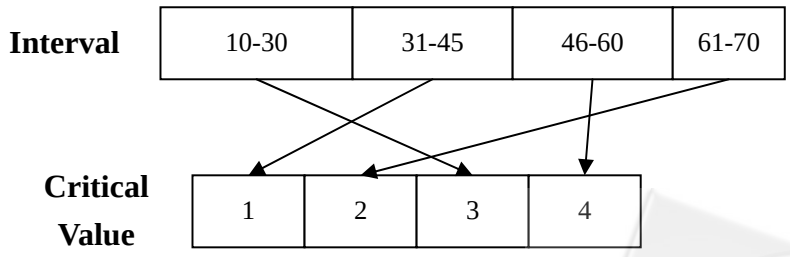
```
procedure MedianCheck(n, a_med, ε):
  request a_{n/2}
  if a_{n/2} ≠ a_med then
    return REJECT
  for i = 1 ... (1/ε) do
    pick j ∈_R {1 ... n} \ {n/2}
    request a_j
    if j < n/2 and a_j > a_med then
      return REJECT
    if j > n/2 and a_j < a_med then
      return REJECT
  return ACCEPT
```

圖三：MedianCheck

原則上查詢者就是在收到彙集結果後再送出多次隨機的索引給彙集者，要求彙集者提供索引所對應的數值，以驗證方才收到的結果。由於所有感測讀值理應經過單向雜湊處理，惡意的彙集者難以在驗證時偽造合格的讀值。理論上，在$O(\log n/\varepsilon)$驗證次數下，彙集者成功欺騙查詢者的機率小於$(1/\varepsilon)^{\log n}$，其中 n 為節點個數。

其他研究

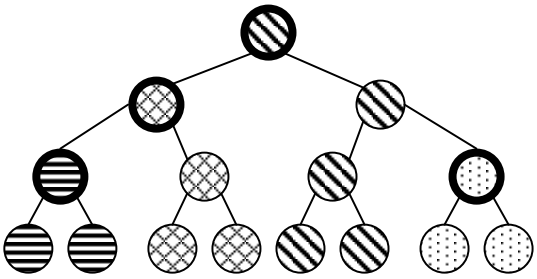
Cam 等人[2]提出 pattern code 的概念，叢集頭可以藉由比對 pattern code 避免重複傳輸類似的資料。舉例而言，若感測節點 A 在一段時間內的讀值為（25, 66, 29），根據圖一，其傳給叢集頭的 pattern code 為 321。如果感測節點 A 傳送的 pattern code 也是 321，那麼叢集頭只會要求 AB 兩者其中之一回傳真實的讀值。這種彙集函數可算是非線性且對複本遲鈍型（duplicate insensitive）的類型。



圖四：pattern code

Yang [20]等人指出知情不報，也就是『緊縮』（suppression）攻擊，是彙集的致命傷，基地台很難察覺是否有被攻破的節點試圖隱瞞事件的發生。作者們聲稱它們提出的機率

性編組（probabilistic grouping）技巧可以有效減緩此類攻擊造成的傷害。機率性編組的運作方式如下：首先以基地台為根（root）、網路中每一個感測節點為節點，展開成樹狀結構。感測節點將其 ID 以及此次得到的階段金鑰（session key）放入雜湊函數中演算，若大於某個臨界值，便宣告自己為叢集頭。圖五的範例展示了使用機率性編組後，叢集頭如何決定其成員集合。圖中相同背景者屬於同一個叢集，雙線框者為叢集頭。這種動態分組的策略，使得攻擊者無法藉由掌控少數重要節點進而掌控整個網路。



圖五：機率性編組

由於感測節點網路先天上為分散式的架構且有電源與計算量的限制，因此安全機制必須仰賴感測節點之間的互助合作。例如 Du[6]等人以 witness-based 的方式，讓 witness nodes 監視 data fusion node 送出的結果；或是 Mahimkar[15]等人根據門檻式簽章（threshold signature）的概念，一個 n 成員的叢集內最多有 t 個被攻破的感測節點才能顛覆傳送給基地台的資料；也有許多機制採用類似 commit-and-attest 的方式，如 Yang[20]等人。

肆、近期研究

Proof Sketches

Garofalakis[7]等人於 2006 年提出了很特別的方式，有別於通訊或密碼的思維，他們採用處理大量資料的統計技巧。如同 TinyDB，他們將感測網路視為一個大型資料庫，以著名的 Flajolet-Martin （FM） sketches 技巧來處理感測資料。以 COUNT 為函數原型，每個感測節點感測值為 0 或 1，如果感測值為 1 則該節點將 1 串聯其 ID 經過雜湊後得到一亂數字串，除了最小位（least significant）的『1』外，字串上其他位元都歸零，然後所有節點得出的字串一起經過互斥或（XOR）運算，結果就是 FM-sketch；如果感測值為 0 則不傳送。由機率上不難得出，越往高位元看去，被設成 1 的機率成等比遞降，因此，FM-sketch 字串中位元數最高的 1 的位元數就是總體計數的估計指標。簡化後的 proof sketches 基本上就是 FM-sketch，彙集者的行為就是對個別的 sketch 做互斥或運算。

為了提升彙集的安全度，proof sketches 要求感測節點除了傳送 FM-sketch 外，必須附上簽章，但是彙集者只會選取 sketch 中被標記為 1 的位元數最高的節點的簽章繼續上傳，如果這樣的下游節點有多個，就會隨機選取一個。最後查詢者所收到的簽章，會是產生

最高位元 1 的 sketch 的節點的簽章，稱為 authentication manifest （AM）。整個機制就稱為 AM-FM sketches。

Proof sketches 可以制止『膨脹』攻擊的發生，因為攻擊者難以偽造出符合雜湊規範的 sketch 值，同時又產生合格簽章。但是惡意的彙集者可以蓄意丟棄下游的資料，達成『緊縮』攻擊。為此，proof sketches 提供很簡單的解法，只要同時互補的 0 的次數，最後與 1 計數的結果相加，成功的彙集結果應該是所有感測節點的個數。

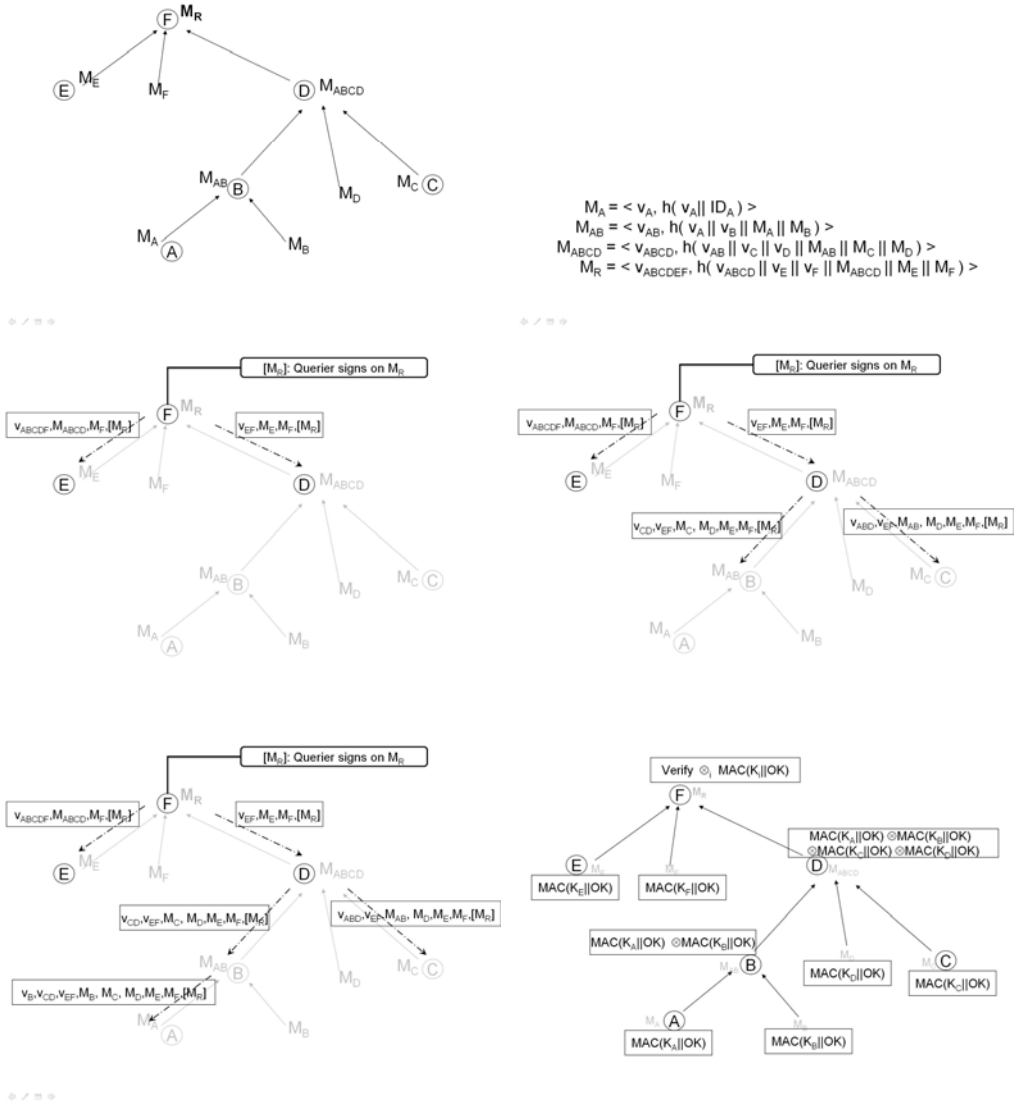
Proof sketches 提供了一個非常特別的優點：對複本遲鈍性（duplicate-insensitive），意指彙集者從各方接收到同一來源的同一筆感測資料時，自然會結合成單一筆資料，這得力於 FM-sketch 中 XOR 的設計。這樣的特性在實作上有極大的優勢，封包可以不循特定的繞送路徑，彙集『樹』可以擴張成彙集『網』。只要封包朝著基地台的方向繞送並彙集，儘管同一封包被多個節點重複繞送也無所謂，這大大降低路由的複雜度。這也表示了任何網路拓僕都可沿用這個機制。這也表示了每一次查詢只需要一回合就可以完成。

Proof sketches 以 COUNT 函數為基礎，理論上可以建構出各類彙集函數，只是複雜的彙集函數就需要更多次的查詢動作。但 proof sketeches 畢竟是提供估計值，對於需要精確彙集結果的應用就較不適用。

CPS

同樣在 2006 年， Chan [4]等人以 SIA 為基礎，提出了階層式的安全資料彙集機制，以下簡稱 CPS。CPS 延續 SIA 使用 Merkle 雜湊樹的邏輯，但這次將彙集樹的結構對應到 Merkle 雜湊樹。CPS 以 SUM 函數為基礎，將檢驗的工作分散給每一個感測節點。CPS 區分成『送出查詢』（query dissemination）、『彙集擔保』（aggregation commit）與『檢查結果』（result-checking）三個階段。送出查詢顧名思義是查詢者對網路散佈查詢要求。第二個階段是資料回傳和彙集的過程，每一個彙集者除了進行彙集（加函數）外，並將自身 ID、下游節點 ID 及其彙集資料與彙集結果輸入公開的雜湊函數中，彙集結果串聯雜湊值給上游節點；所謂的擔保（commit）就是運算雜湊。當最終的彙集結果送至查詢者後，查詢者以自己的私密金鑰簽署，再散佈回網路中進行第三個階段。查詢上事實上已經取得彙集結果，第三個階段是為了遏止攻擊者再前一個階段進行破壞，所以其實是本機制最重要的過程。沿著原先的彙集樹逆向往下游，查詢者的簽章被遞送到每一個節點，此外，每個節點還會收到原傳遞路徑上所有『旁系』（off-path）節點的資料，因此每個節點都可驗證上游節點是否正確處理其資料。系統設定每個感測節點都知道查詢者的公開金鑰，因此可以驗證查詢者的簽章。感測節點如果驗證通過，就會傳遞一個以自己的私鑰產生的訊息認證碼（message authentication code, MAC），其內容是很簡單的『OK』合併查詢編號（query number）等類似訊息。類似資料的彙集，接著會進行認證碼的彙集。彙集者會將其收到的認證碼做互斥或（exclusive-OR, XOR）運算並繼續上傳。最後查詢者等同收到一個所有感測節點的認證碼的互斥或結果。由於查詢者知道所有節點的私鑰，因此可預先推算出如果每個節點都驗證通過，那最後回覆的結果應該為何。如

果結果符合預期，查詢者便接受這次彙集，反之亦然。對於不對稱的彙集樹架構，CPS 進一步訂出更細緻的擔保規則，以降低通訊量。



圖六：CPS

CPS 的優點是僅使用到簡單的運算，雜湊與訊息認證碼對感測節點而言都不算困難的運算。而且 CPS 也不受限於特定的網路拓樸，只要在彙集與檢查的過程中維持彙集樹的架構就好。

但 CPS 需要兩回合才能完成查詢，特別是檢查的手續需要傳送比原本資料更多的內容，其實製造了許多通訊量。而且在不穩定的無線環境中，完成一回合的傳輸已屬難得，還要以同樣的彙集樹進行第二回合並傳送更多的資料成功率更低。每一個節點都必須存

活且網路結構穩定的條件實際上並不容易達成。

EVIA

Chen[5]等人提出較偏重密碼學的安全彙集機制EVIA，試圖兼併proof sketches與CPS的優點。EVIA 的特別之處是讓每個感測節點都對資料產生簽章，資料彙集的同時也彙集簽章。傳統上的簽章相當於是亂數化後的結果，很難想像簽章可以在被彙集後還有任何意義。所以 EVIA 所定義的簽章演算法事實上是同代像（homomorphic）函數，例如EVIA 所用的指數運算。

在 EVIA 內，查詢者替每個感測節點 i 設定其隨機產生金鑰 a_i 、 b_i 和 δ_i 滿足

$a_i c + b_i d \equiv 1$

其中 c 、 d 是查詢者的私鑰，在網路佈建前，查詢者預先將私密金鑰 α_i 、 β_i 和 δ_i 安置入節點 i 的記憶體。

$$\alpha_i \leftarrow g^{a_i}$$
$$\beta_i \leftarrow g^{b_i}$$

是 Z_p 內的產生器。所有的運算在密碼學常見的 Z_p 交換群內。

節點 i 感測到資料 m_i 後產生簽章 (r_i, s_i) ：

$$r_i \leftarrow \alpha_i^{m_i+\delta_i}$$
$$s_i \leftarrow \beta_i^{m_i+\delta_i}$$

而彙集者 j 所需進行的動作：

$$m_j \leftarrow \sum m_i$$
$$r_j \leftarrow \prod r_i$$
$$s_j \leftarrow \prod s_i$$

彙集者對最後的彙集結果 (m_l, r_l, s_l) 進行檢驗：

$$r_l^{\,c} s_l^{\,d} \equiv g^{m_l} g^{\sum \delta_i}$$

如果上式成立，則接受彙集結果。由於查詢者設定所有的 δ_i ，因此可以進行此步驟。進一步的設計是以雜湊處理每一次查詢所使用的 δ_i ，就可以避免重送攻擊。

EVIA 有一點與其他以往安全彙集函數相當不同之處，EVIA 很大膽的使用了指數運算或橢圓曲線密碼學，而傳統上這被視為非常不適合感測節點所用的演算法，因為以一般感測節點的運算能力執行這種計算會消耗太多時間與電量。作者們的論點是，感測模組的技術並非普遍認知的那樣貧弱，事實上新一代的感測模組已經具備相當的計算力，足以輕鬆應付以往認為不可行的密碼學運算，這點在 TinyECC 的實驗數據上可見端倪。研究人員需要考慮的反而是如何降低整體網路的通訊量，因為通訊所需的電力與時間仍

是感測網路的致命傷，而一回合完成查詢的 EVIA 正符合了這樣的需求。

伍、結論

總結來說，彙集機制的安全性可由兩種數學技巧強化：一種是藉著統計學排除不真實的資料，例如 Wagner[19]所列舉的分析，以及 proof sketches 使用的 FM-sketch；另一種是藉密碼學防止彙集者竄改他人資料，例如 Merkle 雜湊樹的引入以及簽章等。兩種手段並非互斥，也許融合兩種技巧才能有最合適的機制。

參考文獻

[1] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. “Aggregate and verifiably encrypted signatures from bilinear maps.” In *Advances in Cryptology – EUROCRYPT*, pages 416–432, 2003.

[2] H. Cam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, and H. O. Sanli. “Energy-efficient secure pattern based data aggregation for wireless sensor networks.” *Computer Communications*, 29: 446--455, 2006.

[3] C. Castelluccia, E. Mykletun, and G. Tsudik. “Efficient aggregation of encrypted data in wireless sensor networks.” In *MobiQuitous*, pages 109–117, 2005.

[4] H. Chan, A. Perrig, and D. Song. “Secure hierarchical in-network aggregation in sensor networks.” In *ACM Conference on Computer and Communications Security*, pages 278–287, 2006.

[5] Y. S. Chen, J. M. Hellerstein, and C. L. Lei. “EVIA: Efficient and verifiable in-network aggregation for sensor networks.” In *iCAST/TRUST/CMU Joint Conference*, 2007

[6] W. Du, J. Deng, Y. Han, and P. K. Varshney. “A witness-based approach for data fusion assurance in wireless sensor networks.” In *Proceedings of the IEEE Global Telecommunications Conference*, 2003.

[7] M. Garofalakis, J. M. Hellerstein and P. Maniatis. “Proof Sketches: verifiable in-network aggregation.” In *ICDE*, 2007.

[8] L. Hu and D. Evans. “Secure aggregation for wireless network. In SAINT Workshops, pages 384–394, 2003.

[9] R. Huebsch, M. Garofalakis, J. M. Hellerstein, I. Stoica. “Sharing aggregate computation for distributed queries.” In *SIGMOD* 2007.

[10] P. Jadia and A. Mathuria. “Efficient secure aggregation in sensor networks.” In *HiPC*, pages 40–49, 2004.

[11] M. Jakobsson, K. Sako, and R. Impagliazzo. “Designated verifier proofs and their applications.” In *Advances in Cryptology – EUROCRYPT*, pages 143–154, 1996.

[12] A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham. “Sequential aggregate signatures from trapdoor permutations.” In *Advances in Cryptology – EUROCRYPT*, pages 74–90, 2004.

[13] R. C. Merkle, “A certified digital signature”, In *Advances in Cryptology – CRYPTO* 1989.

[14] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong. “Tag: A tiny aggregation service for ad-hoc sensor networks.” In *OSDI*, 2002.

[15] A. Mahimkar and T. Rappaport. SecureDAV: “A secure data aggregation and verification protocol for sensor networks.” In *Proceedings of the IEEE Global Telecommunications Conference*, 2004.
[16] E. Mykletun, J. Girao, and D. Westhoff. “Public key based cryptoschemes for data concealment in wireless sensor networks.” In *ICC* 2006.
[17] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. “Spins: Security protocols for sensor networks.” In *Wireless Networks*, 8（5）:521–534, 2002.
[18] B. Przydatek, D. X. Song, and A. Perrig. “SIA: secure information aggregation in sensor networks.” In *SenSys*, pages 255–265, 2003.
[19] D. Wagner. “Resilient aggregation in sensor networks.” In *Proceedings of the 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks*. 2004.
[20] Y. Yang , X. Wang , S. Zhu , G. Cao. “SDAP: A secure hop-by-Hop data aggregation protocol for sensor networks.” In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing （MobiHoc）*, pp. 356-369, Florence, Italy, May 2006.