高延展性及高安全性的金鑰預先分配機制於階層式無線感測網路

簡宏宇
暨南國際大學
資訊管理學系副教授
hychien@ncnu.edu.tw

陳榮靜
朝陽科技大學
資訊管理學院教授
crching@cyut.edu.tw

沈安妮
朝陽科技大學
資訊管理所研究生
s9514613@cyut.edu.tw

摘要

我們提出一個新的金鑰預先分配機制，解決感測設備中金鑰協議的問題，將它套用於階層式的無線感測網路，以建立在無線感測網路中的安全傳輸通道。無線感測網路是由大量的低成本及體積小的感測節點所組成，感測節點可以透過自我組態的方式成為一個網路。由於感測節點在計算、儲存、電力及傳輸範圍有所限制，目前於傳統網路上的成熟安全機制都因計算量或儲存量過高，而無法適用。相較於現存的機制，我們所提出新的金鑰預先分配機制可以達到：1.保證網路的連通性、2.完全抵抗節點捕獲攻擊、3.不論網路節點數量，每個一般節點只需儲存固定的一把金鑰及一個對稱式多項式方程式。

關鍵字：金鑰管理、成對式金鑰、金鑰協議、階層式無線感測網路

Abstract

In this paper, we propose a new key management scheme to solve the key agreement problem among sensor devices for hierarchical wireless sensor network (WSN). A wireless sensor networks is composed of a large number of low-cost sensor node which connect each others by self-organization. Traditional asymmetric key cryptosystems are infeasible on sensor nodes, due to the limited-resource. Recently, WSN has been applied to a variety of applications, security should be ensured especially for a hostile environment. Therefore, we propose a new key pre-distribution scheme for hierarchical WSN. Compared existing scheme, our proposed scheme achieves 1.full network connectivity, 2.secure against node captured attack and 3.each sensor node only need to store one key and one symmetric polynomial functions.

Keywords: Key management, Pairwise key, Key agreement, Hierarchical wireless sensor network.

1. 前言

由於近年來微電子機械系統（Micro-Electro-Mechanical System, MEMS）技術發展躍進，研發出許多相關的應用，無線感測網路（Wireless Sensor Network, WSN）就為其中的產品之一。WSN 是由大量的感測節點（Sensor Node）所組成，其特色為成本低廉及體積小，且本身具有資料處理、感測環境及無線傳輸的功能。在沒有任何預先設定的網路架構下，感測節點可以透過自我組態（Self-Organization）的方式形成一個網路，並觀察目標所產生的變化（例如：溫度、氣壓、震度及聲音等）。感測節點以單跳躍（One-Hop）或多重單躍（Multi-Hops）的方式，將所收集到的資料傳回基地台（Base Station or Sink）以做為後端的處理及分析的依據。

無線感測網路是源自柏克萊大學（UC

Berkeley）中的一項研究計畫，由美國國防部研究計畫單位（DARPA）所資助，設計出與阿斯匹靈相同大小的感測節點，稱之為智慧灰塵（Smart Dust）[1]。一開始的應用方向是以軍事用途為主，透過低成本及體積小且大量的感測節點，佈署於敵人的區域來收集相關的資料。就特色而言，節點本身在資料處理能力、記憶體大小、傳輸範圍及電力都相當的有限。

WSN 中異質性（Heterogeneity）的網路比同質性（Homogeneous）要來得節省能源。在異質性的網路中，並非所有的感測節點設備都相同，其中一部份在計算、儲存能力、傳輸範圍及電力都優於一般節點，稱為叢集頭（Cluster Head），以此架構，形成階層式（Hierarchical）的 WSN。透過分群的演算法（有關分群的議題，可參考文獻 [13]）將所有節點劃分為數個叢集（Cluster），每一個叢集中會依各叢集的一般節點的數量，安排一個以上的叢集頭。當一般節點需要將資料傳輸至基地台時，都必須先將資料傳輸給叢集頭，這樣的做法的優點在於可以使一般節點縮短傳輸的範圍。且叢集頭接收到資料之後，可以將資料先行處理，減少不必要的資料，降低傳送資料封包的大小，進而節省感測設備的能源消耗。

隨著 WSN 的技術逐漸成熟，在各大產業中的應用也越來越多，也因此 WSN 上的安全機制的重要性也逐日提升。而如應用於軍事方面，敵方可能輕易的取得感測節點，進而讀取內部的資料，或是在節點捕獲後修改內部程式指再放置於網路中，以截取重要資訊。然而傳統網路成熟的安全機制（例如：公開金鑰基礎建設與 Diffie-Hellman key agreement）都由於計算量與儲存量過高，而不適用。基於上述的特性，使得設計 WSN 上的安全機制、入侵偵測及電力節省等方面都成了熱門的研究項目。

我們所關心的議題是如何在階層式網路中，如何使一般節點、叢集頭及基地台之間共享一秘密金鑰，即金鑰協議（Key Agreement）的問題。在本篇論文中，我們將提出一個新的金鑰分配機制用於階層式 WSN 中。與現存的其它機制相較下，我們所提出的機制中，一般節點不論網路節點的大小，都只需要儲存固定的一把金鑰及一個對稱式多項式方程式，即可支援大規模的 WSN。同時也減少了叢集頭的傳輸及計算上的成本。感測節點只要使用對方節點的 ***ID*** 即可建立一把金鑰。且可以保證整個網路的連通性，同時也可以完全的抵抗節點捕獲攻擊。

本篇文章的結構如下，第貳章節將介紹目前相關的研究，在第參章我們將提出新的機制—ESKDM 機制，第肆章針對此機制做安全及效能分析。最後第伍章節為本篇文章的結論。

2. 相關研究

欲在 WSN 上將資訊加密，就必須先解決金鑰協議的問題。而 WSN 上特殊的應用，感測節點在佈署之前無法事先知道所要佈署的位置。如果運用於軍事偵察，可能會遭受觀察區域的人為硬體攻擊，將節點捕獲，進而讀取節點內部的資訊。

如果我們利用比較直觀的想法，將所有節點預先載入同一把金鑰，我們稱為單一金鑰機制，此機制的優點為節點所要儲存的金鑰容量相當的低，而且可以保證網路完整的連通性（即任意二個節點，可以建立一把金鑰）。然而此機制隨即所帶來另一個問題，就是在節點完成部署之後，如果敵人捕獲任何一個節點，其他未被捕獲的節點所傳輸的資訊都會完全被洩露，輕易的遭受節點捕獲攻擊（Captured Node Attack）。另一種方式為節點與網路中其他的節點各分享一把金鑰，也就是說如果整個網路總共有 ***N*** 個節點，每一個節點就必須儲存（***N-1***）把金鑰；此機制可以解決單一金鑰機制的問題，因為當其中一個節點被捕獲也只會影響到該節點與其他節點的通訊資料，不會影

響其他未被捕獲節點間的通訊。但此機制無法支援大型的 WSN，因為隨著節點數量的增加，每個節點所儲存的容量也相對越高。

最近的相關研究中，基本隨機式金鑰預先分配機制[11]是由 Eschenaur 與 Gligor（2002）所提出，是第一個優先提出「金鑰池（Key Pool）」及「隨機」選擇金鑰的學者。此機制的基本精神就是在節點佈署之前，每個節點從基地台所產生的金鑰的池中「隨機」選擇數把金鑰，儲存到節點內。待節點佈署之後再將金鑰的 ***ID*** 廣播至鄰居節點，如果儲存到相同的金鑰，即可建立一把通訊金鑰。如此一來，每個節點不需要再儲存（***N-1***）把金鑰，即可達到相當程度的連通性。但因為節點所儲存的金鑰是從金鑰池隨機挑選的，所以兩個節點之間可能沒有儲存到相同的金鑰，因此無法保証整個網路的連通性。且此機制也無法達到認證的功能，因為二對節點之間可能選擇到同一把金鑰，無法保證訊息是由哪個節點所傳出。在建立金鑰之後，每個節點仍留有金鑰的訊息，如果節點被捕獲之後，仍可能會洩露其他節點的秘密通訊金鑰，無法抵抗節點捕獲攻擊。

之後有許多學者基於「金鑰池」及「隨機」挑選金鑰的方式設計出金鑰管理機制，其中 Liu 與 Ning（2003）所提出的基於多項式池之金鑰預先分配機制[15]就為其中之一，利用了對稱式多項式方程式（Symmetric Polynomial Function）[6]的特性，提升了網路的安全性。而 Multi-Space 金鑰預先分配機制[10]是由 Du、Deng、Han 與 Varshney（2003）基於 Blom（1984）的金鑰分配機制[4]所提出的。Multi-Space 主要是在抵抗當遭受節點捕獲攻擊時，降低被捕獲節點所洩露的金鑰資訊，同樣加強了網路的安全性，並強調只要不超過 λ（為一個安全系數）個節點被捕獲，整個網路都是安全的。另外，Reberto、Luigi、Mancini 與 Alessandro（2004）提出基於擬亂數金鑰預先分配機制[17]，利用擬亂數函式（Pseudo-Random Function）[12]來分配感測節點所需要儲存的金鑰，使得節點在佈署之後，不需要任何額外的訊息交換即可找到是否存有相同的對稱式金鑰，節省通訊成本。至目前為主，只要是基於「金鑰池」及「隨機」挑選金鑰的想法之下，都無法保證整個網路的連通性（任二個節點可以建立一把金鑰），也無法完全的抵抗節點捕獲攻擊。為了解決不連通及抵抗節點捕獲攻擊的問題，Cheng 與 Agrawal（2005）所提出的 EPKEM[8]金鑰分配機制，可以保證整個網路的連通性，作者強調佈署之後的感測節點之間，至少都可以存有二把共同的金鑰。相較於現存基於「金鑰池」及「隨機」想法下的機制，EPKEM 減少了儲存金鑰的數量，但卻可以提供整個網路的連通性。雖然 EPKEM 作者宣稱可以完全抵抗節點捕獲攻擊，但是我們仍發現，在此機制下節點被捕獲的同時，仍可能洩露其他未破解節點的秘密資訊[3]，且在網路節點數量增加時，感測設備所需要儲存的金鑰也會等比例的上升。

在 WSN 的網路架構中，分為平面式（Flat）及階層式（Hierarchical）二種[13]。一般在平面式的架構中，所有的節點設備都是相同的，且佈署之後的密度是很高的，所以必需假設節點與節點之間建立一把共同的金鑰。而在階層式的網路架構中，分為有基地台、叢集頭及一般節點三種感測設備。其中叢集頭的各項配備優於一般節點。而低成本的一般節點只能進行短距離的傳輸，只需要產生與叢集頭之間的秘密通訊金鑰，不需要建立與其他一般節點之間的金鑰。因為每個一般節點廣播的範圍都可以到達該叢集的叢集頭。

Gaurav 等人（2003）提出 LEKM 金鑰分配機制[14]用於階層式的 WSN。在 LEKM 機制中，大量一般節點依造叢集頭的數量被劃分於數個叢集。叢集頭之間可以互相通訊，或透過 Multi-hops 的方式傳送到基地台。

在預先分配的階段，叢集頭需儲存數把金

鑰子集合。針對一般節點，基地台隨機選擇一個叢集頭與該叢集頭所儲存的一把金鑰，結合叢集頭的 ***ID*** 儲存於一般節點內。待節點部署之後，將叢集頭的 ***ID*** 廣播出去，如果隨機部署的一般節點剛好落於基地台所選擇的叢集頭，就可以立即建立一把金鑰。反之，則此節點的叢集頭需向其他叢集頭要求通訊金鑰。然而 LEKM 機制，在部署之後的金鑰探測的階段，叢集頭需耗費大量的通訊成本。

Cheng 與 Agrawal（2007）提出 IKDM（Improved Key Distribution Mechanism）機制[7]，同樣也是運用於階層式的 WSN，此機制不管感測節點數量的增加，每個一般節點都只需要儲存固定的二把金鑰。IKDM 機制與 LEKM 機制的分配金鑰方法相似，不同在於 IKDM 機制中於一般節點所儲存的金鑰由 ***l*** 個多項式子金鑰結合而成。基於對稱式多項式的 ***t***-security 特性，IKDM 增加了安全性。但在建立叢集頭與一般節點金鑰的階段，針對叢集內的每一個一般節點，叢集頭都需向其他 ***l*** 個叢集頭要求 ***l*** 個子金鑰，耗費大量的通訊成本。且作者強調無論捕獲幾個叢集頭都不會影響到其他未捕獲節點的秘密傳輸，其每個叢集頭在完成建立金鑰之後，都仍存有秘密對稱式多項式的子金鑰，在叢集頭被連續破解的情況下，仍有可能洩露其他未捕獲節點的秘密通訊金鑰，因此無法真正抵抗節點捕獲攻擊。

為了使金鑰分配機制的流程更有效率且可以抵抗節點捕獲攻擊，我們將提出 ESKDM 機制，來建立感測節點之間的秘密金鑰。

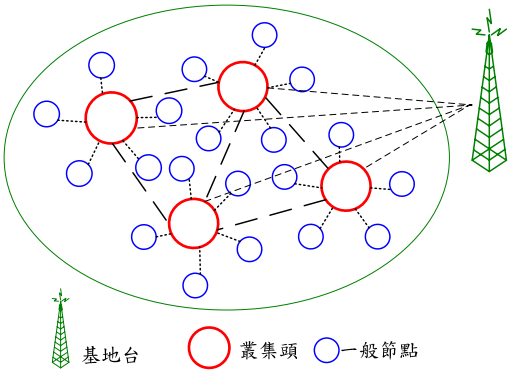
3. ESKDM 金鑰預先分配機制

在此章節我們基於對稱式多項式方程式，提出新的金鑰預先分配機制 ESKDM（Efficient and Scalability Key Distribution Mechanism）運用於階層式的 WSN。與 IKDM 比較，我們所提出的方法中，增加了安全性、連通性，也明顯降低了叢集頭的通訊成本。ESKDM 機制主要特色如下：

- 可完全抵抗捕獲節點攻擊
- 可保證整個網路的連通性
- 最低的儲存成本（無論網路節點數量大小，一般節點只需儲存一把金鑰及一個對稱式多項式方程式）
- 在新增節點時可不需透過線上的 ***BS***
- 減少建立金鑰所耗費的通訊成本

基本假設：

我們所定義的網路模組中，共有三種異質性的感測設備，分別為基地台、叢集頭與一般感測節點，如圖一。



圖一 ESKDM 網路架構

- 基地台：計算能力、儲存能力及能源都是充足的。基地台可能線上或離線的狀況存在於感測網路中。其廣播範圍可以到達整個 WSN 上每一個成員。
- 叢集頭：於基本配備上都優於一般節點。對於通訊範圍而言，叢集頭之間可以互相通訊，也可以透過 Multi-hops 的方式廣播至基地台。叢集頭的佈署，是在一般節點部署之後，以叢集頭的廣播範圍分成數個區域，再安置適當的位置。
- 一般節點：使用低成本、體積小的一般節點，在計算、儲存、能源及傳輸範圍

的配備上都有所限制。網路中的每一個一般節點，都能與該叢集的叢集頭直接通訊。一般節點的佈署是大量的「隨機」撒至欲感測的範圍。.

3.1 對稱式雙變量多項式方程式（Symmetric bivariate Polynomial Function）

在這個小節，將更深入介紹所使用的對稱式多項式方程式，此對稱式多項式於 1993 在文獻[6]中被提出。雙變量多項式 $f(x,y)$ 是一個 ***t***-degree 的方程式，定義為：

$$f(x,y)=\sum_{i,j=0}^{t} a_{i,j}x^i y^j \qquad (1)$$

其中係數 $a_{i,j}(0\le i,j\le t)$ 為一個亂數的選擇於有限域 $GF(Q)$，Q 為一個大質數足夠形成一把加密金鑰。於方程式(1)中，能提供對稱式的特性，如：

$$a_{i,j}=a_{j,i}$$

使得 $f(x,y)=f(y,x)$，在整個 WSN 金鑰預先分配的基本概念上，每個節點都有一個獨一無二的 ***ID***，對節點 N_a 而言，基地台會計算多項式 $f(ID_{N_a},y)$ 儲存於節點內，而 N_b 則儲存多項式 $f(ID_{N_b},y)$。待節點佈署之後，N_a 與 N_b 欲建立一把共同的秘密金鑰，只需要互相交換對方的 ***ID***。N_a 計算 $K_{N_a,N_b}=f(ID_{N_a},ID_{N_b})$，$N_b$ 計算 $K_{N_a,N_b}=f(ID_{N_b},ID_{N_a})$ 即可建立一把秘密金鑰。

對稱式多項式主要的缺點在於有 ***t***-security 的問題。基於 WSN 的應用，不同於一般傳統網路，如果說攻擊者捕獲存有該多項式方程式超過 ***t*** 個節點，並讀取節點內的方程式，即可將該對稱式多項式破解。

3.2 ESKDM 金鑰預先分配機制

整個於階層式 WSN 建立金鑰的過程，一共分為四個階段：金鑰預先分配階段、建立外部成對金鑰階段、建立內部成對金鑰階段與清除關鍵資訊階段。表一為符號說明表：

表一 符號說明表

符號	解釋
BS	基地台
CH_i	***ID*** 為 i 的叢集頭
N_i	***ID*** 為的 i 一般節點
$K_{a,b}$	a 與 b 所建立的對稱式金鑰
$E_{K_{a,b}}(data)$	使用金鑰 $K_{a,b}$ 對 data 加密
$f_{CH-CH}(x,y)$	建立叢集頭之間的秘密金鑰之對稱式多項式方程式
$f_{CH-N}(x,y)$	建立叢集頭與一般節點的秘密金鑰之對稱式多項式方程式
$f_{CH-NS}(x,y)$	新節點與叢集頭的秘密金鑰之對稱式多項式方程式
$H(x)$	單向雜湊函式（One way hash function）

階段一 金鑰預先分配階段

我們將在感測節點佈署之前，預先載入相關的秘密資訊於節點內，待感測節佈署之後，利用這些秘密資訊來建立一把通訊金鑰。同時，我們也假設有 ***n*** 個一般節點與 ***m*** 個叢集頭。三種感測設備所需要預先載入的資訊如下：

BS：

(1) 存有 ***n*** 把 K_{BS,N_i} 金鑰，分別與每一個一般節點分享一把金鑰

(2) ***m*** 把 K_{BS,CH_i} 金鑰，分別與每一個叢集頭分享一把金鑰

CH_i：

(1) 一把與 ***BS*** 共享的秘密金鑰 K_{BS,CH_i}

(2) 多項式方程式 $f_{CH-CH}(ID_{CH_i},y)$，用於建立叢集頭之間的秘密金鑰

(3) 多項式方程式 $f_{CH-N}(ID_{CH_i},y)$，用於建立叢集內一般節點的秘密金鑰

N_i：

(1) 一把與 ***BS*** 共享的金鑰 K_{BS,N_i}

(2) 多項式方程式 $f_{CH-N}(ID_{N_i},y)$，用於與叢集頭建立秘密金鑰

完成金鑰預先分配階段之後，我們假設一般節點以「隨機」的方式佈署於欲偵察的區域，並將感測節點劃分為 ***m*** 個叢集之後，再將叢集頭安置到適當的廣播範圍位置。

階段二 建立外部成對金鑰階段

在叢集頭佈署之後，叢集頭需要相互建立一把秘密金鑰，當某些可能離 ***BS*** 較遠的叢集頭，可以透過鄰近的叢集頭，將資料加密並以多重跳躍的方式，進行短距離的傳輸來節省電力。叢集頭部署之後，將本身的 ***ID*** 廣播給鄰近的叢集頭，收到廣播的 ***ID***，再利用所儲存的多項式代入對方的 ***ID*** 結合單向雜湊函式，即可以建立一把通訊金鑰。叢集頭之間建立的詳細流程如下，我們假設 CH_a 與 CH_b 欲建立秘密金鑰：

(1) CH_a 將 CH_b 的 ***ID*** 代入所儲存的多項式 $f_{CH-CH}(ID_{CH_a},y)$ 之 y 變數，經過單向雜湊函式，產生：

$K_{CH_a,CH_b}=H(f_{CH-CH}(ID_{CH_a},ID_{CH_b}))$

，建立與 CH_b 的秘密金鑰

(2) CH_b 同樣計算

$K_{CH_a,CH_b}=H(f_{CH-CH}(ID_{CH_b},ID_{CH_a}))$

產生與 CH_a 的秘密金鑰

階段三 建立內部成對金鑰階段

此階段，我們將建立 ***CH*** 與 N_i 之間的通訊金鑰。對於感測節點的特性而言，廣播封包容量的成本遠大於計算所耗費的成本。一般節點於傳輸訊息時，將所有資料傳送至叢集頭以將不重要的資料進行刪減，可以減少整個 WSN 的通訊成本。以下我們假設 CH_a 與 N_i 之間需建立一條安全通道，其建立的流程如下：

(1) N_i 以分群機制完成叢集分組後，立即與該叢集頭 CH_a 相互交換 ***ID***

(2) CH_a 將 N_i 的 ***ID*** 代入所儲存的多項式 $f_{CH-N}(ID_{CH_a},y)$ 之 y 變數，經過單向雜湊函數，產生：

$K_{CH_a,N_i}=H(f_{CH-N}(ID_{CH_a},ID_{N_i}))$，

建立與 N_i 的通訊金鑰

(3) N_i 同樣計算

$K_{CH_a,N_i}=H(f_{CH-N}(ID_{N_i},ID_{CH_a}))$，

建立與 CH_a 的通訊金鑰

階段四 刪除重要資訊階段

以上三個階段完成之後，CH_i 即刪除所儲存的多項式 $f_{CH-CH}(ID_{CH_i}, y)$ 與 $f_{CH-N}(ID_{CH_i}, y)$，只儲存 K_{BS,CH_i}、K_{CH_i,CH_j} 金鑰及 K_{CH_i,N_y}。而一般節點也刪除所儲存的多項式 $f_{CH-N}(ID_{N_i}, y)$，只儲存 K_{BS,N_i} 及 K_{CH_a,N_i}。此安排是為了防止感測節點被捕獲，得到一些相關的關鍵資訊，以破解多項式導致洩露其他未被捕獲節點的秘密金鑰。

4. ESKDM 機制安全及效能分析

4.1 新增節點

一般節點大部份都沒有更換電池或充電的功能，執行任務一段時間之後感測設備就會將電力消耗殆盡，而失去感測的功能。此時，在節點收集資料的較少的情況下，就需要新增新的感測設備。

相較於其他機制[8][14]，ESKDM 不同在於 ESKDM 機制可在感測設備佈署之後，***BS*** 是處於線上（On-line）或離線（Off-line）的狀態下新增節點。基於無線感測節點的特性，一些相關的應用，例如：戰爭應用、災難現場偵測與環境汙染區觀察等…應用中，我們會先將一般節點與叢集頭放置欲觀察的地區，等待一段時間之後，再將所有觀察的資料傳送至叢集頭收集回基地台，此時基地台的角色，可能是一台 PDA 或是一台筆記型電腦。所以在整個感測任務新增節點的過程中，基地台可能是離線的狀態。但在大部份的金鑰預先分配的機制下，都會假設基地台一直是線上的，有助於新增節點的秘密資訊分享。於 ESKDM 機制的模組下，我們提出在假設基地台是線上或離線的情況下，都可以達到新增節點功能，與其他鄰居節點建立秘密通訊金鑰。我們將提出 ***BS*** 二種新增節點的方式，來新增新的節點，自動建立與叢集內的 ***CH*** 及 N_h 一條安全的傳輸通道。新增節點的流程如下：

I、 ***BS*** 處於線上（On-line）的情況

新節點 N_h 需預先載入，K_{BS,N_h}（***BS*** 與 N_h 共享之秘密金鑰）及 $f_{CH-NS}(ID_{N_h}, y)$ 多項式。

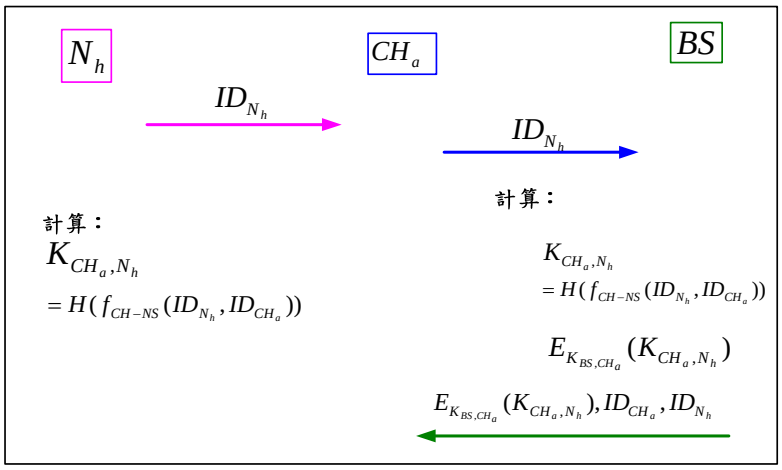
完成儲存重要資訊時，將 N_h 隨機佈署於所需要的地方，我們假設 N_h 佈署於 CH_a 的叢集中，互相廣播 Hello 訊息交換他們的 ***ID***，CH_a 即通報 ***BS*** 新節點 N_h 於叢集 a 中，進行建立秘密金鑰的流程如圖二：

N_h 利用 CH_a 的 ***ID*** 代入多項式 $f_{CH-NS}(ID_{N_h}, y)$ 之 y 變數，$K_{CH_a,N_h} = H(f_{CH-NS}(ID_{N_h}, ID_{CH_a}))$，完成建立與 CH_a 的秘密金鑰，隨即將多項式 $f_{CH-NS}(ID_{N_h}, y)$ 刪除。

(1) ***BS*** 計算

$K_{CH_a,N_n} = H(f_{CH-NS}(ID_{N_h}, ID_{CH_a}))$，且使用與 CH_a 所共享之金鑰將 K_{CH_a,N_n} 加密，產生 $E_{K_{BS,CH_a}}(K_{CH_a,N_h})$。並將訊息 $(E_{K_{BS,CH_a}}(K_{CH_a,N_n}), ID_{CH_a}, ID_{N_h})$ 傳送至 CH_a

(2) CH_a 將訊息 $E_{K_{BS,CH_a}}(K_{CH_a,N_h})$ 解密，取得秘密金鑰 K_{CH_a,N_h} 建立與 N_h 之間的金鑰。



圖二 *BS* 線上狀態新增節點流程

II、 基地台離線（Off-line）的狀態

BS 首先對新節點 N_h 產生：.

(1) 多項式 $f_{CH-NS}(ID_{N_h}, y)$，使用於新節點與 ***CH*** 建立秘密金鑰

(2) 建立 ***BS*** 與 N_h 共享之秘密金鑰 K_{BS,N_h}

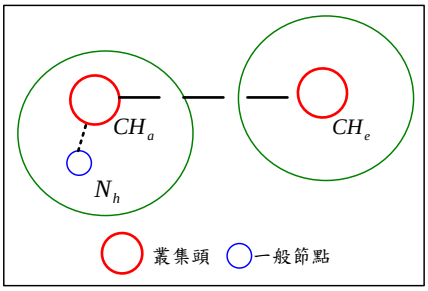
(3) 觀察欲新增節點的區域附近的 ***CH*** 中，隨機選擇 ***l*** 個 ***CH***，假設 ***l***=1 且所選擇的是 CH_e，結合 CH_e 之 ***ID*** 計算

$$K_{CH_e,N_h} = H(f_{CH-NS}(ID_{N_h}, ID_{CH_e}))$$

(4) ***BS*** 利用與 CH_e 之共享金鑰對 K_{CH_e,N_h} 加密，產生 $E_{K_{BS,CH_e}}(K_{CH_e,N_h})$

將 K_{BS,N_h}（***BS*** 共享之金鑰）、K_{CH_e,N_h}（與 CH_e 共享之金鑰）、$E_{K_{BS,CH_e}}(K_{CH_e,N_h})$（加密後的金鑰訊息）與 ID_{CH_e} 儲存於新節點 N_h 中。

資料儲存完成之後，將節點佈署於需要佈署的位置，如果新節點剛好佈署於 CH_e 叢集內，N_h 只需將訊息 $E_{K_{BS,CH_e}}(K_{CH_e,N_h})$ 廣播至 CH_e 解密之後即可建立一把對稱式的金鑰。此外，我們假設佈署之後的情況如圖三：

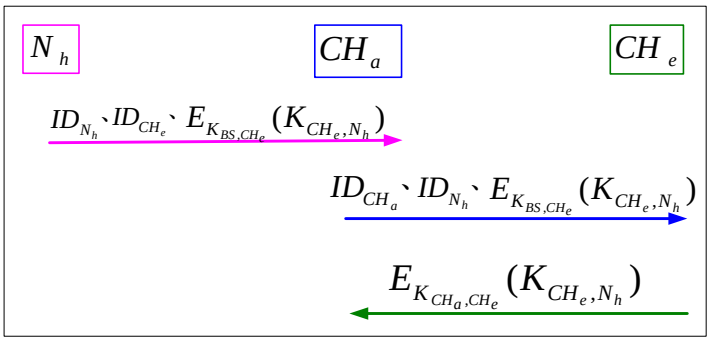


圖三 新節點佈署圖

也就是 N_h 佈署與 CH_a 同一叢集。新節點佈署之後，將開始建立與叢集內的 CH_a 建立一把秘密金鑰，建立的流程如圖四。

(1) N_h 首先將 $(ID_{N_h}, ID_{CH_e}, E_{K_{BS,CH_e}}(K_{CH_e,N_h}))$ 傳送至 CH_a

(2) CH_a 結合自己的 ***ID*** 轉送 $(E_{K_{BS,CH_e}}(K_{CH_e,N_h}), ID_{N_h}, ID_{CH_a})$ 至 CH_e



圖四 *BS* 離線狀態新增節點流程

(3) CH_e 收到資料之後，使用與 ***BS*** 共享之金鑰，將訊息 $E_{K_{BS,CH_e}}(K_{CH_e,N_h})$ 解密，取得 K_{CH_e,N_h}，再利用與 CH_e 共享之秘密金鑰加密，產生 $E_{K_{CH_a,CH_e}}(K_{CH_e,N_h})$，傳送至 CH_a。並隨即將 K_{CH_e,N_h}、$E_{K_{BS,CH_e}}(K_{CH_e,N_h})$ 及 $E_{K_{CH_a,CH_e}}(K_{CH_e,N_h})$ 立即刪除。

(4) CH_a 收到資料之後，解密完成即可取得與新節點 N_h 之秘密金鑰。

我們也許無法確認，CH_e 是否在 CH_a 的廣播範圍中，但基於 WSN 傳輸資料的結構，CH_a 之間仍可能透過其中幾個 ***CH*** 以多重跳躍的方式將資料送至 CH_e。且在 ***BS*** 離線的狀況下，所選擇的 ***l***，數量可以是 2~3 個，除了可以預防所選擇到的 ***CH***，可能因為電力耗盡無法進行轉送的工作，造成新節點與 ***CH*** 無法建立金鑰，還可以讓 CH_a 選擇離自己距離最近的 ***CH*** 傳送，以節省通訊成本。

以兩個新增節點的方式而言，明顯在 ***BS*** 線上時，***CH*** 的計算及通訊成本都低許多。因為所需要分享的秘密資訊，會由 ***BS*** 利用與 ***CH*** 之間分享的金鑰加密之後傳出。相對地，在 ***BS*** 在離線下的運作方式，將資料加密的計算成本轉於 ***CH*** 之中，且 CH_a 須將訊息廣播至 CH_e 解密之後再回傳，這其中可能會產生多餘的通訊成本。但在 WSN 的應用中，仍可能會有離線 ***BS*** 的可能性，我們所設計新增節點機制中，也能支援此架構。

4.2 網路連通性

WSN 是由大量的一般節點及少量的叢集頭所組成，如何使得感測設備與鄰居節點（指廣播範圍內的節點）可以建立一把共同的秘密金鑰，進而進行安全通訊，取得整個網路的連通性，是非常重要的一環。其他目前所提出的機制中[11][15]，節點設備如果無法與全部的鄰居節點建立金鑰，需透過其他可以信任的節點轉送至目的端，都會增加網路額外的通訊成本，或甚至在節點分布不均勻的狀況下，產生不連通的狀況。我們所提出的 ESKDM 機制中，叢集頭之間的秘密金鑰和叢集頭與一般節點的秘密金鑰，可以提供整個網路的連通性。

4.3 節點捕獲攻擊

於 3.1 節中，我們討論到關於對稱式多項式方程式的特性，若捕獲持有該多項式的節點超過 ***t*** 個，此對稱式多項式就會被破解，間接危急到整個網路的安全。為了抵抗私密多項式的洩露，在完成建立金鑰之後，進入第四階段刪除重要資訊，叢集頭與一般節點將所儲存的私密多項式刪除。且在計算金鑰的流程中，我

們也加入了單向雜湊函式計算，預防攻擊者進行反推私密多項式分享。單向雜湊函式[9][16]（例如 MD5 或 SHA1 等…）運算具備二種特性：

(1) 令 $h = H(x)$，給定 x 值，可以輕易的計算 $h = H(x)$，當給定雜湊輸出值 h 之後，欲找出任何文件可以輸出此一特定的雜湊值 h ，為計算上不可行，此為抗拒事先描繪的特性（Preimage Resistance）

(2) 令 $h = H(x_1)$，當給定一份文件 x_1 及雜湊值 h ，找出第二份文件 x_2（$\neq x_1$），並讓 $H(x_1) = H(x_2)$ 為計算上不可行，此為抗拒第二事先描繪的特性（Second Preimage Resistance）

所以在我們所提出的 ESKDM 機制中，可以完全抵抗節點捕獲攻擊。

4.4 效能分析

由表二我們列出 ESKDM、IKDM 及 LEKM 於一般節點及叢集頭效能方面的各項比較。在 LEKM 的金鑰分配機制中，完成建立金鑰之後，***CH*** 立即將多餘的金鑰刪除，只留下該叢集內節點之間的通訊金鑰，因此可以抵抗節點捕獲攻擊。但在預先分配的階段，***CH*** 所需要儲存的金鑰量過多，且會隨著網路節點的數量大小而上升，對於設備仍有限的 ***CH*** 而言，無法支援大規模的網路。在金鑰探測的階段，***CH*** 仍需向其他的 ***CH*** 取得叢集內一般節點的通訊金鑰，需耗費相當高的通訊成本。

表二 效能分析比較表

機制名稱		ESKDM	IKDM	LEKM
抵抗節點捕獲攻擊		YES	NO	YES
儲存成本	一般節點	一把金鑰及一個多項式方程式	二把金鑰及 l^* 個叢集頭 ***ID***	二把金鑰及一個叢集頭 ***ID***
	叢集頭	1 把金鑰及 2 個多項式方程式	1 把金鑰及 2 個多項式方程式	$\frac{n}{m}+(m-1)+1$ 把金鑰
廣播成本	一般節點	無**	$l^* \times ID_{CH_i}$	一個叢集頭的 ***ID***
	叢集頭	無**	$(\frac{m-1}{m}) \times 2l^*$	$3(\frac{n}{m}-\frac{n}{m^2})$
計算成本	一般節點	t_{poly}***	無	無
	叢集頭	$(t_{poly}{}^{***} \times C_i n^{****})$	$\frac{(n \times t_{poly}{}^{***} \times l)}{m}$	無
新增節點		不需依賴基地台	—	需依賴基地台

*：IKDM 機制中一般節點儲存金鑰所分割的次數

：*ID*** 交換為 WSN 自我組態中必要的流程，因此在 ESKDM 機制中無額外的廣播成本

：計算 ***t-degree 的對稱式多項式所耗費的計算成本為 $O(t^2)$ ，若運用 Cramer's Rule[5]則所耗費的時間為 $O(t)$

****：叢集 i 內的一般節點數量

對 IKDM 機制而言，***BS*** 建立 K_{CH_e,N_i} ，是由 ***l*** 個 ***CH*** 多項式分享結合而成的，待一般節點被佈署之後，必須廣播 ***l*** 次的 ***ID***，告知該 ***CH*** 金鑰的位置。而針對每一個叢集內的節點，***CH*** 需廣播 ***l*** 次並等待 ***l*** 個叢集頭回覆子金鑰，才能將通訊金鑰組合起來。其為了降低節點捕獲攻擊所受到影響，IKDM 的作者強調 ***l*** 的數值不能過小，形成了一個安全性及通訊成本權衡的問題，但無論 ***l*** 的數值大到多少，每個叢集頭完成金鑰分配階段之後，都仍存有 $f_{CH-N}(ID_{CH_i}, y)$ ，所以仍無法完全避免節點捕獲攻擊所帶來的潛在危機，仍可能取得未捕獲節點的通訊金鑰。

我們所提出的 ESKDM 機制中，可以完全抵抗節點捕獲攻擊。在預先分配的流程中，感測設備所要儲存為固定的資訊，不會隨著網路節點數量而上升。在金鑰探測的階段，感測設備也不需要任何額外的訊息交換，因為 ***ID*** 的交換為自我組態中的必要的流程，因此大幅度的降低感測設備所消耗的通訊成本。但相較於 IKDM 及 LEKM 機制，ESKDM 機制雖然增加了計算通訊金鑰的成本，基於感測節點的特性而言，傳送 1 位元 100 公尺所需的能量大致等於感測器內部執行 3000 個指令[2]。為達到節省能源的目的，如何降低通訊成本仍為感測設備首要的考量。我們也提出二個新增節點的方式，讓一般節點可以不依賴基地台就可以與該叢集頭建立金鑰。

5.結論

我們基於階層式 WSN 與對稱式多項式方程式提出 ESKDM 機制。在此機制中可以保證整個網路的連通性，且運用了多項式的特性，使感測節點之間只需透過 ***ID*** 的訊息交換即可建立金鑰。相較於 LEKM 與 IKDM 機制，ESKDM 機制大幅度的降低感測設備的通訊成本，並完全抵抗節點捕獲攻擊。無論網路節點的大小，一般節點所需要儲存的秘密資訊都為固定的資訊，能夠支援大型的 WSN。也提出於新增節點的同時，不需要「線上」的 ***BS*** 存在，更能套用於實際的應用。我們所提出的機制中達到高連結、高延展性、安全性、低運算成本與低通訊成本。

參考文獻

[1] UC Berkeley, “Smart Dust,” 2007 年 09 月 17 日取自 http://robotics.eecs.berkeley.edu/~pister/SmartDust/

[2] 常若愚、林志敏、李維聰(2004)，IEEE802.15.4 低速率無線個人區域網路之 CSMA/CA 碰撞效能分析與研究，碩士論文，逢甲大學資訊工程系，台中.

[3] 簡宏宇、陳榮靜、沈安妮，“高效率、高連結、低儲存成本的感測節點金鑰分配，” ***2007 第十屆電子商務研討會***，台灣，2007。

[4] R. Blom, “An Optimal Class of Symmetric Key Generation System,” in: Proceedings of ***EUROCRYPT***’84, pp. 335-338, 1984

[5] C.B. Boyer, “A History of Mathematics,” John Wiley, 1968; 2nd edition

[6] C. Blundo, A.D. Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, “Perfectly-secure key distribution for dynamic conferences,” Lecture Notes in ***Computer Science***, pp. 471-486, 1993

[7] Y. Cheng and D. P. Agrawal, “A Improved Key Distribution Mechanism for Large-Scale Hierarchical Wireless Sensor Networks,” ***Ad Hoc Networks***, pp.35-48, January 2007

[8] Y. Cheng and D. P. Agrawal, “Efficient Pairwise Key Establishment and Management in Static Wireless Sensor Networks”, in: Proceedings of ***Mobile Adhoc and Sensor Systems*** Conference, November 2005

[9] I. B. Damgard, "A Design Principle for Hash Functions," Advances in ***Cryptology-CRYPTO***’89 Proceedings, Springer-Verlag, pp. 416-427, 1990.

[10] W. L. Du, J Deng, Y. Han and P. K. Varshney, “A Pairwise Key Pre-distribution Scheme for Wireless Sensor Network,” in: Proceedings of 10th ACM Conference on ***Computer and Communications*** *Security*, pp. 42-51, October 2003

[11] L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” in: Proceedings of 9th ACM Conference ***Computer and Communications Security***, pp. 41-47, November 2002

[12] O. Goldreich, S. Goldwasser and S. Micali, “How to construct random function,” ***Journal of the ACM***, 33(4), 1986

[13] W.R. Heinzelman, A.P. Chandrakasan and H. Balakrishnan, “An Application Specific Protocol Architecture for Wireless Microsensor Networks,” IEEE ***Transactions on Wireless Communications***, pp. 660-670, October 2002

[14] G. Jolly, M.C. Kuscu, P. Kokate and M. Yuonis, “A Low-Energy Management Protocol for Wireless Sensor Networks,” in : Proceedings of the 8th IEEE International ***Symposium Computers and Communication***, pp.335-340, June 2003.

[15] D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks,” in: Proceedings of 10th ACM Conference on ***Computer and Communications Security***, pp. 52-61, October 2003

[16] R. Merkle, "One-Way Hash Functions and DES," Advances in Cryptology, CRYPTO’89, Lecture Note in ***Computer Science***, Vol. 435, pp. 428-446, 1989.

[17] R. D. Pietro, L. V. Mancini and A. Mei, “Efficient and Resilient Key Discovery Based on Pseudo-Random Key Pre-Deployment,” in: Proceedings of the 18th International ***Parallel and Distributed Processing Symposium***, pp. 26-30, April 2004