# 以互斥基底系統為基礎應用於叢集式無線感測網路之分散式金鑰管理機制

# A Distributed EBS-Based Key Management Scheme for Clustering Wireless Sensor Networks

黃志銘
逢甲大學
資訊工程學系
e-mail: jmhuang@fcu.edu.tw

曾嘉祥
逢甲大學
資訊工程研究所
e-mail: m9489621@fcu.edu.tw

## 摘要

資訊加、解密在無線通訊上已是必然之手段，而相關金鑰管理(Key Management)措施的良窳及安全性，常是決定該機制成功與否的條件。本篇論文即是在叢集式無線感測網路(Wireless Sensor Network )中，提出一個異於傳統集中式金鑰管理的作法，以互斥基底系統(Exclusion Basis System，EBS)為技術的分散式金鑰管理機制，稱之為 D-EBS (Distributed EBS)。在 D-EBS 作法上，我們將網路金鑰的管理工作(包括金鑰分配、重置及撤銷)分散至各個叢集中，利用叢集間的交互合作與地域空間的限制條件，有效控管通訊金鑰，以避免節點遭到破解後嚴重影響整體網路的通訊安全。分析說明了我們所提的分散式金鑰管理機制 D-EBS 有著以下的優點：1.可獨立運作於傳統金鑰分配中心(Key Distribution Center，KDC)支援之外。2. 具高效率的金鑰重置(Rekeying)與撤銷(Revocation)能力。3. 具良好的網路延展性(Scalability)。4. 可適用於多種叢集式架構。

**關鍵詞**：金鑰管理、金鑰重置、金鑰撤銷、互斥基底系統

## Abstract

The achievements of data confidentiality and privacy are closely dependent on the success of key management scheme in wireless communications. In this paper, we propose a distributed EBS-based key management scheme, named D-EBS, for clustering wireless sensor networks. As distinct from traditional centralized key management approach, D-EBS spreads the management workloads, such as key distribution, renew, and revocation, over clusters. By the cooperation and locality between neighboring clusters, D-EBS provides an efficient and effective key management paradigm, and thus ensures the security of network communications. Detail analysis illustrates that our proposed D-EBS can : 1. independently run with the exclusion of key distribution center (KDC). 2. achieve a good performance for key renew and revocation processes. 3. be with a better scalability. 4. be well adaptive to a variety of cluster-based frameworks.

**Keywords: Key management, Rekeying, Key revocation, Exclusion basis system, EBS**

## 1. 前言

近年來由於微電子電機系統(MEMS)技術的成熟，相關的應用相繼被提出，無線感測網路(Wireless Sensor Networks, WSNs )即為其中之一。無線感測網路是由大量感測節點(Sensor Node)所建構而成的無線通訊網路；通常感測節點具有感測、處理資料、以及無線傳輸的功能；資源有限(如記憶體、計算能力、電源供應等)、體積小、成本低廉是為其特色[1][18]。感測節點在隨機配置於感測環境後，可經由自我組態(Self-organization)形成通訊網路，並且偵測週遭環境所產生的變化(如溫度、壓力、聲、光、影像等)，在收集感測資料後，以單點或多重跳躍(Single- or Multi- hop)的方式，將之傳回基地台(Base Station or Sink)，提供後端人員處理、分析、以及決策支援。目前常見的應用包括軍情資訊蒐集、生態環境控管、健康醫療監測、住家保全系統等方面。

配合無線感測網路資訊蒐集與傳輸，多種網路拓樸(Topology)與繞徑協定(Routing Protocol)相繼地被提出；叢集式繞徑協定(Cluster-based Routing Protocol)即為其中之一[9][10]。而所謂的叢集式架構，或依節點通訊特性(如距離)，或依節點地域關係，將感測環境建構成多個圓形叢集(Cluster)[10]或矩形網格(Grid)[19]。叢集中感測節點分為兩種角色：叢集首(Cluster Head，CH) 與一般節點(Non-Cluster Head)，並形成階層式(Hierarchical)的網路結構。在此架構下，一般節點會先將感測資訊統一交由叢集首處理並整合，再由叢集首以直接或接力(即 Single- 或 Multi- hop)的方式傳回基地台(Base Station，BS)。因此，叢集首在所屬叢集中扮演著舉足輕重的角色，但也相對地必須多方考量資源的使用條件，慎選叢集首；最常見的選擇方式是定期或不定期地輪換叢集首，如 LEACH[10]與 PEGASIS[12]兩協定即是如此。

無線感測網路資訊的傳輸，常因為感測節點隨機配置的暴露，及無線通訊先天的安全防護脆弱，傳輸訊號極易遭受入侵者(惡意者)的攔截、監聽、竄改、仿冒與複製，常見的攻擊手法有 DoS (Denial of Service)攻擊、Sybil 攻擊、以及重製(Replication)攻擊[17] [15] [16]。為了保障傳輸訊息的隱密性，尤其在安全考量要求極高的應用環境下，於通訊協定中加入必要的安全控管機制，以防訊息外洩，造成無法彌補的憾事，已是不可或缺的手段。然而安全控管機制的成功與否，依賴於通訊金鑰(Key)的有效管理，包括金鑰分配(Key distribution)、金鑰重置(Rekeying)、與金鑰撤銷(Key revocation)等措施。

傳統網路的金鑰管理機制概可分為兩大支[2]，其一為非對稱式金鑰系統(Asymmetric Key System，如公開金鑰機制[6])，其二為對稱式金鑰系統(Symmetric Key System，如 DES 金鑰機制[4])。非對稱式金鑰系統雖有較佳的金鑰保密措施，但卻因為計算負荷需求過高，並不適用於計算能力有限的感測節點上。相反地，對稱式金鑰機制雖然有著金鑰管理的問題，但由於計算量遠小於非對稱式金鑰系統，反使其成為無線感測網路安全機制設置上優先考量的主流技術。目前已有甚多的相關作法被提出，如共享金鑰(Share Key)、配對金鑰(Pair-wise Key)、隨機金鑰池(Random Key Pool)[5] [8] [11]、多項式金鑰(Polynomial-based Key)[3][13]、及互斥基底系統(Exclusion Basis System)[7]等，然各項作法或因安全性欠佳，或因金鑰記憶體負荷過高，或因網路連通性太低，或因需金鑰分配中心的全程參與運作，而限制了其應用。詳細做法與相關優、缺點將於下一章節中述明。

為了讓金鑰管理更具效率、更具安全性、應用更普遍化，本篇論文結合廣為大家喜愛的叢集式無線感測網路架構，提出了一個分散式的管理機制，我們稱之為 D-EBS (Distributed

EBS)。D-EBS 以互斥基底系統(Exclusion Basis System，EBS)為技術基礎，將傳統集中式金鑰分配中心的管理觀念與責任，分散至各個叢集首身上，並利用叢集間的聯合運作與地域空間的限制條件，有效的管理通訊金鑰，以避免節點遭到擄獲後，嚴重影響整體網路的通訊安全。分析說明我們所提的分散式金鑰管理機制有著以下的優勢：1.可獨立運作於傳統金鑰分配中心支援之外。2. 具高效率的金鑰重置與撤銷能力。3. 具良好的網路延展性(Scalability)。4. 可適用於多種叢集式架構。

本篇論文的結構概分如下，第二章節將先簡介一些目前被提出應用於無線感測網路上的金鑰管理機制，並分析其優、缺點。之後，再介紹本篇機制所採用基礎技術 EBS 之觀念。第三章節則對本文所提出的分散式金鑰管理機制 D-EBS 作詳盡介紹。第四章則深入分析、討論 D-EBS 相關的管理細節與特性。第五章則為本文的結論。

## 2. 相關研究

為了讓本文的研究動機更明顯，本章節將優先簡述一些目前常見於無線感測網路的對稱式金鑰管理機制，並於結束前詳細說明本文所提分散式金鑰管理機制所採用的基本技術-互斥基底系統(Exclusion Basis System， EBS)的觀念。描述中亦將分析各種作法的優、缺點，以突顯本文所提管理方式的優點與價值。

### 2.1 共享金鑰機制(Share Key Schemes)

對稱式金鑰系統中對金鑰的管理，最簡單的作法即為共享金鑰。其觀念乃是網路內所有節點均預先載入相同的一把金鑰，往後所有節點皆透過此金鑰與網路上其它節點進行秘密通訊。此機制的優點將因為節點內只需儲存唯一的一把金鑰，其記憶體需求量甚低，且可保證網路的連通性。但其缺點將會因入侵者擄獲任意節點，而輕鬆得知了網路共享金鑰，進而破解所有通訊。

### 2.2 配對金鑰機制(Pair-wise Key Schemes)

配對金鑰機制，則是網路上任一節點與其它節點皆分享一把不同的通訊金鑰。因此，若網路中有 $N$ 個節點，則每一節點必須同時儲存 $(N-1)$ 把不同金鑰，以便與其他節點作個別通訊之用。此機制雖解決了共享金鑰機制的部份缺點，讓入侵者無法順利破解網路所有節點間的通訊，但節點記錄金鑰的儲存空間，卻會隨著網路內節點數目的增加而隨之上揚，欠缺網路擴充性(Scalability)的特性。

### 2.3 隨機金鑰池機制(Random Key Pool Schemes)

Eschenaur 與 Gligor 是第一個提出隨機金鑰池預先分配機制的作者[8]。該機制結合預設金鑰池(Key Pool) 與隨機選取金鑰的概念，於節點佈署至目標區域前，預先從由大量不同金鑰集合而成的金鑰池中隨機挑選數個金鑰，將之儲存至節點記憶體內。感測節點於佈署目標區域後，可藉由瞭解彼此間所擁有的共同金鑰進行通訊。即使兩個感測節點間因隨機挑選而無共同金鑰，但亦可透過同時持有雙方金鑰的第三者，來達到相當程度的連通性。雖然此方法節點可藉由大量金鑰配置的技術來增加其連通性，但相對的，當節點遭受攻擊(Compromised)後，所洩漏的金鑰資訊量，其影響程度將隨之擴大，甚至遭到整體網路完全被破解的命運。為了改善其安全，之後亦有多位學者基於此觀念，提出一些更嚴謹的金鑰管理機制[5][11]。

### 2.4 多項式金鑰機制(Polynomial-Based Key Schemes)

Liu 與 Ning 於 2003 年提出基於多項式池之金鑰預先分配機制[13]。此機制主要是利用

對稱多項式函式[3]的特性，加上金鑰池與隨機金鑰挑選之概念建構而出。對稱多項式函式是個 $t$-degree 之多項式函式，表示如下

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

其中 $a_{ij}$ 由一有限域 $F_q$ 中亂數選出，$q$ 為一質數，其值足夠大以形成加密金鑰。$f(x,y)$ 有一對稱之特性，意即 $f(x,y)=f(y,x)$。因此，感測節點 $n_i$ 與 $n_j$ 可經由此函式帶入彼此的 ID，以取得相同的通訊金鑰 $K_{i,j}=f(i,j)=f(j,i)=K_{j,i}$。在多項式池金鑰預先分配機制中，作者以對稱多項式函式代替以往的金鑰，集合而成多項式池後，再隨機挑選載入感測節點內。往後擁有相同原始多項式的感測節點只需互相代入自己與對方的 ID，即可產生出相同的金鑰，以形成安全通訊。由於 $t$-degree 的雙變數多項式函式只有在 $t+1$ 個已代入單一變數的函式 (如 $f(i,y)$ ) 遭到入侵者得知後，方有可能被破解 (意即推導出 $f(x,y)$ )。相較於單純直接的金鑰，多項式池金鑰預置機制顯然強健許多。即便如此，多項式池金鑰預先分配機制仍存在類似前項隨機金鑰池機制的風險。

### 2.5 互斥基底系統(Exclusion Basis System)

由於本文所提的分散式金鑰管理機制乃建構於互斥基底系統(Exclusion Basis System，EBS) [7]基礎上，為了讓本文更易被瞭解，本小節將詳細介紹 EBS 的基本觀念與作法，並於下一章節再詳細說明本文如何應用 EBS 技術於叢集式的感測網路中，以達成分散式金鑰管理功能。EBS 之觀念如下：

令 $n,k,m$ 為正整數，其中 $1<k,m<n$。$EBS(n,k,m)$ 是多個整數子集所構成的母集合 $\Gamma$，子集的樣本空間為 $[1,n]=\{1,2,\ldots,n\}$，其中 $t$ 為整數，$t\in[1,n]$ ，且滿足以下兩個特性：

1. $t$ 最多存在於 $k$ 個子集內。
2. 恰好有 $m$ 個子集 $A_1,A_2,\ldots A_m$，當 $\bigcup_{i=1}^{m}A_i$ 時，其聯集將獨缺 $t$。

舉例而言， $EBS(8,3,2)$可為一個擁有 5 個子集的集合，

$$\Gamma=\left\{\begin{array}{l} A_1=\{5,6,7,8\},\\ A_2=\{2,3,4,8\},\\ A_3=\{1,3,4,6,7\},\\ A_4=\{1,2,4,5,7\},\\ A_5=\{1,2,3,5,6,8\}\end{array}\right\}$$

所有子集內的(整數)元素 $t\in[1,8]$，每個元素恰好存在於 3 個子集內，且任意 2 個子集的聯集恰好缺少某一個元素(如 $A_2$ 與 $A_4$ 聯集缺少元素 6)。$\Gamma$ 通常亦可表示成矩陣形式，如表一；其中子集 $A_m$ 代表不同的金鑰， $t$ 代表使用者的編號(或金鑰擁有者之 *ID*)， $N_t$ 則為編號 $t$ 的感測節點。

$EBS(n,k,m)$ 擴展至無線感測網路環境下的應用可解釋為：設有 $k+m$ 個金鑰的情況下， $n$ 個感測節點，若每個感測節點儲存 $k$ 個金鑰，則最少僅需送出 $m$ 個訊息即可解決某個被擄獲節點(Compromised node)的金鑰重置問題。

**表一　EBS 金鑰矩陣**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $A_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| $A_2$ | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| $A_3$ | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| $A_4$ | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| $A_5$ | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| | – | – | $N_8$ | $N_7$ | $N_6$ | $N_5$ | $N_4$ | $N_3$ | $N_2$ | $N_1$ |

如表一中的節點 $N_6$ 在 $A_1,A_3,A_5$ 列的值為 1 ，意思即代表節點 $N_6$ 持有金鑰 $A_1,A_3,A_5$，而獨缺金鑰 $A_2,A_4$ 。當 $N_6$ 遭到擄獲攻擊時，為了避免整體網路進一步遭到瓦解，而必須將 $N_6$ 迅速從網路中移除，並更新 $N_6$ 所暴露的金鑰。此時 EBS 機制只需發佈兩個加密訊息，即

$E_{A_2}(S', E_{A_1}(A_1'), E_{A_3}(A_3'), E_{A_5}(A_5'))$與
$E_{A_4}(S', E_{A_1}(A_1'), E_{A_3}(A_3'), E_{A_5}(A_5'))$，
群播(Broadcast)至其他感測節點即可。其中，$S$ 表示為共同金鑰，$S'$ 為新的共同金鑰，$E_{A_2}(x)$ 代表使用金鑰 $A_2$ 對 $x$ 加密。由於 $N_6$ 並未持有金鑰 $A_2$ 和 $A_4$ ，故無法順利解讀此兩則新訊息。但 $N_6$ 之外的其他感測節點則因持有金鑰 $A_2$ 或 $A_4$，將順利解密，並進行新的金鑰重置後，即可將 $N_6$ 節點排除在外。

表一矩陣中最左方的兩欄表示現階段並無安排任何對應的感測節點，若往後感測網路有節點新增時，只需將該節點金鑰配置情形對應至該空白兩欄中的任一欄即可。若不足則可擴大建立 EBS 矩陣來完成金鑰分配。

$EBS(n,k,m)$ 系統能負擔的感測節點數量上限須滿足 $C_k^{k+m} \geq n$ 之條件。當有新的感測節點加入導致 $C_k^{k+m} < n$ 時，此時金鑰分配中心只需將本身儲存的金鑰數量調整至 $k+m+x$，使得 $C_k^{k+m+x} \geq n$ 。之後在金鑰重置時，讓每個感測節點所儲存的金鑰數增加至 $k+x_k$ 、金鑰重置的訊息數量增加至 $m+x_m$即可正常運作管理。其中$x_k + x_m = x$, $x_k, x_m \geq 0$。

EBS 最大之優點在於可迅速有效地以極少量的訊息來重新分配或重置金鑰。但通常必須藉由金鑰分配中心來進行 EBS 矩陣建立與金鑰分配。Mohamed 等人曾於 2006 年提出異質性叢集式網路動態組合金鑰管理機制(Dynamic Combinatorial Key Management，簡稱為 DCK)[14]。他們利用建構雙層(two-tier) EBS 作法來進行金鑰管理。DCK 雖將 EBS 金鑰矩陣分散於一般節點中，以避免金鑰矩陣遭到入侵者一舉擄獲之可能性，但運作上卻需要金鑰分配中心(即基地台 BS)的全程參與。在目前並非所有無線感測網路環境下的基地台皆永遠保持連線狀況下，若發生感測節點需進行金鑰管理之相關措施時，當無法順利運作。除此之外，DCK 作法因在網路中加入一些功能較強的節點(異質性網路)來擔任特殊工作，對同質性網路因叢集首輪替所造成的網路變化，導致 EBS 金鑰矩陣必須如何異動，卻未著墨。

綜合上面列述多種金鑰管理機制的優、缺點，再配合目前廣被採用的叢集式繞徑架構，本文將於下面章節提出一個安全且具效率的分散式互斥基底系統金鑰管理機制(Distributed EBS Key Management Scheme)，簡稱 D-EBS。

# 3. 分散式互斥基底系統金鑰管理機制 (Distributed EBS Scheme)

本節將針對本文所提出的分散式互斥基底系統金鑰管理機制(Distributed EBS，爾後將簡稱為 D-EBS)作詳細描述。在描述之前，則先對該機制的應用環境做一些假設，並表列說明該金鑰管理機制中所採用的符號意義。

## 3.1 網路模式(Network Model)

本文對網路模式做如下之假設：

(1) 同質性無線感測網路(Homogeneous WSN)：基於分散式的對等特性，在不考量特殊功能強大的 KDC 一定存在的條件下，我們假設所有感測節點均具有相同的資源與能力。

(2) 叢集式的繞徑架構：叢集結構的如何產生，在過去一些相關叢集式繞徑協定的文獻已多有探討[9][10][12]，本文將不深入說明。但為方便解釋本文所提出的金鑰管理機制，我們將假設網路為網格式(Grid-based)叢集結構，如圖一。其中第 $a$ 列第 $b$ 行的網格標記為 $Grid_{a,b}$ 。同一網格內的感測節點則視為同一叢集(Cluster)或群組(Group)，標記為 $G_{a,b}$ 。叢集內的感測節點亦有叢集首與一般節點之區分，並扮演自己在繞徑上的角色功

能。除此之外，叢集首亦將在 D-EBS 機制中代替傳統金鑰分配中心的角色，負責叢集金鑰矩陣的建立與管理。叢集(群組) $G_{a,b}$ 內的任一感測節點皆假設能夠與周圍鄰近四個叢集（$G_{a+1,b}$、$G_{a-1,b}$、$G_{a,b+1}$、$G_{a,b-1}$）內的節點直接通訊。文後若提到鄰近叢集，除非特別申明，即定義為此四個叢集。

(3) 完善的入侵偵測機制：由於本文主在探討金鑰管理的機能，因此對於入侵偵測機制的功能將不深入著墨，而是預先假設系統中已存在了完善的入侵偵測機制，可以快速正確的偵知任何已遭擄獲的節點。

(4) 安全的金鑰設定階段：為了讓金鑰管理機制可行，並保證其安全，我們亦假設金鑰設定完成前的一小段時間內，入侵者無法立即擄獲感測節點，破解節點內的安全資訊。此種假設在過去文獻[20]已被採用。

(5) 節點位置已知(Location-aware)：我們假設網路中的感測節點的位置已知，並可根據其位置計算出其所屬的網格座標。至於節點座標之取得，可藉由全球定位系統(Global Positioning System，GPS) 得到。

| | | | |
|---|---|---|---|
| $G_{1,1}$ | | $G_{a,b-1}$ | |
| | $G_{a-1,b}$ | $G_{a,b}$ | $G_{a+1,b}$ |
| | | $G_{a,b+1}$ | |

**圖一　$G_{a,b}$ 與鄰近叢集關係圖**

### 3.2 符號定義

表二說明本文分散式金鑰管理機制 D-EBS 所採用的符號與意義。

**表二　符號定義表**

| 符號 | 定義 |
|---|---|
| $n_i$ | $id$ 為 $i$ 的感測節點 |
| $Grid_{a,b}$ | 第 $a$ 列第 $b$ 行的網格 |
| $G_{a,b}$ | $Grid_{a,b}$內感測節點集合(群組) |
| $CH_{a,b}$ | $G_{a,b}$ 中的叢集首 |
| $BS$ | 基地台，亦即初始金鑰分配中心 |
| $K_{n_i,n_j}$ | $n_i$ 與 $n_j$ 所共享的金鑰 |
| $K_{G_{a,b}}$ | $G_{a,b}$內的共同金鑰(Common Key) |
| $K_{ini\_uni}^{n_i}$ | $n_i$ 的唯一初始金鑰 (Unique Initial Key) |
| $K_{ini\_com}$ | 節點初始共享金鑰(Initial Common Key) |
| $E_K(msg)$ | 使用金鑰 $K$ 對訊息 $msg$ 加密 |
| $EBS_{a,b}$ | $G_{a,b}$ 所使用的 EBS 矩陣 |
| $EBS_{a,b}^{n_i}$ | $n_i$ 所擁有的 $EBS_{a,b}$ 金鑰子集 |
| $K_{EBS_{a,b}}^{u}$ | $EBS_{a,b}$ 中 $id$ 為 $u$ 的金鑰 |
| $H(x)$ | 單向雜湊函式(One-way Hash Function) |

### 3.3 分散式互斥基底金鑰管理機制 (Distributed EBS，D-EBS)

本文所提 D-EBS 的金鑰管理機制可分成三個階段，分別為金鑰預置階段 (Key Pre-distribution Phase)、金鑰設定階段 (Key Setup Phase)、與通訊階段 (Communication Phase)，茲分述如下。

#### 3.3.1 金鑰預置階段

金鑰預置階段的作業時間點在感測節點佈署至目標感測區域前。在此階段，BS(即初始金鑰分配中心)會預先將一些必要的安全資訊 (Security Information) 儲存至各個感測節點內，以為第二階段金鑰設定預作準備。此階段感測節點 $n_i$ 所需儲存的資訊計有：

(1) 一個與 BS 共享的私有秘密金鑰 (Secret Key) $K_{n_i,BS}$，用以加密與 BS 之間的通訊資料，同時 BS 亦可以此金鑰

認證 $n_i$。

(2) 一個不同於金鑰 $K_{n_i,BS}$ 的唯一初始金鑰 (Unique Initial Key) $K_{ini\_uni}^{n_i}$ ；所有感測節點的唯一初始金鑰皆不同，此金鑰將用以產生 EBS 金鑰，見下述。

(3) 一個與所有節點共享的初始金鑰 (Initial Common Key) $K_{ini\_com}$ ，此金鑰將被用以產生最初始的群組金鑰 $K_{G_{a,b}}$ ，見下述。

(4) 一個不可逆的單向雜湊函式 (One-way Hash Function) $H(x)$ ，用以計算新的金鑰。

### 3.3.2 金鑰設定階段

此階段的運作時間點在感測節點佈署至目標感測區域後的一小段時間內，目的是為建立往後通訊協定加、解密訊息所需之金鑰集 (Key Set)。為了保證金鑰系統之安全可行，我們參考了過去一些文獻，假設於此設定階段完成前，感測節點皆不會遭受惡意者的捕獲或入侵[20]。設定階段的作業流程可細分成四個步驟：

步驟一： $G_{a,b}$ 內的感測節點 $n_i$ 透過網格座標 $(a,b)$，及其內置之單向雜湊函式計算取得叢集(群組)共通金鑰 $K_{G_{a,b}}$。

步驟二：叢集 $G_{a,b}$ 決定叢集內的叢集首 $CH_{a,b}$。叢集首的挑選方式因非本文探討重點，故不在文中贅述。

步驟三： $CH_{a,b}$ 建構出屬於自己叢集的 EBS 金鑰系統矩陣，$EBS_{a,b}$。

步驟四： $G_{a,b}$ 將 $EBS_{a,b}$ 的金鑰資訊分別傳送至對應的感測節點，同時更新 $K_{G_{a,b}}$。

當感測節點完全佈署至目標感測區域之後，便即刻進行設定階段各項步驟。首先，在 $G_{a,b}$ 內的感測節點利用自己的叢集座標 $(a,b)$ 與節點共享初始金鑰 $(K_{ini\_com})$，透過單向雜湊函式，計算取得所屬叢集(網格)共享金鑰 $K_{G_{a,b}} = H(K_{ini\_com}, a, b)$。同時亦推算出與鄰近叢集的共享金鑰 $K_{G_{a+1,b}}$、$K_{G_{a-1,b}}$、$K_{G_{a,b+1}}$ 與 $K_{G_{a,b-1}}$。之後，即將 $K_{ini\_com}$ 從記憶體中刪除，以避免當有感測節點遭到捕獲 (captured) 時，金鑰 $K_{G_{a,b}}$ 遭到破解。詳細理由將在章節 4.2 中討論。

當叢集 $G_{a,b}$ 的叢集首 $CH_{a,b}$ 被選出之後， $CH_{a,b}$ 可得知自己叢集內感測節點的數量 $N_{a,b}$ ，並與鄰近叢集之叢集首交換彼此的數量資訊，來取得 $N_{a+1,b}$ 、 $N_{a-1,b}$ 、 $N_{a,b+1}$ 與 $N_{a,b-1}$。再帶入 $EBS(n,k,m)$ 條件公式，計算出所需的金鑰數量 $k+m$ 和單一感測節點應持有的金鑰數量 $k$ ，其中 $n = N_{a,b} + N_{a+1,b} + N_{a-1,b} + N_{a,b+1} + N_{a,b-1}$。此時叢集首 $CH_{a,b}$ 即可產生 $EBS_{a,b}$ 所需的金鑰 $K_{EBS_{a,b}}^{u}$，其中 $u = 1,2,\ldots,k+m$ 。$K_{EBS_{a,b}}^{u}$ 的產生可由下列單向雜湊函式計算而得。

$$K_{EBS_{a,b}}^{u} = H(K_{ini\_uni}^{CH_{a,b}}, nonce_u)$$

其中 $nonce_u$ 為一足可產生不同 $K_{EBS_{a,b}}^{u}$ 金鑰之亂數。 $CH_{a,b}$ 成功產生所有 $K_{EBS_{a,b}}^{u}$ 後，亦會將 $K_{ini\_uni}^{CH_{a,b}}$ 立刻更新，其運算之單向雜湊函式如下：

$$K_{ini\_uni}^{CH_{a,b}}{}' = H(K_{ini\_uni}^{CH_{a,b}}, a, b)$$

進行此動作之目的在於避免節點遭到捕獲後，入侵者可藉由 $K_{ini\_uni}^{CH_{a,b}}$ 金鑰推導出過去的 $EBS_{a,b}$，並進一步地危害現有的金鑰系統。詳細理由亦將在 4.2 章節中詳述。

當 $EBS_{a,b}$ 成功建立後，$CH_{a,b}$ 便利用 $K_{G_{a,b}}$ 對 $K_{EBS_{a,b}}^{u}$ 加密，並分送至對應的感測節點上。其中亦包括鄰近叢集的成員。當然，若管理者對 $K_{G_{a,b}}$ 加密之安全性有所顧慮，則可在金鑰預置階段時，讓每一感測節點 $n_i$ 額外儲存一個對稱多項式金鑰函式 $f(x,y)$ (具 $f(x,y) = f(y,x)$特性)，於此時利用此函式計

算出對個別節點之金鑰後，再利用此金鑰對 $EBS_{a,b}$ 之金鑰子集分配訊息加密後，以一對一方式，將訊息分送至 $EBS_{a,b}$ 內所含的感測節點。然此方式因採用單點傳輸(Unicasting)，故所花費時間將較使用叢集共通金鑰 $K_{G_{a,b}}$ 群播方式更長，間接增長設定階段所需時間，也提高金鑰被破解的可能性。此二種方式各有利弊，端視使用者之需求而定。當此步驟完成後，$CH_{a,b}$ 也將立即對成員節點(包括鄰近節點的節點)進行一次 $K_{G_{a,b}}$ 的更新。新的 $K_{G_{a,b}}$ 取得方式如下：

$$K_{G_{a,b}}^{'} = H(K_{ini\_uni}^{CH_{a,b}}{}', a, b)$$

### 3.3.3 通訊階段

經過設定階段後，叢集 $G_{a,b}$ 內一般感測節點 $n_i$ 與叢集首 $CH_{a,b}$ 所持有的金鑰資訊綜合如下：

- 一般感測節點 $n_i$ ：
  (1). $K_{n_i,BS}$
  (2). $K_{G_{a,b}}$、$K_{G_{a+1,b}}$、$K_{G_{a-1,b}}$、$K_{G_{a,b+1}}$、$K_{G_{a,b-1}}$
  (3). $K_{ini\_uni}^{n_i}$
  (4). $EBS_{a,b}^{n_i}$、$EBS_{a+1,b}^{n_i}$、$EBS_{a-1,b}^{n_i}$、$EBS_{a,b+1}^{n_i}$、$EBS_{a,b-1}^{n_i}$
  (5). $H(x)$
- 叢集首 $CH_{a,b}$：
  (1). $K_{CH_{a,b},BS}$
  (2). $K_{G_{a,b}}$、$K_{G_{a+1,b}}$、$K_{G_{a-1,b}}$、$K_{G_{a,b+1}}$、$K_{G_{a,b-1}}$
  (3). $K_{ini\_uni}^{CH_{a,b}}$
  (4). $EBS_{a+1,b}^{CH_{a,b}}$、$EBS_{a-1,b}^{CH_{a,b}}$、$EBS_{a,b+1}^{CH_{a,b}}$、$EBS_{a,b-1}^{CH_{a,b}}$
  (5). $EBS_{a,b}$
  (6). $H(x)$

在通訊階段，感測節點將使用其內擁有的金鑰資訊組成更嚴謹的通訊金鑰，並用於各種不同通訊型態下的資訊加密。D-EBS 的通訊型態可分成三種：節點至叢集首的通訊、叢集首之間的通訊、與節點至基地台的通訊。由於叢集式繞徑協定，資料最後通常是由叢集首傳遞至基地台。在 D-EBS 中，叢集首當然為一般節點，故叢集首與基地台的通訊可視為節點至基地台的通訊型態。

節點至基地台的通訊的方法極為單純，只需利用兩者共享的私有金鑰 $K_{n_i,BS}$ 對訊息加密，產生 $E_{K_{n_i,BS}}(msg)$，即可互相通訊。

至於節點 $n_i$ 至叢集首 $CH_{a,b}$ 的通訊則會使用 $EBS_{a,b}$ 與 $EBS_{a,b}^{n_i}$ 的訊息。由於 $CH_{a,b}$ 持有的金鑰集合為

$EBS_{a,b}^{CH_{a,b}} = \{K_{EBS_{a,b}}^{1}, K_{EBS_{a,b}}^{2}, \ldots, K_{EBS_{a,b}}^{k+m}\}$，

$n_i$ 持有的金鑰子集為

$EBS_{a,b}^{n_i} = \{K_{EBS_{a,b}}^{u_1}, K_{EBS_{a,b}}^{u_2}, \ldots, K_{EBS_{a,b}}^{u_t}\}$，

其中 $t$ 為 $n_i$ 所擁有的 EBS 金鑰數，

又 $EBS_{a,b}^{n_i} \subset EBS_{a,b}^{CH_{a,b}}$。因此 $CH_{a,b}$ 可從 EBS 中得知 $n_i$ 持有的金鑰集合，因此兩者的共同金鑰可計算為

$K_{CH_{a,b},n_i} = K_{EBS_{a,b}}^{u_1} \oplus K_{EBS_{a,b}}^{u_2} \oplus \ldots \oplus K_{EBS_{a,b}}^{u_t}$。

由於 EBS 金鑰矩陣中，$EBS_{a,b}^{n_i} \neq EBS_{a,b}^{n_j}$ 、$i \neq j$，故 $K_{CH_{a,b},n_i} \neq K_{CH_{a,b},n_j}$。因此 $n_i$ 與 $CH_{a,b}$ 之間的通訊將可保有隱密性。

叢集首 $CH_{a,b}$ 與鄰近叢集首 $CH_{e,f}$ 通訊則會使用到 $EBS_{a,b}$、$EBS_{a,b}^{CH_{e,f}}$、$EBS_{e,f}$、$EBS_{e,f}^{CH_{a,b}}$等金鑰矩陣資訊，其中 $(e,f) = (a \pm 1, b)$ 或 $(a, b \pm 1)$。值得再提醒的是，D-EBS 機制於金鑰設定階段時 $G_{a,b}$ 內的感測節點，除了隸屬於 $EBS_{a,b}$ 的金鑰系統外，亦同時隸屬於鄰近的 $EBS_{e,f}$ 的成員。換言之

$EBS_{a,b}^{CH_{e,f}} = \left\{K_{EBS_{a,b}}^{u_1}, K_{EBS_{a,b}}^{u_2}, \ldots, K_{EBS_{a,b}}^{u_t}\right\}$、

$EBS_{a,b}^{CH_{e,f}} \subset EBS_{a,b}$，同時

$EBS_{e,f}^{CH_{a,b}} = \left\{K_{EBS_{e,f}}^{v_1}, K_{EBS_{e,f}}^{v_2}, \ldots, K_{EBS_{e,f}}^{v_s}\right\}$、

$EBS_{e,f}^{CH_{a,b}} \subset EBS_{e,f}$。因此，兩者的共通金鑰可計算如下：

$$K_{CH_{a,b},CH_{e,f}} = K_{EBS_{a,b}}^{u_1} \oplus K_{EBS_{a,b}}^{u_2} \oplus \ldots \oplus K_{EBS_{a,b}}^{u_t} \oplus K_{EBS_{e,f}}^{v_1} \oplus K_{EBS_{e,f}}^{v_2} \oplus \ldots \oplus K_{EBS_{e,f}}^{v_s}$$

由於上述金鑰取得均採行最簡單的互斥運算(Exclusive OR)，計算複雜度並不高，故不會對節點能源造成太多的浪費。再者，金鑰 $K_{CH_{a,b},CH_{e,f}}$ 乃是由雙方 EBS 交集組成，其集合與任一節點持有之金鑰皆不相同，故亦可保證兩者通訊之機密性。

當然，以上僅為 D-EBS 金鑰管理機制的基本觀念與作法，至於其他因網路條件變化所產生相關管理措施與特性，則在下一章說明與討論。

## 4. 金鑰相關管理措施與特性之討論

隨著網路運作環境的改變 (如節點增減、節點被擄獲 )，D-EBS 機制亦可能必須相對地配合應變。因此，本章節中，將進一步地深入討論 D-EBS 運作期間其他相關的管理措施。

### 4.1 金鑰系統之變動

在網路的持續運作下，金鑰系統亦可能隨著感測節點的新增與移除，或叢集首的輪替而發生改變，以下則針對各種情況討論。

#### 4.1.1 節點未遭受擄獲攻擊時

(1) **正常運作下 EBS 金鑰矩陣之轉移**

由於本文中無線感測網路乃以叢集結構為基礎，為平衡節點能源耗損，正常運作下叢集首可能需經常更換，而在更換的過程，新、舊叢集首必須交接其金鑰矩陣。但金鑰矩陣的移轉，不需重新計算獲得，只需將新叢集首所缺少的金鑰，以及矩陣中感測節點 ID 順序，經舊叢集首傳送即可。

舉例來說，假設新叢集首為 $CH_{new}$，金鑰移轉前持有金鑰 $K_3$、$K_4$、$K_5$，而缺少金鑰 $K_1$、$K_2$；舊叢集首為 $CH_{old}$ ，移轉前持有金鑰包括 $K_1$ 至 $K_5$。此時 $CH_{new}$ 可在 $CH_{old}$ 告知 $EBS(n,k,m)$ 中參數 $k$ 與 $m$ 後，自行產生一個與 $CH_{old}$ 相同特徵之矩陣(意即同樣大小，0 與 1 位置亦相同之矩陣)，但其中不包括金鑰 $K_1$、$K_2$，與感測節點對應之順序。此時， $CH_{old}$ 僅需將金鑰 $K_1$、$K_2$以及感測節點之順序傳送至新叢集首 $CH_{new}$ ，並將自身的金鑰 $K_1$、$K_2$移除，取代原先 $CH_{new}$ 的位置即可。新叢集首 $CH_{new}$ 則將矩陣內的 $CH_{new}$ id 改成 $CH_{old}$ 。至此，$CH_{new}$ 即可完全繼承 $CH_{old}$ 的金鑰資訊，扮演新叢集首的角色。

(2)**正常運作下節點之移除與新增**

在網路正常運作下，感測節點可能因能源耗盡或其他因素而需自網路中移除，此時，可利用第二章 EBS 之基本演算法，解除其金鑰效力後排除之。

至於新節點之加入，則 BS 必須通知新節點擬加入群組之叢集首 $CH_{a,b}$ ，以協助其相關通訊金鑰之建立。由於 D-EBS 機制中，BS 所持有的金鑰資訊並不包括各個叢集群組之共通金鑰，以及 EBS 矩陣金鑰。因此，BS 與 $CH_{a,b}$ 的通訊金鑰僅能透過兩者之私有金鑰 $K_{CH_{a,b},BS}$ 為之。當欲將新節點 $n_{add}$ 新增至叢集 $G_{a,b}$ 時，其步驟大致如下：

(1). $n_{add}$ 預置金鑰訊息： $K_{n_{add},BS}$、$K_{ini\_uni}^{n_{add}}$、$K_{temp}^{n_{add}}$、$H(x)$

其中 $K_{temp}^{n_{add}}$ 為新增節點與其叢集首溝通之金鑰，其餘三者為加入網路後，通訊金鑰建立時所需之基本金鑰資訊。

(2). 將 $n_{add}$ 佈署至 $G_{a,b}$。

(3). BS 傳送下列訊息至 $CH_{a,b}$：

$$E_{K_{CH_{a,b},BS}}(add\_node(n_{add}), K_{temp}^{n_{add}})$$

(4). $CH_{a,b}$ 分配 $EBS_{a,b}^{n_{add}}$ 矩陣金鑰後，加密後傳送至 $n_{add}$：

$$E_{K_{temp}^{n_{add}}}(K_{G_{a,b}}, EBS_{a,b}^{n_{add}})$$

(5). $CH_{a,b}$ 與 $n_{add}$ 同時刪除 $K_{temp}^{n_{add}}$，此時新增節點工作完成。

當然，$n_{add}$ 加入時亦將同時影響鄰近叢集 EBS 金鑰矩陣的變化，BS 亦須同時傳遞相關訊息至 $G_{a,b}$ 鄰近叢集之叢集首，以啟動新增節點管理機制。

#### 4.1.2 節點遭受擄獲攻擊時

事實上網路運作期間，節點隨時都會遭受外力攻擊。當感測節點遭到惡意者擄獲時，必須做最壞的考量：假設節點內所有金鑰資訊都被惡意者完全破解。為了讓網路傷害降至最低，必須立刻撤銷或更改淪陷節點所持有的全部金鑰，並將淪陷節點從網路中移除。同時亦更新其它正常節點內的相關金鑰。此為金鑰重置與撤銷之意義。關於此部分將分成兩個方向來討論。

(1) **一般節點遭擄獲之情況**

對叢集首 $CH_{a,b}$ 而言，當其中節點 $n_i$ 遭到捕獲時，可透過第二章所述之 EBS 演算法，找出 $n_i$ 所缺少的金鑰，再利用這些金鑰加密新的金鑰訊息，通知同屬相同 EBS 系統中的其他感測節點變更(包括鄰近叢集的節點)。當然，對鄰近叢集首 $CH_{e,f}$ 而言，$n_i$ 亦隸屬於其 EBS 系統一員，故其金鑰重置與撤銷方法亦與 $CH_{a,b}$ 雷同。

(2) **叢集首遭擄獲之情況**

設若叢集首 $CH_{a,b}$ 遭受惡意者捕獲時，其所掌握之金鑰矩陣亦讓惡意者知曉，即 $EBS_{a,b}$ 遭到破解。此時 $CH_{a,b}$ 無法由自身 $EBS_{a,b}$ 機制撤銷。但因 $CH_{a,b}$ 本身仍為鄰近 $EBS_{e,f}$ ( $(e,f) = (a \pm 1, b)$ 或 $(a, b \pm 1)$)之一員，因此可由鄰近叢集首 $CH_{e,f}$ 啟動，來進行 $CH_{a,b}$ 金鑰重置與撤銷作業，並啟動挑選新叢集首，重建 $EBS_{a,b}$ 新金鑰矩陣。同時，相關叢集群組金鑰也將更新為最新版本。

### 4.2 舊有金鑰資訊刪除之必要性

在 3.3.2 章節的設定階段內，我們曾提及在一些新的金鑰被產生後，需立刻將舊有金鑰移除或更新(前者如 $K_{ini\_com}$，後者如 $K_{ini\_uni}^{CH}$ 以及 $K_{G_{a,b}}$)，以避免入侵者破解密碼系統，其理由敘述如下：

在 D-EBS 中，EBS 金鑰第一次被分配到感測節點時所使用的加密金鑰為叢集群組金鑰 $K_{G_{a,b}}$，也就是傳送 $E_{K_{G_{a,b}}}(EBS_{a,b}^{n_i})$ 訊息。此時入侵者若攔獲該訊息，短期內雖然無法解讀 $E_{K_{G_{a,b}}}(EBS_{a,b}^{n_i})$，但仍可先將此訊息保留。俟入侵者擄獲感測節點取得 $K_{G_{a,b}}$ 後，即可解密所保留的資訊，進而破解取得 $EBS_{a,b}^{n_i}$。再者，由於所有節點的 EBS 金鑰分配訊息皆是群播方式，入侵者亦可輕易竊聽並保留，最後終將破解出 $EBS_{a,b}$。因此，在第一次配置 EBS 金鑰後， $K_{G_{a,b}}$ 與 $K_{ini\_com}$ 必須立刻更新或移除，以避免入侵者有機可乘。

又由於 D-EBS 金鑰矩陣建立完成並正常運作後，後續金鑰之更新均透過舊有金鑰加密新的金鑰後傳送，如 $E_{K_2}(E_{K_1}(K_1'))$ 。其中舊有金鑰 $K_1$ 與 $K_2$ 由舊叢集首 $CH_{old}$ 所產生，新的金鑰 $K_1'$ 由現任叢集首 $CH_{new}$ 所產生。假設此時 $CH_{old}$ 遭到入侵者擄獲，且 $K_{ini\_uni}^{CH_{old}}$ 亦未更新，則入侵者有可能利用 $K_{ini\_uni}^{CH_{old}}$ 推出舊有的 EBS 金鑰 $K_1$ 及 $K_2$。又

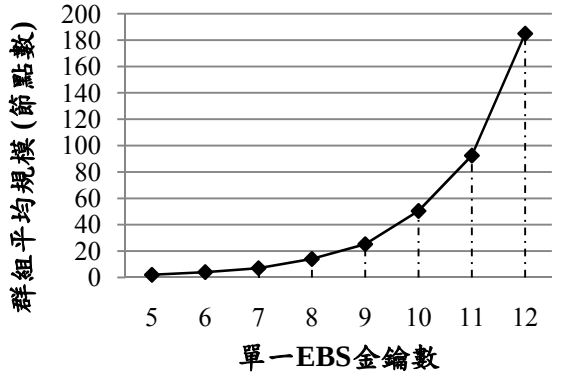
倘若入侵者也竊聽保留訊息 $E_{K_2}(E_{K_1}(K_1'))$ ，則可解出新的 EBS 金鑰 $K_1'$，使得新建立的 EBS 完全遭到破解。因此， 在產生 EBS 金鑰後，$K_{ini\_uni}^{CH_{old}}$ 也必須立刻進行更新。

### 4.3 特性分析

說明了 D-EBS 金鑰管理機制的管理細節後，以下將對 D-EBS 的良好特性作分析。

#### 4.3.1 延展性(Scalability)

所謂的延展性我們定義為，當網路規模成長時，每個感測節點為了維持 D-EBS 運作所需負擔的金鑰記憶體之增長情形。由於 D-EBS 中的金鑰數量乃決定於所含叢集節點數量的多寡，使用者或可視情況調整叢集(網格)大小或節點密度，以控制叢集內的節點數量，如此 D-EBS 之金鑰矩陣將不會受到整體網路大小之嚴重衝擊，記憶體空間需求能有效控制，故其延展性可謂良好。圖二為 D-EBS 機制中，單一 EBS 系統內金鑰數量與叢集規模之關係圖。圖中顯示當金鑰數目為 10 時，可支援至每個叢集內含 50 個感測節點，而到了金鑰數目為 12 時，則可大幅增長支援 180 個感測節點以上的使用。




**圖二 EBS 之金鑰數量與叢集規模關係圖**

#### 4.3.2 相容性與容錯能力

D-EBS 的架構考量是以可實作之環境為基礎，因此對於叢集式繞徑中各個階層之通訊，皆考慮了其金鑰管理之安全，以使其能正常通訊。如一般節點與叢集首、叢集首之間、一般節點至 BS，皆有不同之專用金鑰，以防其他節點竊聽。因此對於叢集式繞徑協定，D-EBS 在應用上具有良好的相容性。

此外，D-EBS 機制也藉由叢集與叢集間成員的交錯包含，使得各個叢集的 EBS 得以產生交集，以保障管理上的嚴密性。雖然在金鑰重置與撤銷時，會連動影響鄰近叢集，但同時也增加了金鑰系統的容錯(Fault Tolerance)能力。當叢集 $G_{a,b}$ 之 $EBS_{a,b}$ 遭到破解時，鄰近叢集或可利用重疊之 EBS 重建其相關金鑰，此為金鑰系統之容錯。

## 5. 結論

本文以互斥基底系統(EBS)為基礎，提出了一個應用於叢集式無線感測網路之分散式金鑰管理機制，D-EBS。D-EBS 可在不依賴傳統金鑰分配中心的情形下，快速且有效地進行的金鑰分配、更新、與撤銷維護作業，並藉由叢集群組交織之特性，建構出更安全的管理效果、容錯效果，來保障通訊安全。除此之外、D-EBS 因擁有高度的延展性，更能符合大型無線感測網路的金鑰管理需求。

## 參考文獻

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y. and Cayirci, E., “A Survey on Sensor Networks,” ***IEEE Communications Magazine***, Vol. 40, Issue 8, pp. 102–114, Aug. 2002.

[2] Beutelspacher, A., ***The Future Has Already Started or Public Key Cryptography***, Cryptology, translation from German by J. Chris Fisher, pp. 102, 1994,

[3] Blundo, C., Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M., “Perfectly-Secure Key Distribution for

Dynamic Conferences," ***Advances in Cryptology – CRYPTO '92, LNCS 740***, pp. 471-486, 1993.

[4] Biham, E. and Shamir, A., ***Differential Cryptanalysis of the Data Encryption Standard***, Springer Verlag, 1993.

[5] Chan, H., Perrig, A. and Song, D., "Random Key Predistribution Schemes for Sensor Networks," ***IEEE Symposium on Security and Privacy,*** pp. 197-213, 2003.

[6] Diffie, W. and Hellman, M., "New Directions in Cryptography," ***IEEE Transactions on Information Theory***, Vol. 22, Issue 6, pp. 644–654, Nov. 1976.

[7] Eltoweissy, M., Heydari, M.H., Morales, L. and Sudborough, I.H., "Combinatorial Optimization of Group Key Management," ***Journal of Network and Systems Management***, Vol. 12 Issue 1, pp. 33-50, Mar. 2004.

[8] Eschenauer, L. and Gligor, V., "A Key-Management Scheme for Distributed Sensor Networks," ***Proceeding of 9th ACM Conference on Computer and Communications Security***, pp. 41-47, Nov. 2002.

[9] Heinzelman, W.R., Chandrakasan, A.P. and Balakrishnan, H., "An Application Specific Protocol Architecture for Wireless Microsensor Networks," ***IEEE Transactions on Wireless Communications***, Vol. 1, Issue 4, pp. 660-670, Oct. 2002.

[10] Heinzelman, W.R., Chandrakasan, A. and Balakrishnan, H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," ***Proceedings of the 33rd Annual Hawaii International Conference on System Sciences***, Vol.2, pp. 1-10, Jan. 2000.

[11] Ito, T., Ohta, H., Matsuda, N. and Yoneda, T., "A Key Pre-Distribution Scheme for Secure Sensor Networks Using Probability Density Function of Node Deployment," ***Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks,*** pp. 69-75, Nov. 2005.

[12] Lindsey, S. and Raghavendra, C. S., "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," ***IEEE Aerospace Conference Proceedings***, Vol. 3, pp. 1125-1130, 2002.

[13] Liu, D. and Ning, P., "Establishing Pairwise Keys in Distributed Sensor Networks," ***Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS'03)***, pp. 52–61, 2003.

[14] Moharrum, M., Eltoweissy, M. and Mukkamala, R. "Dynamic Combinatorial Key Management Scheme for Sensor Networks," ***Wireless Communications & Mobile Computing***, Vol.6, Issue 7, pp. 1017-1035, Nov. 2006.

[15] Newsome, J., Shi, E., Song, D. and Perrig, A., "The Sybil Attack in Sensor Networks: Analysis & Defenses," ***Third International Symposium on Information Processing in Sensor Networks, 2004***, pp. 259-268, Arp. 2004.

[16] Parno, B., Perrig, A. and Gligor, V., "Distributed Detection of Node Replication Attacks in Sensor Networks," ***IEEE Security and Privacy Symposium***, May 2005.

[17] Peng, T., Leckie, C. and Ramamohanarao, K., "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems," ***ACM Computing Surveys (CSUR)***, Vol. 39, Issue 1, No. 3, 2007.

[18] Römer, K. and Mattern, F., "The Design Space of Wireless Sensor Networks," ***IEEE Wireless Communications***, Vol. 11, Issue 6, pp. 54-61, Dec. 2004.

[19] Ye,F., Luo,H., Cheng, J., Lu,S. and Zhang, L., "Sensor Networks: A Two-Tier Data Dissemination Model for Large-scale Wireless Sensor Networks," ***Proceedings of the 8th Annual ACM/IEEE International Conference on Mobile Computing and Networking***, pp.148-159, Sept. 2002.

[20] Zhu, S., Setia, S. and Jajodia, S., "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," ***Proceedings of the 10th ACM conference on Computer and Communications Security***, pp. 62-72, 2003.