Journal of Science and Engineering Technology, Vol. 4, No. 2, pp. 43-50 (2008)

適用於無線感測網路上動態金鑰管理協定

陳金鈴　李政達
朝陽科技大學資訊工程研究所
413 台中縣霧峰鄉吉峰東路 168 號

摘　要

近幾年來，無線感測網路廣泛地應用在許多領域上，例如：在無線感測網路中，當感測節點被佈置在敵方地區時，爲了能使感測節點間的傳輸更爲安全，必須要使用秘密的金鑰做爲它們之間的通訊。雖然現今已經有許多金鑰建立的方法被提出，且應用在各種類型的無線感測網路中，但在目前的方法中，大部份都是預先從金鑰池中選出 m 把金鑰，形成一個金鑰鏈，每個感測節點再使用這些金鑰鏈的金鑰來進行資料的加密。然而在傳送秘密金鑰時，這把秘密金鑰很容易暴露在傳送的路徑中。本文提出了一種動態金鑰管理協定，跟之前的方法比較，我們提出的方法可以提高金鑰的安全性，而且透過動態的更新金鑰，使得金鑰被猜中的機率降低，除此之外，透過我們所設計的協定，也可避免感測網路上被攻擊的情況發生。

關鍵詞：無線感測網路，金鑰管理，安全性

A Dynamic Key Management Protocol for Wireless Sensor Network

CHIN-LING CHEN and CHENG-TA LI
Computer Science and Information Engineering, Chaoyang University of Technology
168 Jifong E. Rd., Wufong Township, Taichung County, 41349, Taiwan

ABSTRACT

Recently, wireless sensor networks have been extensively used in different domains. For example, if the wireless sensor node of such a network is disposed in an unfriendly area, a secret key must be used to protect the transmission between the sensor nodes. Although several methods for making the key have been proposed and already adopted in different types of networks, most of the existing methods involve pre-selecting m keys from a key pool to form a key chain. Then, the sensor nodes utilize the key in the chain to encrypt the data. However, a secret key can be easily exposed along the transmission path. This research proposes a dynamic key protocol that can improve the security of the key, compared with existing methods. Moreover, the dynamic update of the key can reduce the probability of its being correctly guessed. Furthermore, with this new protocol, an attack on the wireless sensor network can be avoided.

Key Words: wireless sensor network, key management, security

一、前言

（一）感測網路的組成與應用

無線感測網路的主要組成單元，可分爲四個單元，分別爲感測單元、處理單元、傳輸單元、電力供應單元，以下將詳細介紹各單元的主要功能：

1. 感測單元：感測元件負責偵測，而蒐集到的資料使用類比訊號表示，經由訊號轉換元件，負責將感測元件感測到的類比訊號轉換成數位訊號，並將資料送到處理單位加以處理。
2. 處理單元：處理單元裏包含了儲存元件和處理元件，儲存元件的功能類似電腦中的儲存裝置，將蒐集到的資訊儲存在儲存元件中，在經由處理元件，功能類似個人電腦中的中央處理機，負責執行事先儲存好的程式碼，以協調並控制感測器之間不同的單位元件。處理元件可以根據原先所儲存的程式指令，或是藉由後端伺服器所發送的命令，啓動感測單元來收集資訊，並將所收集的資料經過彙整後，透過傳輸單元將資料發送回去。
3. 傳輸單元：傳輸單元主要負責連接感測器與其他感測器之間的溝通，或是將感測器的資料傳送到基地台。傳輸單元可使用的傳輸介質有紅外線、無線電波、以及光纖介質等，配合環境及應用的不同，可以使用不同的選擇。
4. 電力供應單元：電力供應單元負責感測器中所有單元的電力能量，無論是任何一種功能運作都必須使用電量，是非常重要的單元。通常感測器的電力是由電池所支援，因此在軟硬體的設計上，如何節省電力可以說是最主要考量的因素。

而無線感測網路通常具有多數的部署、低廉的價格、體積小以及電池式的電力供應等特色。無線感測網路的網路路由傳輸方式，主要分爲以下幾種：

1. 叢集式：叢集式架構是最具有代表性的路由協定，其主要作法爲，將網路中大量的感測器分割成數群的叢集，另外再由每個叢集中選出一個節點作爲叢集頭，負責收集叢集裏其它感測節點的資料，並將資料匯合傳送至基地台。
2. 鏈結式：鏈結式是有別於叢集式架構，而以鏈結架構爲基礎的路由協定，它將整個網路中的感測節點互相連結成一條鏈，接著每回合中，從鏈架構的節點裏選擇出一個鏈頭，而兩端鏈架構尾端的節點開始將資料透過相鄰的節點往鏈頭的方向傳送，並且每個接收節點會進行資料的聚集，最後由鏈頭將資料傳送至基地台。

近幾年來，無線感測網路被廣泛的應用在環境的監視，如氣象資料的搜集、健康資訊的監視、戰場上資料的搜集和追蹤等。在不安全的環境裏，使用感測網路去搜集資料，像是在戰場上，應用環境是非常不安全的。因爲敵人可以透過感測節點間傳送資料時，進行竊聽、捕獲節點，來取得節點搜集到的資料。因此在無線感測網路上，加上適合的安全方法是必要的。然而無線感測網路在資源上卻有很大的限制，不管是在處理器、記憶體、頻寬和電池的消耗都有很大的限制。因此選擇一個適合的加密系統，是一個很重要的關鍵。而無線感測節點在硬體資源上的限制，如果要將公開金鑰演算法，像是 Diffie-Hellman 金鑰管理 [4] 或者 RSA 簽章 [10] 等，這類的方法被應用在感測節點的實作上成本太高，且不切實際。

（二）相關研究

在這節裏，我們將回顧現今在無線感測網路上金鑰產生的協定，我們將這些協定分成三類：亂數金鑰預先部署協定、群組金鑰預先部署協定和階層金鑰預先部署協定。

1. 亂數金鑰預先部署

在 2002 年，Eschenauer 等人 [5] 提出了一個亂數金鑰預先配送的架構，此架構包含了三個步驟：金鑰預先部署步驟、偵測分享金鑰步驟和路徑金鑰建立步驟，此架構是每個感測節點在部署前，從一個很大的金鑰池裏選取 m 把金鑰，透過 m 把的金鑰去形成金鑰鏈，分送給各個感測節點，且各個節點間去協商出一把金鑰，使用這把金鑰在他們群組裏傳送資料，這個方法雖然可達到安全性，但相對的，每個感測節點必需記憶 m 把的金鑰，對於感測節點來說，在記憶體和電源消耗都是一個問題。Pietro 等人 [9]，提出了一個亂數金鑰配送協定，由在每個感測節點間，去配送亂數金鑰，使得任兩個感測節點間能夠建 立起溝通管道，此方法的缺失也在於每個感測節點必須去記憶三把以上的金鑰，如要將安全性提高，往往都需要再增加金鑰個數，但一增加金鑰個數，則感測節點的負載就會更重，資源的消耗也更爲嚴重。

2. 群組金鑰預先部署協定

所謂的群組金鑰預先部署協定，是將要佈署節點的區域劃分出來，分成數個群組，在經由直升機空投到劃分好的區域，透過預先劃分的區域，使得感測節點間有較高的溝通機率。Liu 等人 [8]，提出了一對金鑰協定，基於多項式金鑰

池和格子式金鑰預先配送下，此協定在針對感測節點捕獲攻擊和溝通上有較高的彈性。但在計算金鑰的運算方面，所使用到的運算較爲複雜，往往在產生金鑰方面會花較長的時間，雖然可提高安全性，但較不能達到感測網路所需的即時性與方便性。

3. 階層架構協定

在階層架構協定中，會包含有數個叢聚節點在基地台和感測節點中，叢聚節點通常有較強的運算能力，在部署前每個叢聚節點會去儲存金鑰，在網路部署後，每個節點會去交換節點的編號，同時也會通知叢聚節點，讓叢聚節點知道感測節點的編號，透過這樣的方法，使得整個網路能進行溝通，但如果當有一個節點被補獲，則叢聚節點和感測節點間的訊息，會很容易的被敵人所知道，因此叢聚節點必需增加金鑰的數量，才能增加安全性，但相對的來說，感測節點的資源有限，使用此方法並不是最好，所以在 2007 年 Cheng 和 Agrawal [3] 提出了經由二元多項式部署，使得每個叢聚節點不再直接去儲存節點的叢聚金鑰，而是儲存二元多項式，透過節點的編號，得到感測節點和叢聚節點間的金鑰。

4. 其它協定

Chan [2] 等人提出了兩個安全的協定，第一個爲，基地台如果想要達到資料的機密性和認證性，必需透過一個有效率的金鑰分享演算法，如：RC5 使用此類的安全演算法去確保資料的認證和隱密性；第二個爲，要確保資料來源的安全，使用一維赫序鏈，像 TESLA（time efficient streamed loss-tolerant authentication）去達到資料的認證。

（三）環境需求條件

1. 資料隱密性：無線感測網路通常都是被部署在我們無法直接到達，或危險的區域來進行監視、搜集資料，例如：敵軍陣地戰場，所以感測節點所搜集到的資料必須是相當準確與機密的。其次，因無線感測網路傳輸的方法，是採用無線射頻的方式傳送，所以當感測節點要將這些機密性的資料回傳給後端伺服器時，如果不使用安全機制來處理資料，則會輕易的曝露傳送的資訊內容，尤其在敵軍的陣地，要傳回資料時，我們必須使用加密系統來完成，加密系統中我們分成兩類：對稱性加密系統和非對稱性加密系統。在對稱加密系統中，感測節點間會共享一把會議金鑰，使用這把金鑰進行傳輸。非對稱加密系統，則是使用公開金鑰的方法，來進行傳輸的工作，但因感測網路上的資源限制，使用非對稱加密系統，成本太高，不切實際。
2. 資料認證：感測網路中，每個區域可能都包含了上百或上千個感測節點，節點間的資料傳輸可能是很常有的事，如果此時節點間包含了一個惡意的節點，不斷地去廣播資料，而感測節點間並沒有使用資料認證，則會使得網路癱瘓；其次是感測節點的資源消耗，使得感測節點的壽命減少，因此如何設計一個通訊回合數少，具有可認證性的動態金鑰管理方式是感測網路中一項重要的議題，傳送端的感測節點可使用共享的金鑰，對要傳送的資料進行加密，接收端的感測節點，也可使用共享的金鑰進行解密。
3. 中間人攻擊：所謂的中間人攻擊法，是指在感測節點和叢聚節點或叢聚節點和基地台間進行互相傳輸資料時，受到惡意感測節點的攔截，將感測節點要傳送的資料進行竄改，然後將竄改的資料再進行傳送，此時接收的感測節點所收到的訊息則不是傳送端所要傳的真正資料，因此後端基地台所收到的資料爲不正確的，所以必需使用加密方法來解決。
4. 重送攻擊：所謂的重送攻擊法，是指在一個區域裏的感測節點，如果有惡意的節點侵入，想去取得感測節點間的金鑰，會使用重覆發送封包的方法，去試著找出感測節點間的金鑰，得到金鑰，進行破壞工作。通常在解決這類的攻擊法，我們會使用接收端和傳送端時間的設定，透過兩端的差值，來判斷封包是否可接受，或者直接丟棄。
5. 記憶體限制：受限於感測節點的體積，所以感測節點的記憶空間也有所限制，每個感測節點的記憶空間通常都在幾十 MB 之間，在加強無線感測網路安全性時，也必需考慮到每個感測節點的記憶體空間。
6. 運算能力限制：每個感測節點裏，都嵌入 CPU 來處理和運算資料，但受限於體積和電力消耗的因素，所使用的 CPU 都爲較低階的 CPU，例如：Intel 公司的 StrongARM [7] 或者 ATmel 公司的 ATmega [1]，都爲常用的 CPU。
7. 本文植基於對稱式加密法、單向雜湊涵數和互斥或匣等運算技術，我們提出了一種動態產生金鑰的方法。並且透過每次感測節點在要傳送資料時，透過之前兩把舊的金鑰，產生出一把新的金鑰，使用這把金鑰將資料加密。此感測節點下次要再傳送資料時，透過新產生的一把金鑰，和舊的其中一把金鑰進行運算，做爲此次要傳送資

料時的金鑰，其它感測節點也是使用此方法。當感測節點傳送給叢聚節點時，此時叢聚節點會向基地台，要求所收到的感測節點的金鑰。因基地台擁有各感測節點初始的兩把金鑰，便將所需的感測節點金鑰傳送給叢聚節點。叢聚節點收到後便可進行解密，當搜集到的資料，個數大於 t 個門檻值時，便將資料進行加密，傳送到基地台，金鑰的產生方法如同一般感測節點的金鑰產生方法，以確保資料的正確性。且基地台和叢聚節點間，以及基地台和感測節點間會動態的更改會議金鑰的其中一把，來提高網路的安全性。

二、本協定內容

（一）符號

在本架構下，會使用到一些符號，以下列出使用到的符號和其代表的涵意：

$h(\,)$：用於產生金鑰的單向赫序函數。

$\oplus$：互斥或匣運算。

a_i、a_{i-1}：預先配置在第 i 個感測節點的兩個產生金鑰的參數。

b_i、b_{i-1}：預先配置在第 i 個叢聚節點的兩個產生金鑰的參數。

msg_{finish}：叢聚節點通知感測節點更新金鑰之訊息。

K_{si}：第 i 次感測節點的金鑰。

K_{ci}：第 i 次叢聚節點的金鑰。

K_{msg}：用於加/解密 msg_{finish} 訊息之金鑰。

$Seed$：預先配置在各感測節點之更新金鑰種子。

ID_{si}：第 i 個感測節點的編號。

ID_{list}：叢聚節點所收到 t 個感測節點編號集合列表，如 $ID_{list}=(ID_{s1},ID_{s2},...,ID_{st})$。

K_{list}：叢聚節點所需的感測節點金鑰，如 $K_{list}=(K_{s1},K_{s2},...,K_{st})$。

T_i：時間參數,i 是整數。

$\triangle T$：傳送端和接收端的時間差值。

M_i：第 i 個感測節點要傳輸的明文資料。

M_f：基地台最後所收到的平均資料值。

$E(M,K)$：架構中所使用的對稱式加密表示法，使用金鑰 K 來將 M 加密。

$D(M,K)$：架構中所使用的對稱式解密表示法，使用金鑰 K 來將 M 解密。

（二）環境條件

1. 無線感測網路裏，我們採用叢聚的管理方法來進行資料的傳輸，通常在一個無線感測網路裏，我們會部署上百或上千個感測節點，並且從我們所部署的感測節點裏去劃分區域，使得每個感測節點可在有效的範圍裏傳輸資料。
2. 在我們每個區域，所部署的感測節點裏，會自動去選取一個感測節點當作一個叢聚節點，當每個感測節點搜集到資料，要將資料傳送到後端基地台時，會將其所搜集到的資料加密並傳送給叢聚節點，當叢聚節點收到一定的封包量時，再將資料整理、加密後傳送到後端基地台（圖 1 為感測網路傳送路徑的示意圖）。
3. 每個感測節點出廠時，我們會預先配置兩個參數，例如：a_i,a_{i-1}，並且使用單向赫序函數方法來產生新的一把金鑰，透過所產生的金鑰來和叢聚節點溝通，叢聚節點也會預先配置兩個參數如：b_i, b_{i-1}，金鑰產生方法如同感測節點。
4. 感測網路第一次被部署完成時，會選出叢聚節點，此時感測節點會發出廣播給叢聚節點，使叢聚節點得知此區域的感測節點有多少個，叢聚節點也會記錄感測節點的編號，以便傳輸資料時使用。
5. 每個感測節點會預先配置一把訊息金鑰 K_{msg} 及一個更新金鑰種子 $Seed$，用來加/解密通知感測節點變更金鑰之訊息，每一回合都會使用赫序函數來變更訊息金鑰，使得感測節點能夠安全獲得變更金鑰訊息。
6. 節點傳輸資料部份，我們使用跳躍式傳輸方式，當第一層感測節點搜集到資料時，會將資料加密，連同感測節點的編號傳送給第二層感測節點，第二層感測節點也會將搜集到的資料加密，連同第一層感測節點傳來的資料

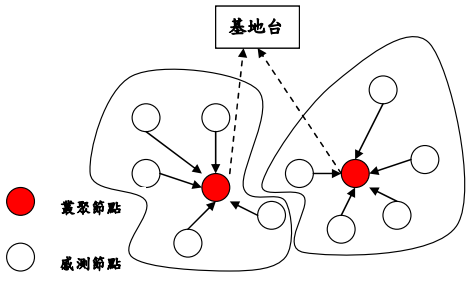

圖 1. 感測網路傳輸路徑

和本身的編號，再傳送給上一層的感測節點，依此類推，當叢聚節點收到一連串的資料時，會由感測節點的編號得知有哪幾個感測節點傳送給它，叢聚節點便可依據感測節點編號的資料，向基地台要求感測節點金鑰列表。

（三）金鑰產生協定

在我們的安全協定裏，使用動態的金鑰管理機制，每個感測節點，會先預分配兩把金鑰，透過這兩把金鑰去產生下一回合新的金鑰。叢聚節點也會預分配兩把金鑰，會議金鑰產生方法如同感測節點。

我們將所提的協定分成下列五個步驟，如圖 2 所示。

步驟 1：當我們所部署的感測節點 i，要回傳所搜集到的資料時，感測節點會使用出廠時預先配置的兩個參數 a_i 和 a_{i-1}，去產生出一把金鑰 K_{si}，$K_{si} = h(a_i, a_{i-1})$，同時也將預先配置在各節點的二把金鑰 K_{msg} 和 *Seed* 進行赫序運算，產生新的訊息金鑰 K'_{msg}，$K'_{msg} = h(K_{msg}, Seed)$，此時感測節點會使用 K_{si} 將測得之資料 M 和預先配置在感測節點上的 K'_{msg} 加密，並連同感測節點的編號 ID_{si} 製成一個完整的封包 C_{si}，$C_{si} = \{E((M_i, K'_{msg}), K_{si})ID_{si}\}$，再傳送 C_{si} 給叢聚節點。

步驟 2：叢聚節點收到大於 t 個封包或大於一事先設定時間時，叢聚節點會去記錄，並傳送資料的感測節點編號 ID_{si}，並將收到的感測節點編號，整理列出一張表 ID_{list}，令 $ID_{list} = (ID_{s1}, ID_{s2},..., ID_{st})$，叢聚節點也會使用預先配置的兩個參數 b_i、b_{i-1}，去產生出一把金鑰 K_{ci}，$K_{ci} = h(b_i, b_{i-1})$，此時叢聚節點會使用 K_{ci} 將 ID_{list} 和時間戳記 T_1 加密，並連同叢聚節點的編號 ID_{ci}，當成一個完整的封包 C_{ci}，$C_{ci} = \{E((ID_{list}, T_1), K_{ci}), ID_{ci}\}$ 傳送給叢聚節點。

步驟 3：當基地台在 T_2 時間收到叢聚節點的封包時，會先確認叢聚節點的編號 ID_{ci}，並依照叢聚節點的編號到資料庫去尋找叢聚節點的金鑰 K_{ci}，使用 K_{ci} 進行解密 $D(C_{ci}, K_{ci}) = (ID_{list}, T_1)$，透過時間參數的計算判斷是否 $T_2 - T_1 \le \Delta T$，如果不符合，則基地台便丟棄此封包，且基地台就可得到由叢聚節點所傳來的 ID_{list}，如果符合，並到資料庫去尋找相對應的感測節點金鑰，整理成金鑰列表 K_{list}，$K_{list} = (K_{s1}, K_{s2},..., K_{st})$，此時基地台會使用 K_{ci} 將 K_{list} 和時間戳記 T_3 加密，將

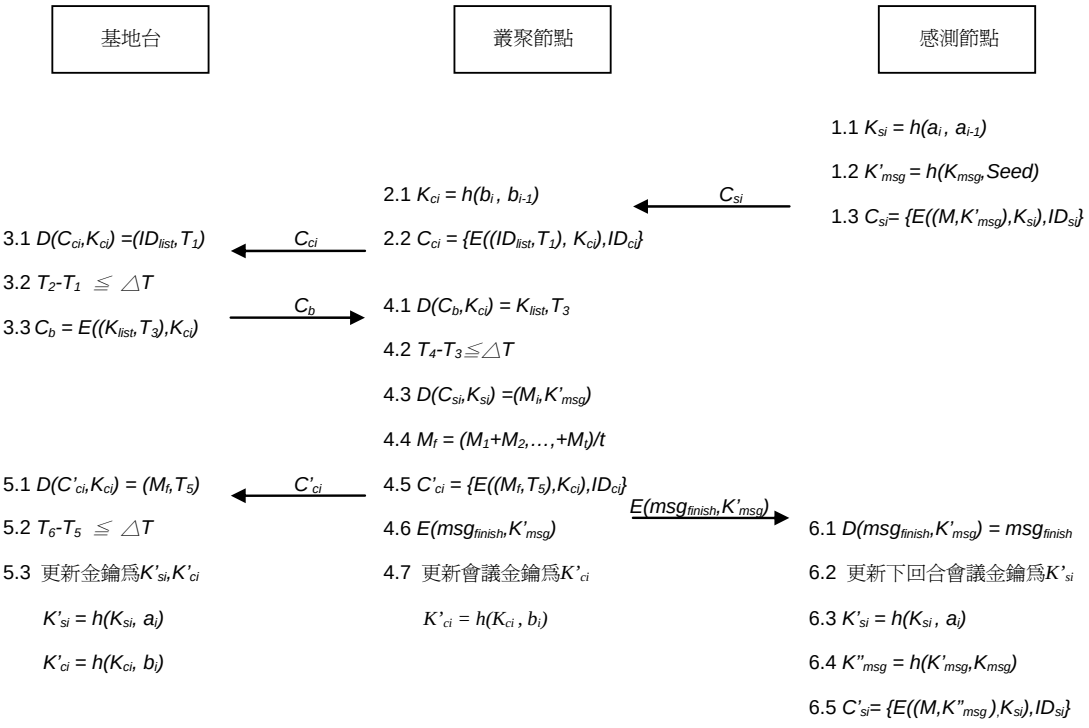

圖 2. 金鑰產生溝通協

加密的資料 C_b，$C_b = \{E((K_{list}, T_3), K_{ci})\}$ 回傳給叢聚節點。

步驟 4：當叢聚節點在 T_4 時間收到基地台回傳的資料時，使用叢聚節點自已產生的金鑰 K_{ci} 進行解密，$D(C_b, K_{ci}) = (K_{list}, T_3)$，透過時間參數的計算判斷是否 $T_4 - T_3 \le \Delta T$，如果不符合，則叢聚節點便丟棄此封包，如果符合叢聚節點便可由 K_{list} 得 K_{si}，得知各個傳送資料過來的感測節點金鑰，個別使用金鑰 K_{si} 進行解密，得到感測節點所回傳的資料 $D(C_{si}, K_{si}) = (M_i, K'_{msg})$，叢聚節點則進行各資料值的平均值運算得到 M_f，$M_f = (M_1+M_2+,...,+M_t)/t$，使得所搜集的資料在傳到後端時，能確保資料更爲正確；此時叢聚節點會使用 K_{ci} 將 M_f 和時間戳記 T_5 加密，並連同叢聚節點的編號 ID_{ci}，當成一個完整的封包 C'_{ci}，$C'_{ci} = \{E((M_f, T_5), K_{ci}), ID_{ci}\}$ 傳送給基地台，此時叢聚節點更新下回合會議金鑰 $K'_{ci} = h(K_{ci}, b_i)$。其次，叢聚節點會使用感測節點傳送過來的訊息金鑰 K'_{msg} 加密傳送完成變更金鑰的訊息 msg_{finish} 且傳送加密完成的封包 $E(msg_{finish}, K'_{msg})$ 廣播給所有感測節點，通知感測節點完成訊息傳送。

步驟 5：在 T_6 時間，基地台收到叢聚節點的封包時，會先確認叢聚節點的編號 ID_{ci}，並依照叢聚節點的編號到資料庫去尋找叢聚節點的金鑰 K_{ci}，並使用 K_{ci} 進行解密 $D(C'_{si}, K_{ci}) = (M_f, T_5)$，透過時間參數的計算判斷是否 $T_6 - T_5 \le \Delta T$，如果不符合，則基地台便丟棄此封包，基地台就可得到由叢聚節點所傳來的資料 M_f，同時基地台也會更新叢聚節點和感測節點的金鑰，更新成爲 K'_{si} 和 K'_{ci}，$K'_{si} = h(K_{si}, a_i)$, $K'_{ci} = h(K_{ci}, b_i)$。

步驟 6：感測節點收到訊息後，使用 K'_{msg} 進行解密得到叢聚節點所傳來的完成訊息 $D(E(msg_{finish}, K'_{msg}), K'_{msg}) = msg_{finish}$，便進行金鑰的替換，使用上一次產生的金鑰 K_{si} 和 a_i 進行運算，產生新的金鑰 K'_{si}，$K'_{si} = h(K_{si}, a_i)$，當下一次要進行回報資料時，便使用 K'_{si} 來進行加密傳送的工作；第二回合感測節點要傳送資料時，原本產生的訊息金鑰 K'_{msg} 需進行變更成 K''_{msg}，$K''_{msg} = h(K'_{msg}, K_{msg})$，感測節點會將變更後的訊息金鑰 K''_{msg} 連同訊息 M 使用 K''_{si} 加密成 C'_{si}，$C'_{si} = \{E((M, K''_{msg}), K_{si}), ID_{si}\}$ 更改過後的 K''_{msg} 爲叢聚節點傳送完成訊息給感測節點的訊息金鑰；同理第三回合感測節點要傳送資料時，需進行變更成 K'''_{msg}，$K'''_{msg} = h(K''_{msg}, K'_{msg})$，感測節點會將變更後的訊息金鑰 K'''_{msg} 連同訊息 M 使用 K'''_{si} 加密成 C'_{si}，$C'_{si} = \{E((M_i, K'''_{msg}), K_{si}), ID_{si}\}$，此處更改過後的會議金鑰 K'_{si} 爲加密傳送量測訊息 M_i 之會議金鑰，而更改過後的 K''_{msg} 及 K'''_{msg} 爲叢聚節點傳送第二及第三回合完成訊息給感測節點的訊息金鑰，金鑰產生方式依此類推。

三、安全性與效能分析

（一）安全性分析

1. 動態金鑰管理：在金鑰產生方面，改變之前預先配送的方法，不再使用從同一個金鑰池裏去挑選 m 把金鑰，在使用這 m 把固定的金鑰去形成一個金鑰鏈。任兩個節點間的溝通都是使用這 m 把金鑰去做協商、溝通。在我們的架構中，我們使用了每傳送一次資料，金鑰就會透過先前兩把舊的金鑰，去產生一把新的金鑰，如：第一次傳輸時 $K_{si} = h(a_i, a_{i-1})$，第二次傳輸時 $K'_{si} = h(K_{si}, a_i)$，第三次傳輸時 $K''_{si} = h(K'_{si}, K_{si})$，依此類推，讓攻擊者如果想從金鑰鏈中去猜中金鑰的重覆使用頻率的機率降低，也提高此網路的安全性；其次叢聚節點在傳輸完成訊息時，也使用類似的動態金鑰產生，將預先配置的 K_{msg} 和 $Seed$ 進行運算，$K'_{msg} = h(K_{msg}, Seed)$，$K'_{msg}$ 爲訊息金鑰，第二回合時訊息金鑰會進行變更 $K''_{msg} = h(K'_{msg}, K_{msg})$，依此類推，使得攻擊者無法假冒叢聚節點發送完成訊息金鑰，進行金鑰變更。
2. 預防惡意猜測攻擊：當所部署的感測網路存在一段時間後，便進行金鑰的變更和基地台資料庫的更新，使得攻擊者無法得知金鑰，同時每個節點至多只有記錄三把金鑰，二把舊金鑰、一把新產生的金鑰，當產生出新的金鑰時，便會將最舊的一把金鑰進行更新，進而提高網路的安全性且又可減少節點記憶體的空間。
3. 預防重送攻擊：在各個溝通環節中，感測節點到叢聚節點或是叢聚節點到基地站，都採用了記載時戳 T_i 的方法，算出所需的參數值，透過此參數值來預防重送攻擊的發生。例如：叢聚節點到基地台間，叢聚節點使用 K_{ci}

將 T_2 進行加密，並透過時戳 T_i 的比較，$T_3-T_2\leq\Delta T$，如節點在傳送資料時，不能在限定時間ΔT裏完成傳送，則所傳的資料將會被丟棄，所以傳送者必需要在限定時間ΔT裏傳送完畢，否則即被視爲非法的傳送者。

4. 預防資料竄改攻擊：叢聚節點和感測節點間，我們採用了 K_{si} 金鑰來加密，當感測節點回傳資料到叢聚節點聚集時，使用 $E(M, K'_{msg}), K_{si})$ 加密，等到叢聚節點和基地台溝通完成後得到 K_{list}，基地台回傳給叢聚節點的 K_{si} 便可進行解密的動作，如果所獲得的金鑰解不開感測節點所傳過來的加密封包，則視此封包爲危險封包便將此封包丟棄，這樣的作法，可確保傳送資料的完整性，也可確保資料是由叢聚節點管理的感測節點所發出的。
5. 預防中間人攻擊法和確保資料隱密：我們在感測節點和叢聚節點的溝通時，採用加密系統，$C_{si}=\{E((M, K'_{msg}), K_{si}), ID_{si})\}$，來防止攻擊和確保資料隱密，叢聚節點和基地台也使用相似的方法， 來預防攻擊和確保資料隱密，如：$C_{si}=\{E((ID_{list}, T_1), K_{ci}), ID_{ci})\}$，$C_b=E(K_{list}, K_{ci})$，$C'_{ci}=\{E((M_\beta, T_5), K_{ci}), ID_{ci})\}$，因此惡意的攻擊者無法獲得被保護的資料；其次，叢聚節點在傳送完成訊息時使用 K_{msg} 加密，且每一回合都會更新訊息金鑰，使得攻擊者無法假冒叢聚節點發送完成訊息，避免中間人攻擊。

（二）效能分析

表 1 爲本協定之效能分析表，記載感測節點、叢聚節點和基地台，各個回合數和運算式，其中：TE：使用對稱式加密演算法之時間複雜度。TM：傳送訊息所需之時間複雜度。

四、結論

在這本文中，我們提出了動態產生金鑰的架構，不再使用之前所使用的方法，從金鑰池中選取出 m 把金鑰，再形成金鑰鏈的諸多缺點，透過產生動態金鑰的管理方式，我們所提出的架構有以下的貢獻：

1. 因爲無線感測網路的一些限制，例：電源、記憶體等，我們使用資料的批次溝通，來降低感測節點的耗電力，且我們的方法在使用時，每個感測節點，最多只需要記錄三把金鑰，不需記錄整個金鑰鏈，此方法可有效的節省感知節點的記憶空間。
2. 在每一次的傳輸中，所使用的金鑰都是只適用於此次的傳輸，下次要在傳輸時，所使用的金鑰又有所不同，這樣的方法可降低攻擊者去猜測出金鑰，進而提高它的安全性。
3. 在傳輸方面，我們在每個傳輸的過程中，都使用到記錄時間戳記，透過接收端和傳送端兩方的計算，可確保預防重送攻擊的發生。

在無線感測網路的應用方面，我們提出的架構，可被應用在戰場上，監測一個區域裏，敵軍的戰情配備，透過我們協定裏，叢聚節點會先將感測節點所回傳的值進行統計運算，再傳送到後端基地台，可確保後端的基地台所接收的資料更爲準確，也可應用在天氣感測方面，經過叢聚節點的運算，使得感測出的溫度和溼度等，能夠更爲準確。

表 1. 效能分析

節點間傳送關係	回合數	時間複雜度
感測節點和叢聚節點間	2	$2T_E+1T_M$
叢聚節點和基地台間	3	$3T_E+2T_M$

參考資料

1. Atmel company website (2007) AVR 8-Bit RISC processor. Retrieved November 5, 2007, from: http://www.atmel.com/dyn/products/param_table.asp?family_d=607&OrderBy=part_no&Direction=ASC.
2. Chan, H., A. Perrig, and D. Song (2003) Random key predistribution schemes for sensor networks. IEEE Symposium on Security and Privacy, Carnegie Mellon University, Pittsburgh, PA.
3. Cheng, Y. and D. P. Agrawal (2007) An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. *ACM Security Issues in Sensor and Ad Hoc Networks*, 5, 35-48.
4. Diffie, W. and M. E. Hellman (1976) New directions in cryptography. *IEEE Transactions on Information Theory*, 22, 644-654.
5. Eschenauer, L. and V. D. Gligor (2002) A key-management scheme for distributed sensor networks. ACM Conference on Computer and Communication Security, Washington, DC.
6. Ganesan, P., R.Venugopalan, P. Peddabachagari, A. Dean, F. Mueller and M. Sichitiu (2003) Analyzing and modeling encryption overhead for sensor network nodes. ACM International Conference on Wireless Sensor Networks and Applications, San Diego, CA.

7. Intel company website (2007) Retrieved November 5, 2007, from: http://www.intel.com/design/pca/applications processors/1110_brf.htm.
8. Liu, D. and P. Ning (2005) Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(1), 41-77.
9. Pietro, R., L. Mancini and A. Mei (2003) Random key-assignment for secure wireless sensor networks. ACM Workshop on Security of Ad Hoc and Sensor Networks, Fairfax, VA.
10. Rivest, R. L., A. Shamir and L. Adleman (1978) A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 120-126.

收件：96.09.21　修正：96.11.05　接受：97.01.08