行政院國家科學委員會專題研究計畫成果報告

感測器網路容錯路由及安全協定之研發

Design of Fault-Tolerant Routing and Security Protocols in Sensor Networks

計畫編號：NSC 93-2213-E-032-032
執行期限：93 年 8 月 1 日至 94 年 7 月 31 日

主持人：莊博任　淡江大學電機系
計畫參與人員：趙惇豪、李柏逸、邱育賢、
林志信、謝繼華、林鈞傑
淡江大學電機系

一、中文摘要

近年來，無線網路技術的研發進展極為迅速，相關應用日益普遍，感測器網路便是其中之一。有鑒於感測器網路在未來的應用發展，前景熱絡可期，本計畫運用以往的研究成果及心得，從兩個方向探索，為增進感測器網路的效能而努力。我們的研究目標包括：一、設計一個可以容錯並且突破現有效率的感測器網路路由協定，以提升網路之資料匯集速度：我們構想在設計感測器網路路由協定之際，帶入超立方體拓樸之特性，利用一定之演算步驟，先行確認感測器節點如何依距離構成超立方體拓樸，然後經由類似超立方體傳輸樹進行資料匯集，並在感測器節點發生故障或死亡時，藉由容錯傳輸樹或不完全超立方體的方式，加速達成資料匯集的目的。二、為強化感測器網路的資訊安全，深入研究感測器網路之認證與加密兩項議題，參考文獻上既有之無線網路認證協定與加密協定，經適當調整改進，設計出一套便利可行且適用於具耗電低、便宜特性之感測器網路的安全協定，以維護感測器網路中資料傳輸的安全。

針對第一個目標，基於超立方體之資料匯集方法已建制完成，從模擬結果中可以看出我們的新方法在不同的方面都各有所長，像是利用基地台的強大運算力幫我們算出合適有效率的拓撲或是分散式的建出省能源且延遲短的拓撲。藉由我們所提出之機制，無線感測器網路的資料匯集機制考量層面將從單純的節省能源到高即時性及具分散性，未來其應用層面也可以更多樣化、更強健，更合乎無線感測器網路此種特殊網路所需。針對第二個目標，我們認為金鑰分發是影響訊息加密與認證等安全機制能否正常運作的基本前提，本計畫因此提出一個具有可擴充性、群組式之隨機金鑰先發機制，它將所有節點分為多個群組並利用單向函數來產生群組對群組的金鑰，以提高金鑰之連結性與最大支援節點數。在效能評估上，我們分析出在目前所有基於隨機先發的金鑰機制中，本機制能夠提供最大支援的節點數，而在安全性方面，模擬結果也顯示此機制對於入侵節點之攻擊具有良好的抵禦能力。

關鍵詞：無線感測器網路、資料匯集、容錯路由協定、安全協定、超立方體拓樸、認證與加密、金鑰分發、複雜度與效能評估。

Abstract

One of the most popular research topics in today's technological fields is the development and application of the wireless network. Among the various applications of the wireless network, the sensor network has been drawing increasing research attention in recent years due to its wide scope of usage. In this research, we aim to enhance the overall performance of the sensor network by improving its data transmission speed and tightening its transmission security. To speed up data transmission, we plan to develop a

new routing protocol using the hypercube topology under which data will be collected from nodes to the sink through tree communication, and when faulty nodes exist, fault-tolerant communication trees or incomplete hypercubes can be brought in to facilitate data gathering. To tackle the security problem of the sensor network based on current authentication and encryption findings for wireless networks, we will engage in the construction of specific authentication and encryption designs for the sensor network to ensure further transmission security for the network.

The proposed hypercube-based data gathering scheme gathers data from all nodes to the base station through the communication tree in the constructed hypercube. It is able to shorten communication delay by parallel transmissions and to replace dead nodes through reconfiguration. Simulation results show that compared with other data gathering schemes, the proposed hypercube-based scheme brings up favorable results, including reduced transmission delay, balanced energy loads, satisfying system scalability and as a result prolonged system lifetime. As to the security problem of the sensor network, we have observed that key management, a basic security service, is the core design for various security services like encryption and authentication. This research thus presents a Scalable Grouping (SG) random key predistribution scheme which divides all nodes into several groups and uses the one-way function to generate group-to-group pairwise keys to increase the connectivity of each key and to enlarge the maximum supportable network size. Experimental results show that the SG scheme is able to yield more enhanced resilience against node capture in large-scale networks, generate higher scalability than existing random key based schemes, and limit global payoff from local compromised nodes.

Keywords: Wireless sensor networks, data gathering, fault-tolerant routing protocols, security protocols, hypercube topology, authentication and encryption, key distribution, complexity and performance evaluation.

二、計劃緣由與目的

近年來，無線網路技術的研發進展極為迅速，相關應用日益普遍，感測器網路便是其中之一。感測器網路環境的形成，乃是以大量的感測器節點(sensor nodes)佈建在一待感測區域(sensor field)中[1]，各個節點相互通訊的主要目的，是為了將感測到的資料傳遞到資料匯集點(sink — 通常為基地台 base station)，而後將這些資料做處理，使其成為有用的資訊。感測器網路以感測為主要目標，其基本組成單元包括電源、發射/接收單元、感測單元(感測及類比轉數位單元)、運算單元(運算及記憶體單元) 、定位和移動等選項功能。感測器網路通訊協定分為實體層(physical layer)、鏈結層(data link layer)、網路層(network layer)、傳輸層(transport layer)和應用層(application layer) 。其主要管理方式對應所需之工作項目，可分為工作管理(task management) 、移動管理(mobility management) 、電源管理(power management)等三大部分，三者之間且相互影響。有別於無基礎架構式網路(ad hoc network)，感測器之節點具有多功能、低製造成本、低電能、體積小、傳輸距離短及易於失效故障等特性，在電能、計算能量、記憶體部份皆有所限制。

有鑒於感測器網路在未來的應用發展，前景熱絡可期，本計畫運用以往的研究成果及心得，從兩個方向探索，為增進感測器網路的效能而努力。我们的研究目標包括：一、設計一個可以容錯並且突破現有效率的感測器網路路由協定，以提升網路之資料匯集速度；二、針對感測器網路之認證及加密進行探討，發展一套簡便合用的安全協定，以維護感測器網路中資料傳輸的安全。關於感測器網路路由及安全協定之研發，文獻上各種相關協定雖然不斷推陳出新（如[2-6]），此一議題實際上仍存在相當大的改進空間。有鑑於此，我們希望能在多方參考既有的協定後，根據其特性及優缺點，截長補短，尋找改進的方向並提出新的協定，以低成本且安全

的方式，有效達成感測器網路節點資料匯集及傳輸安全的目的。換言之，我們希望透過此一計畫的執行，分別設計出新的感測器網路容錯路由及安全協定，使其效能得以超越現今既有之協定，裨益實際之應用及後續之研究。

三、結果與討論

假設 C_i 是 i-cube 的集合，E_i 則是兩個 i-cube 間之連線的集合，以下為將整個無線感測器網路建立成一個超立方體的演算法[7]，在一開始時所有的超立方體節點被放在 C_0：

START
i = 0
while (the number of cubes in C_i is greater than 1)
{
  for each pair of cubes in C_i select the connection with the minimum weight (i.e., sum of squares) and put the selected connection into E_i.
  while (C_i is not empty)
  {
    if (there is only one cube in C_i)
      increase the dimension number of the cube's links and let the dimension 0 neighbor of each node in the cube to be itself
      remove it from C_i add it to C_{i+1}
    if (a cube has no related connections in E_i)
      re-compute connection between it and each cube in C_i and put all such connections into E_i
    while (a cube c in C_i has only one related connection in E_i with another cube c' in C_i)
      connect c and c' to form an (i+1)-cube by the related connection
      delete all the other related connections of c'
      remove c and c' from C_i and add the formed (i+1)-cube to C_{i+1}
    delete the connection with the maximum weight in E_i
  }
  i ++
}
END

在超立方體建立完成後，我們會利用此超立方體中的 communication tree [8] 來完成 data gathering。

為了提升網路最大支援節點數，並且對於入侵節點之攻擊也能提供良好的抵禦能力，我們提出了一個具有可擴充性、群組式之隨機金鑰先發機制（Scalable Grouping random key predistribution scheme，簡稱為 SG scheme）[9]。

SG scheme 的特點如下：

1. 每個節點均有一個群組識別證（group ID）。
2. 每個群組至多有 k 個節點。同群組的節點存有共享的一把群組金鑰（group key）與一個群組單向函數（group one-way function）。
3. 不同群組的節點利用群組單向函數產生 group-to-group pairwise key，並以此金鑰建立安全連線。
4. 當兩節點擁有兩把以上的共享金鑰時，即使用 XOR 運算將所有共享金鑰合成一把連線金鑰。

k-SG scheme（k 為群組的大小）其運作流程共有三個階段，分別為 Initialization、Link key setup 與 Secure link establishment，分述如下：

1. Initialization phase：在網路部署前，我們先將所有節點隨機分為多個群組，每個群組至多有 k 個節點，其中同群組的節點均共享一個群組識別證 GID_i、一把群組金鑰 K_i、與一個群組單向函數 F_i。接著每個節點隨機選擇 r 個群組，未來此節點可與這 r 個群組的節點建立連線，並藉由 $K_{ji} = F_j (GID_i)$計算出 r 把金鑰，每個節點儲存 r 對 K_{ji} 與 GID_j。
2. Link key setup phase：當網路部署完成後，每個節點先廣播自己的 GID 給鄰近節點。當一節點 A 收到了節點 B 所廣播的 GID_j 時，先檢查兩節點是否屬於同個群組：如果是即回傳一個同群組的訊息以及自己的 key ring 列表；如果不是則節點 A 即回傳 GID_i。接著雙方節點即開始

執行 link key setup algorithm，此演算法的運作流程如下：

if（節點 A 與節點 B 屬於同群組）{
  if（有共享的金鑰）
    連線金鑰 K_s 即為群組金鑰⊕共享金鑰
  else
    K_s 為群組金鑰
}
else {
  switch {
    case1（節點 A 存有 K_{ji} 且節點 B 存有 K_{ij}）：
      節點 A 計算 $K_{ij} = F_i(GID_j)$
      節點 B 計算 $K_{ji} = F_j(GID_i)$
      K_s 為 $K_{ij}⊕K_{ji}$
      break
    case2（節點 A 存有 K_{ji} 但節點 B 並未存有 K_{ij}）：
      節點 B 計算 $K_{ji} = F_j(GID_i)$
      K_s 為 K_{ji}
      break
    case3（節點 B 存有 K_{ij} 但節點 A 並未存有 K_{ji}）：
      節點 A 計算 $K_{ij} = F_i(GID_j)$
      K_s 為 K_{ij}
      break
    case4（節點 A 並未存有 K_{ji} 且節點 B 並未存有 K_{ij}）：
      此兩節點無法建立連線金鑰 K_s
      break
    }
  }

3. Secure link establishment phase：在執行完 link key setup algorithm 後，如果兩節點可建立一連線金鑰 K_s，則它們可利用一簡單的 challenge response 機制來驗證此連線金鑰。一旦驗證通過，此兩節點即建立了一條使用此金鑰傳遞訊息的安全連線。

四、計畫成果自評

我們使用 NS-2 來進行模擬。在模擬環境中，我們的無線感測網路有 100 個感測器，隨機散布在 100*100 公尺的平面之中，且每個感測器的初始能源均為 0.25J，基地台在距此網路之中心位置 200 公尺遠的地方。在每個資料匯集回合中，每個存活的感測器都有一個 2000 位元的封包要傳至基地台。模擬結果顯示，與其他既有方法（如 LEACH[2]與 PEGASIS[3]）相較，我們以超立方體為基礎之資料匯集方法，在降低傳輸延遲、平衡能源負載、滿足系統擴充方面，都有超越之表現，也因而能延長系統之壽命。

至於評估我們的隨機金鑰先發機制上，我們針對以下三個方面來驗證既有機制與我們提出的 SG scheme：

1. 安全性：這裡我們評估的是對節點入侵攻擊的抗性，也就是模擬在各個機制下，攻擊者利用已取得的金鑰能入侵多少比例的其他安全連線。
2. 網路最大支援節點數：在有限的記憶體下，各機制最多能支援的節點數目。
3. Limited global payoff requirement：評估 SG scheme 是否能符合 Limited global payoff requirement。

在效能評估方面，我們分析出在目前所有的隨機金鑰先發機制中，我們的機制所能支援的節點數是最多的，而且還可藉由調整群組大小來支援更多的節點。在安全性方面，模擬結果顯示我們的機制對於入侵節點之攻擊有著良好的抵禦能力，而在網路節點數增加時，其間接入侵連線數之比例也會隨之下降，這就是使用 pairwise key 所帶來的優勢。另外在 Limited global payoff requirement 的評估上，我們的機制也能有效避免攻擊者以極少的投資獲得大量的報酬。

本研究計畫所預計達成的目標皆如期圓滿達成，其所設計出之「SG Scheme」已為國際研討會接受並發表[9]，「超立方體為基礎之資料匯集方法」亦被國際研討會接受，即將與會發表[7]。我們並已擬定在相關領域更深入研究的方向與大綱，期望在既有基礎上，繼續努力耕耘，尋求進一步的突破。

五、參考文獻

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, Aug. 2002.

[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *Proc. 33rd Hawaii Int'l Conf. on System Sciences*, Jan. 2000.

[3] S. Lindsey, C. Raghavendra, and K. M. Sivalingam, "Data Gathering Algorithms in Sensor Networks Using Energy Metrics," *IEEE Trans. on Parallel and Distributed Systems*, Vol. 13, No. 9, pp. 924-935, Sept. 2002.

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

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

[6] S. Y. Wu and S. P. Shieh, "Adaptive Random Key Distribution Schemes for Wireless Sensor Networks," *Proc. 2003 Int'l Workshop on Advanced Developments in Software and Systems Security*, Dec. 2003.

[7] P.-J. Chuang, B.-Y. Li, and T.-H. Chao, "Efficient Data Gathering Schemes for Wireless Sensor Networks," to appear in *Proc. 2005 Int'l Conf. on Mobile Ad-hoc and Sensor Networks*, Dec. 2005.

[8] P.-J. Chuang, S.-Y. Chen, and J.-T. Chen, "Constructing Fault-Tolerant Communication Trees in Hypercubes," *Journal of Information Science and Engineering*, Vol. 20, No. 1, pp. 39-55, Jan. 2004.

[9] P.-J. Chuang, T.-H. Chao, and B.-Y. Li, "A Scalable Grouping Random Key Predistribution Scheme for Large Scale Distributed Sensor Networks," *Proc. 3rd Int'l Conf. on Information Technology and Applications*, July 2005, pp. 535-540.