行政院國家科學委員會專題研究計畫 成果報告

無線感測網路之關鍵技術及在社區照護之應用--子計畫五：無線感測網路下位置知覺醫療照護服務之安全性架構(3/3)

研究成果報告(完整版)

計 畫 類 別 ： 整合型
計 畫 編 號 ： NSC 95-2221-E-002-062-
執 行 期 間 ： 95 年 08 月 01 日至 96 年 07 月 31 日
執 行 單 位 ： 國立臺灣大學電機工程學系暨研究所

計 畫 主 持 人 ： 雷欽隆

計畫參與人員： 博士班研究生-兼任助理：黃俊穎、邱建樺、李俊頡
碩士班研究生-兼任助理：李立源、吳辰杞

處 理 方 式 ： 本計畫可公開查詢

中 華 民 國 96 年 11 月 02 日

行政院國家科學委員會專題研究計劃成果報告

無線感測網路下位置知覺醫療照護服務之安全性架構

A Security Framework for Location-Aware Healthcare Services over Wireless Sensor Networks

計劃編號：NSC NSC 95-2221-E-002-062
執行期限：93 年 8 月 1 日至 96 年 7 月 31 日
主持人：雷欽隆　台大電機系教授

一、中文摘要

在本計畫中，我們將針對無線感測網路下位置知覺醫療照護服務之安全性架構必須具有的關鍵性要求進行深入剖析，並根據分析的結果設計一套可以實際運作的安全性架構。這套安全性架構至少必須達成以下的目標：（一）提高整體系統的可用性(Availability)；（二）保障被照護者的個人隱私；（三）提供具時效性的資訊傳遞方式；（四）避免惡意攻擊造成的醫療資源損耗。除了上述的主要目標之外，由於無線感測網路與位置知覺醫療照護服務擁有與傳統網路應用程式迥異的限制與特性，我們也深深地感覺到發展一個新型態安全性評估模型的需要。在這個安全性評估模型當中，必須先對無線感測網路下位置知覺醫療照護服務所可能面對的攻擊行為做適當的分類，從中找出一般系統內潛在的弱點，再進一步驗證所提出的安全性架構是否可以成功地阻擋住這些攻擊行為。舉例來說，可攜式發送裝置會隨著被照護者的移動而發生實體位置的改變，而當被照護者跨越不同感測器的監測區域時，則會發生交接 (Handoff) 的動作；如何在時常發生交接的情況下保持身份認證的連續性（此時也必須兼顧保持低度能源消耗的目標），避免惡意攻擊者利用交接的動作而冒用被照護者的身份，即是一個必須額外考量的重點。藉由安全性評估模型的提出，我們將可以建立現在與未來安全性架構的衡量標準，為無線感測網路下位置知覺醫療照護服務的實際建置提供穩固的基礎。

在計畫的第一年度我們設計了一個植基於中國餘數定理的高效能無線感測網路金鑰管理機制。在計畫的第二年度我們設計了兩個植基於二次剩餘的高效能隱私保護協定。我們提出利用二次剩餘的新認證協定，不但能保護使用者的隱私，而且使協定具擴充性，使整個系統有效率地運作。在計畫的第三年度我們探討感測網路的安全資料彙集機制，並歸納出安全資料彙集的共通模型及發展趨勢。由於感測網路/RFID的應用廣泛，各種應用的應用環境不同，所以一個協定通常無法同時滿足所有應用在安全性、效能和成本三方面的求，因此我們以應用以安全需求度作區分，分別對一般安全需求的應用和安全需求較高的應用設計認證協定，在達到各自的安全性目標下，將效能提高和將成本降低，使我們所提出的協定真正地適合實作的環境。

關鍵詞：網路安全、無線感測網路、位置知覺運算、隱私保護協定、醫療照護服務、安全性評估

Abstract

In this project, we are going to investigate the key requirements of a security framework for location-aware healthcare services over sensor networks, and attempt to formulate a complete and practical design based on the results of the investigation. To the least extent, the resulting framework is supposed to improve the availability of the system, to preserve the privacy of the subjects being cared, to assert timely response, and to prevent the abuse of medical resources. In addition, because of the stringent constraints and certain application-specific considerations incurred by the particular combination of wireless sensor networks and healthcare services, it is required to explore new evaluation models for the security analysis in this unique situation. For example, the cross-location continuity of authenticity, or the consistency of sensed information emitted by an authenticated moving subject, ought to be taken into account as well. As a result, we also plan to propose unconventional evaluation models tailored for both location-aware healthcare services and wireless sensor networks.

In the first year of the project, we develop an efficient key management mechanism for sensor networks based Chinese Remainder Theorem (CRT). In the second year of the project, we develop two privacy protection schemes based on quadratic residues. In the third year of the project, we develop a secure data aggregation scheme EVIA for sensor networks. Compared with existing schemes, our scheme are not only more secure but also more scalable. It turns out that our schemes are suitable for practical implementation.

Keywords: Security, wireless sensor networks, location-aware computing, location privacy, privacy protection, healthcare service, security evaluation model

二、緣由與目的

隨著全球人口老化現象成為社會學家及公共衛生學者所關注的重大議題之一，醫療照護服務也逐漸地在其他專業領域引發相關的技術研究。在醫療照護服務的範疇之內，如何善用資源而適當地掌握被照護者的生理資訊及所在位置，以便於在緊急情況提供及時的救護與協助，無疑地是一項受到高度關切的重要課題。而無線感測網路技術發展至今，因為具有反應迅速、建置容易及成本低廉等特性，十分適合應用在上述的位置知覺醫療照護服務。另一方面，雖然無線感測網路技術具有減少人力使用與即時偵知危急狀況的潛在優勢，如果缺乏一個完善的安全性架構，終究也無法得到一般民眾的信任，更遑論在醫療照護服務方面得到發揮的機會。然而，在無線感測網路的環境之下是一項充滿挑戰的艱鉅任務。為了讓被照護者攜帶方便，蒐集與發送生理及位置資訊的設備必須是一個微型裝置，因此有運算能力及儲存空間的限制；為了讓這種類型的可攜式發送裝置能夠長時間運作，能源消耗的問題也必須加以考慮。除此之外，在無線感測網路的工作模式下，受限於傳輸能力的限制，發送裝置與感測器之間的距離不能夠過於遙遠，而且網路的拓樸也會隨著被照護者的移動而持續地改變；這些因素都使得應用於傳統網路服務上的安全性架構與網路安全通訊協定變得無用武之地，進而產生研發新一代安全性架構的迫切需要。

在本計畫中，我們將針對無線感測網路下位置知覺醫療照護服務之安全性架構必須具有的關鍵性要求進行深入剖析，並根據分析的結果設計一套可以實際運作的安全性架構。

三、結果與討論

在計畫的第一年度我們設計了一個植基於中國餘數定理的高效能無線感測網路金鑰管理機制。與文獻上其他機制相比，我們所設計的機制具有下列優點:

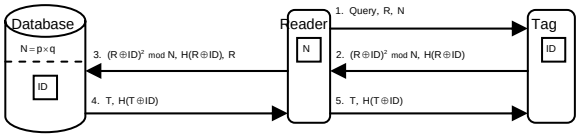
(1)當系統中有節點被破解時，金鑰伺服器可以廣播一個不需加密的更新

信息給所有的節點。而每一個合法節點都可利用此更新信息以一個簡單的模運算來導出一個更新seed並更新群體金鑰。

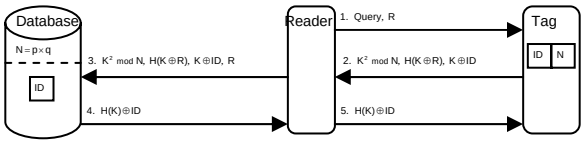
(2)與文獻上其他機制不同，我們所設計的金鑰管理機制可更改key spaces，此優點可加長金鑰之有效期且使得心結點的加入更為容易。

我們所設計的金鑰管理機制在rekeying時空間使用很有效率，一個節點僅需$O(\lambda)$的空間，其中λ是一個預定的安全參數，在$\lambda+1$個節點被破解前 key space 是安全的。

在計畫的第二年度我們設計了兩個植基於二次剩餘的高效能隱私保護協定。我們提出利用二次剩餘的新認證協定，不但能保護使用者的隱私，而且使協定具擴充性，使整個系統有效率地運作。由於感測網路/RFID的應用廣泛，各種應用的應用環境不同，所以一個協定通常無法同時滿足所有應用在安全性、效能和成本三方面的求，因此我們以應用以安全需求度作區分，分別對一般安全需求的應用和安全需求較高的應用設計認證協定，在達到各自的安全性目標下，將效能提高©降低，使我們所提出的協定真正地適合商業的實作環境。



圖一 可抵擋被動式攻擊之隱私保護協定



圖二 可抵擋主動式攻擊之隱私保護協定

在計畫的第三年度我們探討感測網路的安全資料彙集機制，並歸納出安全資料彙集的共通模型及發展趨勢。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。如同來Proof sketches、CPS等，我們提出更全面的方案EVIA。

我們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。

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

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)：

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

而彙集者j所需進行的動作：

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

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。

四、計劃成果自評

在計畫的第一年度我們設計了一個植基於中國餘數定理的高效能無線感測網路金鑰管理機制。與文獻上其他機制相比，我們所設計的機制具有效能空間以及方便等優點，我們我們所設計的機制已經整理發表論文，這些結果不但有學術參考價值且有助於後續無線感測網路安全之研發。

在計畫的第二年度我們設計了兩個植基於二次剩餘的高效能隱私保護協定。我們提出利用二次剩餘的新認證協定，不但能保護使用者的隱私，而且使協定具擴充性，使整個系統有效率地運作。與文獻上其他機制相比，我們所設計的機制具有效能空間以及方便等優點，詳見表一~三之比較。我們所設計的機制已經整理發表文，這些結果不但有學術參考價值且有助於後續無線感測網路安全之研發。

表一. 安全性比較

	Spoofing	Replay	Traffic analysis	Weak anonymity	Strong anonymity	DB sync
Hash-lock	×	×	×	×	×	Not needed
Randomized hash-lock	×	×	×	×	×	Not needed
Hash-chain	×	×	○	○	○	Not needed
Hash-based ID variation	×	○	○	○	×	Needed
Rhee *et al.*'s protocol	○	○	○	○	○	Not needed
Protocol 1	×	×	×	○	×	Not needed
Protocol 2	○	○	○	○	○	Not needed

註： ○代表能避免攻擊，×代表不能避免攻擊。

表二. 儲存空間比較

	Memory (bits)		
	Tag	Reader	Back-end database
Hash-lock	2L	-	3L
Randomized hash-lock	1L	-	1L
Hash-chain	1L	-	2L
Hash-based ID variation	3L	-	8L
Rhee *et al.*'s protocol	1L	-	1L
Protocol 1	1L	1L	1L
Protocol 2	2L	-	1L

表三. 效能比較

	Computation (times)			Suitability to distributed database environment
	Tag	Reader	Back-end database	
Hash-lock	H: 1	-	-	○
Randomized hash-lock	R: 1, H: 1	H: $\frac{\text{The number of IDs}}{2}$	-	○
Hash-chain	H: 2	-	H: $\frac{\text{The number of IDs}}{2}\times i$	○
Hash-based ID variation	H: 3	-	R: 1, H: 3	×
Rhee *et al.*'s protocol	R: 1, H: 2	R: 1	H: $\frac{\text{The number of IDs}}{2}+1$	○
Protocol 1	H: 2, M: 2, X: 3	R: 1	SR: 1, H: 5, R: 1, X: 2	○
Protocol 2	R: 1, H: 2, M: 2, X: 3	R: 1	SR: 1, H: 5, X: 6	○

在計畫的第三年度我們探討感測網路的安全資料彙集機制，並提出更全面的方案 EVIA。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。

五、參考文獻

1. I. F. Akyildiz, E. Cayirci, W. Su, and Y. Sankarasubramaniam, “A Survey on Sensor Networks,” IEEE Comm., Vol. 40, No. 8, pp. 102-114, August 2002.
2. M. Bohge and W. Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,” Proceedings of 2003 ACM Workshop on Wireless Security, pp. 79-87, September 2003.
3. 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.
4. 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.
5. C. Castelluccia, E. Mykletun, and G. Tsudik. “Efficient aggregation of encrypted data in wireless sensor networks.” In *MobiQuitous*, pages 109–117, 2005.
6. 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.
7. H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” IEEE Computer, Vol. 36, No. 10, pp. 103-105, October 2003.
8. H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 2003, pp. 197-213.
9. H. Chan and A. Perrig, “PIKE: Peer Intermediaries for Key Establishment in Sensor Networks,” IEEE Infocom 2005, March 2005.
10. H. M. Chao, S. H. Twu, and C. M. Hsu, “A Secure Identification Access Control Scheme for Accessing Healthcare Information Systems,” Proceedings of 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Boimedicine, pp. 122-125, April 2003.
11. G. H. Chiou and W. T. Chen, “Secure Broadcasting Using the Secure Lock,” IEEE Transactions on Software Engineering, 15(8), August 1989, pp. 929-934.
12. 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
13. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A Pairwise Key Pre-distribution Scheme for Wireless Sensor Network,” Proceedings of the 10th ACM conference on Computer and communication security, October 2003, pp. 42-51.
14. W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,” IEEE Infocom 2004, March 2004, pp. 586-597.
15. L. Eschenauer and V. D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proceedings of the 9th ACM Conference on Computer and Communications Security, November 2002, pp. 41-47.
16. P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, “Analyzing and Modeling Encryption Overhead for Sensor Network Nodes,” Proceedings of 2nd ACM International Conference on Wireless Sensor Networks and Applications, pp. 151-159, September 2003.
17. M. Garofalakis, J. M. Hellerstein and P. Maniatis. “Proof Sketches: verifiable in-network aggregation.” In *ICDE*, 2007.
18. D. Henrici and P. Muller, “Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers,” The Second IEEE Annual Conference of Pervasive

Computing and Communications Workshops, 2004.
19. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” Proceedings of 2003 ACM Workshop on Wireless Security, pp. 30-40, September 2003.
20. L. Hu and D. Evans. “Secure aggregation for wireless network. In SAINT Workshops, pages 384–394, 2003.
21. Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, “Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks,” Proceedings of 2nd ACM International Conference on Wireless Sensor Networks and Applications, pp. 141-150, September 2003.
22. R. Huebsch, M. Garofalakis, J. M. Hellerstein, I. Stoica. “Sharing aggregate computation for distributed queries.” In *SIGMOD* 2007.
23. P. Jadia and A. Mathuria. “Efficient secure aggregation in sensor networks.” In *HiPC*, pages 40–49, 2004.
24. M. Jakobsson, K. Sako, and R. Impagliazzo. “Designated verifier proofs and their applications.” In *Advances in Cryptology – EUROCRYPT*, pages 143–154, 1996.
25. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003.
26. J. Lee and D. R. Stinson, “Deterministic key Predistribution Schemes for Distributed Sensor Networks,” Selected Areas in Cryptography, August 2004, pp. 294-307.
27. D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks,” Proceedings of the 10th ACM Conference on Computer and Communication Security, October 2003, pp. 52-61.
28. A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham. “Sequential aggregate signatures from trapdoor permutations.” In *Advances in Cryptology – EUROCRYPT*, pages 74–90, 2004.
29. R. C. Merkle, “A certified digital signature”, In *Advances in Cryptology – CRYPTO* 1989.
30. S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong. “Tag: A tiny aggregation service for ad-hoc sensor networks.” In *OSDI*, 2002.
31. 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.
32. E. Mykletun, J. Girao, and D. Westhoff. “Public key based cryptoschemes for data concealment in wireless sensor networks.” In *ICC* 2006.
33. M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic approach to privacy-friendly tags,” RFID Privacy Workshop, 2003.
34. 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.
35. B. Przydatek, D. X. Song, and A. Perrig. “SIA: secure information aggregation in sensor networks.” In *SenSys*, pages 255–265, 2003.
36. K. Rhee, J. Kwak, S. Kim, and D. Won, “Challenge-Response Based RFID Authentication Protocol,” International Conference on Security in Pervasive Computing (SPC 2005), 2005.
37. N. Sastry, U. Shankar, and D. Wagner, “Secure Verification of Location Claims,” Proceedings of 2003 ACM Workshop on Wireless Security, pp. 1-10, September 2003.
38. B. Schilit, J. Hong, and M. Gruteser, “Wireless Location Privacy Protection,” IEEE Computer, Vol. 36, No. 12, pp. 135-137, December 2003.
39. R. Venugopalan, P. Ganesan, P. Peddabachagari, A. Dean, F. Mueller,

and M. Sichitiu, “Encryption Overhead in Embedded Systems and Sensor Network Nodes: Modeling and Analysis,” Proceedings of International Conference on Compilers, Architectures and Synthesis for Embedded Systems, pp. 188-197, October 2003.

40. D. Wagner. “Resilient aggregation in sensor networks.” In *Proceedings of the 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks*. 2004.
41. S. Weis, S. Sarma, R. Rivest, and D. Engels, ”Security and Privacy Aspects of Low-Cost Radio Frequency Identification,” Security in Pervasive Computing 2003, 2003.
42. 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.
43. S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” Proceedings of the 10th ACM Conference on Computer and Communication Security, October 2003, pp. 62-72.
44. S. Zhu, S. Setia, S. Xu, and S. Jajodia, “GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks,” Proceedings of the 1st ACM International Conference on Mobile and Ubiquitous Systems, August 2004, pp. 42-51.