行政院國家科學委員會專題研究計畫　期中進度報告

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(1/3)

計畫類別：整合型計畫
計畫編號：NSC93-2213-E-002-124-
執行期間：93 年 08 月 01 日至 94 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：李俊頡　廖燕華　陳煜弦　張棋嵐　紀博文

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 94 年 6 月 1 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 93-2213-E-002-124
執行期限：93 年 8 月 1 日至 94 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。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。
(3) 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(λ)的空間，其中λ是一個預定的安全參數,在λ+1個節點被破解前key space是安全的。

關鍵詞：網路安全、無線感測網路、位置知覺運算、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 a key management scheme for wireless sensor network based on CRT (Chinese Remainder Theorem). Compared with existing schemes, the proposed scheme has the following advantages. First, when some node is revoked or compromised, the key server can broadcast update messages to all nodes without encryption. Each node can derive an update seed from the message in only one modulation operation and use this seed to update group key and key spaces. Second, compared to existing schemes, in which key spaces cannot be changed, all key spaces can be updated in our scheme. This advantage makes the life time of key spaces longer and node joining become much easier. Moreover, the rekeying cost of this scheme is also efficient in storage since the memory requirement in every node is just $O(\lambda)$, where λ is a security parameter, and each key space is secure before $\lambda+1$ nodes are compromised.

Keywords: Security, wireless sensor networks, location-aware computing, 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。

(3)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(λ)的空間，其中λ是一個預定的安全參數，在λ+1個節點被破解前key space是安全的。

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。

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. 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.
4. H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” IEEE Computer, Vol. 36, No. 10, pp. 103-105, October 2003.
5. 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.
6. H. Chan and A. Perrig, “PIKE: Peer Intermediaries for Key Establishment in Sensor Networks,” IEEE Infocom 2005, March 2005.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. J. Lee and D. R. Stinson, “Deterministic key Predistribution Schemes for Distributed Sensor Networks,” Selected Areas in Cryptography, August 2004, pp. 294-307.
16. 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.
17. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: Security Protocols for Sensor Networks,” Wireless Networks, pp. 521-534, September 2002.
18. 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.
19. B. Schilit, J. Hong, and M. Gruteser, “Wireless Location Privacy Protection,” IEEE Computer, Vol. 36, No. 12, pp. 135-137, December 2003.
20. 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.
21. 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.
22. 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.