無線感測網路輕量加解密技術實作

Implementation of Lightweight Cryptography in Wireless Sensor Networks

陳心懋 何明達 江振瑞
國立中央大學資訊工程學系 國立中央大學資訊工程學系 國立中央大學資訊工程學系
945002018@cc.ncu.edu.tw 945002204@cc.ncu.edu.tw jrjiang@csie.ncu.edu.tw

摘要

隨著微電機系統(micro electro-mechanical system, MEMS)與無線電通訊(wireless communication)技術的進步，無線感測網路(wireless sensor network, WSN)的發展漸漸成熟，而其應用也日益增多。例如，透過無線感測網路建立數位家庭環境，傳遞使用者居家與生理資料是其中一個重要的應用。然而無線感測網路於通訊時，以無線電傳遞的封包資訊很容易遭攻擊者擷取，造成使用者隱私資料的洩漏。因此，如何於無線感測網路使用通訊加密技術為重要之議題。本論文實作 Rabin 非對稱式金鑰加密機制，解決無線網路感測器因計算能力與記憶體空間不足，無法執行高階加密演算法之問題，藉以改善無線感測網路傳輸安全，保障使用者的隱私。

關鍵詞：無線感測網路、非對稱式加解密、通訊安全、使用者隱私、數位家庭

Abstract

The advances on micro electro-mechanical system (MEMS) and wireless communication technologies make prosperous the development of wireless sensor networks (WSNs). There are more and more applications of WSNs, such as digital home environment where users' private daily living and physical data are transmitted to sink node periodically for the purpose of health-caring. The wireless packets sent in WSNs can be eavesdropped easily, harming the network security and user privacy. In this paper, we demonstrate the implementation of Robin asymmetric cryptography on resource-constrained Cricket sensor nodes for the application of digital home environment to achieve communication security and protect user privacy.

Keywords: wireless sensor networks, user privacy, communication security, asymmetric cryptography, digital home

1. 前言

隨著微電機系統(micro electro-mechanical system, MEMS)與無線電通訊(wireless communication)技術的進步，無線感測網路(wireless sensor network, WSN)[2][10]的發展漸漸成熟，而其應用[3][5][7][8][11][13]也日益增多。例如，透過無線感測網路建立數位家庭環境[8]，傳遞使用者居家與生理資料[5][7][11]是其中一個重要的應用。然而無線感測網路於通訊時，以無線電傳遞的封包資訊很容易遭攻擊者擷取，造成使用者隱私資料的洩漏。因此，如何於無線感測網路使用通訊加密技術[15]為重要之議題。

無硬體支援加密功能之感測器成本價格較低廉，任何人皆可輕易擷取其封包傳遞，因此需要以軟體加密方式，保障使用者之隱私資訊。例如，利用無線感測網路建置的數位家庭環境，若未針對無線感測網路封包進行加密，則使用者的家庭生活與生理資訊將被一覽無遺，毫無任何隱私可言。

過去有對稱式與非對稱式[1][4][12][14]加密技術。對稱式技術之加解密鑰匙相同，若鑰匙被竊取則傳輸之資料都會被破解；非對稱式加密則以公鑰加密、私鑰解密，私鑰存放於伺服器端，公鑰存放於感測器。因伺服器較感測器擁有較強的安全防護機制以防止鑰匙被竊取，盜取者較難以獲得破解傳輸加密之私鑰，因此使用非對稱性加密機制在無線感測網路上，更能保障使用者之隱私。

非對稱加密所需計算成本較對稱式加密高，而感測器運算能力與儲存空間較小(如：Cricket[6])，不適合執行大量計算的非對稱式加

密機制(如：RSA[12])，因此本論文採用Rabin非對稱式金鑰加密演算法[9]，實作感測器間之資訊傳輸。Rabin加密機制具有加密運算量小、解密運算量大的特性，適合使用於無線感測網路。本論文於感測器上執行運算量較低之加密動作，於伺服器上運行較複雜之解密動作，藉此解決感測器處理能力受限，加解密不易之問題。提出Rabin非對稱式金鑰加密演算法實作於Cricket感測器時，如何減少加解密時間、使用記憶體空間與確認明文之方法，以提供使用者安全傳輸環境，保障使用者之隱私資訊。

本論文的其他部份內容的安排如下。在第二節中，我們介紹 Rabin 技術的加解密過程。在第三節中，我們說明如何實作 Rabin 技術的加解密計算。在第四節中，我們進行實作效能評估。最後我們在第五節中總結本論文。

2. 系統加解密流程

本論文以數位家庭環境傳遞使用者居家與生理資料之應用為實例，說明如何實作Rabin非對稱式金鑰加密演算法於Cricket感測器，達到輕量加密的目的。其系統架構如圖 1所示，感測器將明文加入確認資料後，使用Rabin加密獲得密文，再將密文分割成數個封包送出，於伺服器端解密。

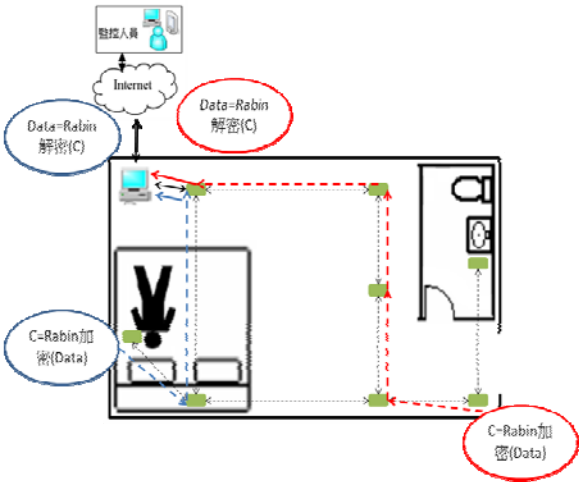

圖 1、系統加解密流程圖

2.1 加密

使用Rabin非對稱式金鑰加密演算法時，隨著明文資料愈長，加密所需之時間愈久，加密方法如公式(1)所示：

$$C = M^2 \% N \qquad (1)$$

其中 C 為密文，M 為明文，N 為公開金鑰，$N = P \times Q$。P、Q 則為私鑰，由兩質數所組成，且 $P \% 4 = 3$、$Q \% 4 = 3$。將明文數值平方，再除以公開金鑰之數值後，可獲得一餘數，此餘數即為加密後所產生之密文。本論文挑選兩大小約 512 位元之私鑰，使產生之公開金鑰約為 1024 位元，較適合感測器之資訊加密。

2.2 解密

當伺服器接收到 Cricket 感測器傳送之完整密文 C 後，可藉由 P、Q 兩私鑰與公開金鑰 N，計算出 $M1 \sim M4$ 四組明文。解密公式如下列所示：

$$\begin{cases} W1 = C^{\frac{P+1}{4}} \% P \\ W2 = P - W1 \\ W3 = C^{\frac{Q+1}{4}} \% Q \\ W4 = Q - W3 \end{cases}$$

$$\begin{cases} a = Q \times \left(Q^{-1} \% P\right) \\ b = P \times \left(P^{-1} \% Q\right) \end{cases}$$

$$\begin{cases} M1 = \left(a \times W1 + b \times W3\right) \% N \\ M2 = \left(a \times W1 + b \times W4\right) \% N \\ M3 = \left(a \times W2 + b \times W3\right) \% N \\ M4 = \left(a \times W2 + b \times W4\right) \% N \end{cases} \qquad (2)$$

2.3 明文驗證

由於Rabin非對稱式金鑰加密演算法，將使一密文解出四組明文，因此，要從中找出正確明文時，可在原明文加上確認資料。本論文使用之方法是從原明文當中，取數個數字當作比對資料，附加在原明文上以形成新明文作加密，如圖 2所示。

同理，密文還原成明文時，即可藉由此比對資料，驗證出正確之明文，如圖 3所示。若原先明文共有m個數字，選取n個數字作比對，則此方法造成一組以上明文驗證結果正確之機率為 $10^{m-n}/10^m$。因此可知選取的確認資料數字愈多，其發生不同明文驗證結果相同之機率愈低。

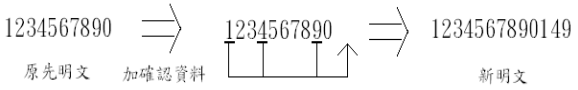

圖 2、增加確認資料

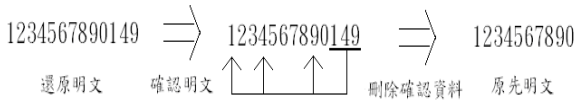

圖 3、驗證確認資料

表 1、記憶體使用量比較表

類型	記憶體使用量 (單位：bits)
10 進位	310 x 8 = 2480
2 進位	1024 x 1 = 1024
2^{16}進位	64 x 16 = 1024
萬進位	78 x 16 = 1248

3. 加解密運算

使用Cricket感測器時，因其僅支援 32 位元整數運算，並不適用於加密所需之運算(如：1024 位元大數運算)，因此，需實作適用於加解密之運算方法。各種方法之記憶體使用量比較如表 1所示，最簡單之方式是將大數當字元陣列處理，每一資料以 0~9 表示，運算方式如同直式計算。此方式優點在於資料以十進位表示，計算過程容易理解，但其缺點在於需使用大量陣列空間(如：1024 位元約為 10^{310}，運算時需大小約為 310 的 8 位元陣列)，不但浪費大量記憶體，且計算速度緩慢。

除上所述外，亦可將大數表示成 0 和 1，用邏輯運算和位移進行二進位處理。優點在於計算快速與記憶體使用率較高，缺點在於難以理解，程式上難以設計。如改以 16 位元儲存資料，每一數字可表示 0~65535(2^{16})，在計算上可使用 2^{16}進位直式計算，只需要大小為 64 的 8 位元數字陣列，但同樣於使用時較為麻煩。本研究將每一數字表示成 0~9999，以大小為 78 之 8 位元數字陣列儲存，進行萬進位計算。

3.1 大數乘法

本論文使用直式運算實作乘法部份，計算前先將資料型態從 16 位元轉換成 32 位元以避免溢位，在每次部份計算過程中，將會得到三個暫存值，分別為累加值、進位與部份積，如圖 4所示，三個暫存值之總和，除以進位數之商數，即為新進位，而餘數則為新的累加值。

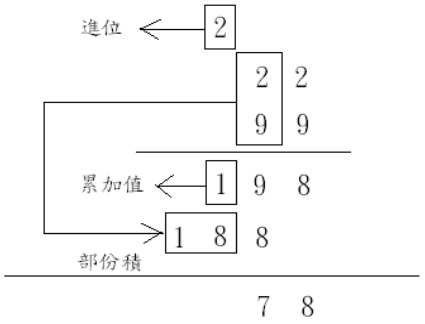

圖 4、暫存值示意圖

表 2、計算次數比較表

類型	記憶體使用量 (單位：bits)	單次計算次數	總計算次數
2^{16}進位	64 x 16 = 1024	4	16384
萬進位	78 x 16 = 1248	2	12168

以 16 位元儲存資料時，有 2^{16}進位與萬進位兩種方式，如表 2所示。使用 2^{16}進位時，一個數字最大可以表示到 65535，所以部份積之最大值可至 2^{32}，若再加上進位與累加值，將產生溢位問題。因此，採用 2^{16}進位時，需兩次計算才能算出新的進位與累加值。另一種採用萬進位之方式，則因三個暫存值總和並無溢位問題，因此可一次計算出新的進位和累加值。兩者相較之下，萬進位所需之計算次數較 2^{16}進位少。

Cricket 感測器因運算處理能力較慢，運行加密機制時，即時性需求仍較記憶體空間需求為高，亦即在有限的記憶體空間內，加密計算次數愈少愈佳，故本論文實作 Rabin 非對稱式金鑰加密演算法時，採用萬進位方式作計算。

3.2 大數求餘數

基本餘數求法為被除數減去除數，直至除數比被除數大時，此時的被除數即為餘數。然而此計算方式過於緩慢，更有效率的方法是預估倍數，一次減去數倍的除數以加快餘數的求得。愈精確的預估倍數，便能愈有效率的取得餘數。

本論文取被除數與除數之第一組數字，以此當作被除數與除數之近似值，估計倍數。若除數之近似值小於原除數時，預估之倍數將大於原始倍數，故在求除數近似值時，必須無條件進位，如圖 5所示。

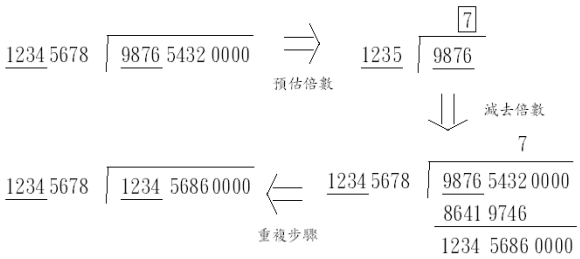

圖 5、預估餘數示意圖

4. 效能評估

本論文實作於Cricket感測器，並佈建於室內天花板上進行測試(如圖 6、圖 7及圖 8)，程式執行畫面如圖 9、圖 10所示。系統本身最大可使用 2048 位元加密。實際測試後，於時間效能方面，使用 1024 位元公鑰加密 512 位元之資料時，只需花費 1 秒即可完成。同樣使用 1024 位元公鑰，改加密 1024 位元之資料時，仍可於 3 秒內完成加密動作。

記憶體空間使用量方面，在 1024 位元公鑰加密下，需要 1248 位元儲存公鑰，2496 位元儲存加密資料，2496 位元儲存暫存資料，瞬間需要最大記憶體空間約為 6240 位元。

圖 6、實際佈建照片 1

圖 7、實際佈建照片 2

圖 8、實際佈建照片 3

圖 9、金鑰產生畫面

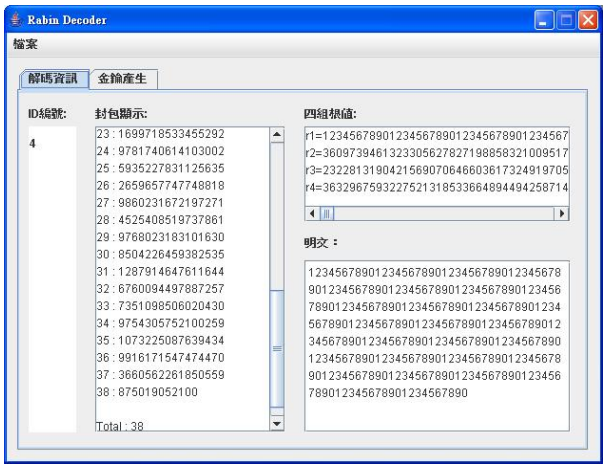

圖 10、解密完成畫面

5. 結論

本論文以數位家庭環境傳遞使用者居家與生理資料之應用為實例，說明如何實作 Rabin 非對稱式金鑰加密演算法於 Cricket 感測器，達到輕量加密的目的。為減輕傳輸加密所造成之負擔，改進運算方式，減少記憶體使用量與計

算次數，擁有即時與空間使用少之特性，解決無線網路感測器因計算能力與記憶體空間不足，無法執行高階加密演算法之問題。此實作可以應用於各種無線感測網路上，藉以改善無線感測網路傳輸安全，保障使用者之隱私。

參考文獻

[1] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, "*Handbook of applied cryptography*," CRC Press Series on Discrete Mathematics and its Applications., CRC Press, Boca Raton, FL, 1997.

[2] Akyildiz, I.F.; Weilian Su; Sankarasubramaniam, Y.; Cayirci, E., "*A survey on sensor networks*," Communications Magazine, IEEE , vol.40, no.8, pp. 102-114, Aug 2002

[3] Arampatzis, Th.; Lygeros, J.; Manesis, S., "*A Survey of Applications of Wireless Sensors and Wireless Sensor Networks*," Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation , vol., no., pp.719-724, 27-29 June 2005

[4] A. Salomaa, "*Public-Key Cryptography*," Springer-Verlag, 1990.

[5] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "*Alarm-net: Wireless sensor networks for assisted-living and residential monitoring*," in Technical Report CS-2006-11. University of Virginia, 2006.

[6] Cricket, http://cricket.csail.mit.edu/

[7] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, and J. Stankovic, "*An advanced wireless sensor network for health monitoring*," In Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2), April 2006.

[8] Huan Chen; Bo-Chao Cheng; Chih-Chuan Cheng; Li-Kuang Tsai, "*Smart Home Sensor Networks Pose Goal-Driven Solutions to Wireless Vacuum Systems*," Hybrid Information Technology, 2006. ICHIT '06. International Conference on , vol.2, no., pp.364-373, 9-11 Nov. 2006

[9] M. Rabin, "*Digital Signatures and Public-Key Encryptions as Intractable as Factorization*," MIT Technical Report No 212, 1979.

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"*Wireless sensor networks: a survey*", Computer Networks 38, Elsevier, pp. 393–422, 2002.

[11] R.-G. Lee, C.-C. Lai, S.-S. Chiang, H.-S. Liu, C.-C. Chen, and G.-Y.Hsieh, "*Design and implementation of a mobile-care system over wireless sensor network for home healthcare applications*," in Proc. 28th Annu. Int. Conf. IEEE Engineering in Medicine and Biology Society, New York, USA, Aug. 30–Sep. 3, 2006, pp. 6004–6007.

[12] R. Rivest, A. Shamir and L. Adleman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*," Communications of the ACM, Vol. 21, No 2, pp. 120{126, 1978.

[13] Ruizhong Lin; Zhi Wang; Youxian Sun, "*Wireless sensor networks solutions for real time monitoring of nuclear power plant*," Intelligent Control and Automation, 2004. WCICA 2004. Fifth World Congress on , vol.4, no., pp. 3663-3667 Vol.4, 15-19 June 2004

[14] W. Diffie and M. Hellman, "*New Directions in Cryptography*," IEEE Transaction on Information Theory, IT-22,6, pp. 644{654, 1995.

[15] Y. Wang, G. Attebury, and B. Ramamurthy, "*A survey of security issues in wireless sensor networks*," IEEE Communications Surveys and Tutorials, vol. 8, no. 2, 2006.