行政院國家科學委員會專題研究計畫 期中進度報告

高可靠無線網路暨安全訊息通訊之研究(2/3)
期中進度報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 95-2221-E-002-068-
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：郭斯彥

處 理 方 式 ：期中報告不提供公開查詢

中 華 民 國 96 年 05 月 31 日

行政院國家科學委員會補助專題研究計畫 □ 成 果 報 告 ■期中進度報告

高可靠無線網路暨安全訊息通訊之研究

計畫類別：■個別型計畫　　□整合型計畫
計畫編號：NSC－95－2221－E－002－068
執行期間：95 年 8 月 1 日至 96 年 7 月 31 日

計畫主持人：郭斯彥

計畫參與人員：王思齊、吳明蔚、黃耀文、周宏儒

成果報告類型(依經費核定清單規定繳交)：■精簡報告 □完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立台灣大學 電機工程學系

中　華　民　國　96　年　5　月　30　日

行政院國家科學委員會專題研究計畫成果報告
高可靠無線網路暨安全訊息通訊之研究

Research on Dependable Wireless Network and Secure Message Communication

計畫編號：NSC 95-2221-E-002-068
執行期限：民國95年08月01日到96年07月31日
主持人　：郭斯彥　台灣大學電機工程學系教授

一、中英文摘要

隨著低功率微機電與無線通訊等技術的進步，許多學術機構和企業都積極在開發各式各樣的感測器或無線節點，因應用目的或開發單位不同，其大小、外觀和附加的功能也有殊異。由具無線通訊和基本運算能力的節點所組成的網路可統稱為MANET (mobile ad hoc networks)，其本身就是前瞻的研發議題。因為這類網路天生的特性，如動態的網路拓樸、非常有限的系統資源等等，為其發展帶來很多挑戰。因此本計劃對於可靠度與穩定度的議題進行深入探索，並提出從理論面到實作面的解決方案。我們相信經由發展這方面的關鍵技術，可有效解決未來更廣泛應用無線隨意感測網路時的障礙。

在新一代的網路架構中，不但會存在獨立的 MANET 環境，也會出現與不斷演化的大型網路(如 Internet 或 3G/4G 網路)相連結的 MANET 網路。在這應用下，使用者經由手持裝置可以隨時隨地接收或分享資訊串流。由於這類網路會大大增加維護系統可靠度與穩定度的困難度。基本上，資料備份可以有效建構具有容錯能力的分散式應用系統。其基本原理是在不同節點上同時擁有數份資料複本，如果原先負責服務的節點有錯誤發生，則改由其他有資料複本的節點接手。此外，群組成員的加入維護或是訊息廣播等功能，都與系統的穩定性和可擴充性密切相關，在實際應用層面的考量上，由於分散式計算環境潛在的不同步性，使得我們無法精確的預估不同裝置間通訊延遲、時脈偏移與執行時間的上限。眾多的研究指出，與資訊可靠性相關的問題，將變得極複雜和困難。為了本計劃更具有實用價值，我們將致力於研究在分散式環境下錯誤偵測服務以及群組成員協定等基礎問題的解決之道。

另外，企業對資訊科技的依賴越來越大，垃圾郵件已變成每日生活的一部份，隨之而來的，對於面臨資安威脅也愈來愈多，故資安相關議題日趨重要。然而，放眼今日全球資安產業，所有廠商均集中於發展硬體式的安全防護，這類解決方案只能治標式地在出現安全漏洞時，進行各種防堵措施，卻未能從最源頭，及程式設計之初，便完全避開可能產生任何安全風險的疑慮，讓政府與企業均能安心、安全地以資訊作業，提高工作效率與商業效益。

本計畫以高可靠無線網路暨安全訊息通訊之研究為主軸，我們仔細觀察並擬定三項子題目，做為研究主題：(1) 在移動無線網路環境下動態基礎結構之可靠度；(2) 評估並解決隱私暨安全管理；(3) 實際可行之 Web 應用軟體安全性驗證。

關鍵詞：無線隨意網路、錯誤偵測、系統可靠度、隨機分散式演算法、垃圾郵件、Web 應用程式安全、程式碼漏洞

Abstract

Thanks to the advances in wireless communication technology, we believe that a deeper understanding of MANET (mobile ad hoc networks) is necessary. If fact, these networks pose significant challenges in academia due to their unique characteristics. dependability-related issues will play a key role in system development.

In this project, we aim to investigate fault-tolerant computing and dependable data communications in wireless ad hoc networks. Basically, we provide fault tolerance via failure detectors, randomized distributed schemes, and data replication. Furthermore, we introduce the concept of cross-layer design to guarantees higher system stability in a mobile wireless environment.

On the other hand, both enterprises and individuals is relying more and more on ICT (information and communication technology). Consequently, we face greater threat from the outside cyberspace. However, most security vendors addressed existing security threat from the view point of network solution and hardware approach, while these root causes of most security vulnerabilities are at the source – the source code. It is essential to fix the bug at the earliest stage of SDLC and prevent any possible vulnerability before it actually takes place.

The main theme of this project is "research on dependable wireless networks and secure message communications". It consists of three sub-projects, namely (1) Survivability of Dynamic Infrastructures in Wireless Ad Hoc Networks; (2) Evaluating and Resolving Privacy and Security Management; and (3) A Practical Verification Platform for Web Application Security.

Keywords: Mobile Ad hoc Networks, Failure Detectors, System Dependability, Randomized Distributed Algorithms, Spam e-mails, Web Application security, Source Code Vulnerabilities.

二、前言

本研究計畫由三個面向來探討高可靠無線網路暨安全訊息通訊之研究主題。第一階段的主題是探討無線環境下之可靠度，包括網路的拓樸控制，尤其影響無線行動網路效能的最重要因素在於組成網路的行動節點能源保存的能力，由於能源的消耗主要來自於持續進行的資料通訊，因此我們需要在設計網路拓樸演算法時就將能源效能的理念導入，以建構用來進行資料通訊的虛擬骨幹。

第二階段的主題則是提供無線行動網路錯誤偵測的機制。當錯誤被偵測出來之後，群組成員協定則提供了群組內協調狀態的管道，利用這個管道各成員將可更新內部的狀態資訊，並選出新的領導者。在以往的研究中多只針對電腦叢集或具有高度同質性的固接式分散式環境討論，很少有在無線網路上的探討。因此我們必須構思如何對過去群組成員協定的方法做相關的調整與修正。

至於第三階段在於探討系統之隱私及安全之問題，尤以垃圾郵件及監視軟體為近幾年最嚴重的問題，有迫切解決之需要。從諸多報告顯示，目前並沒有有效解決此問題之完整方案，是以我們從系統面切入，以最少之資源，提出最有效之機制，期使一般使用者亦能有效地管理自身

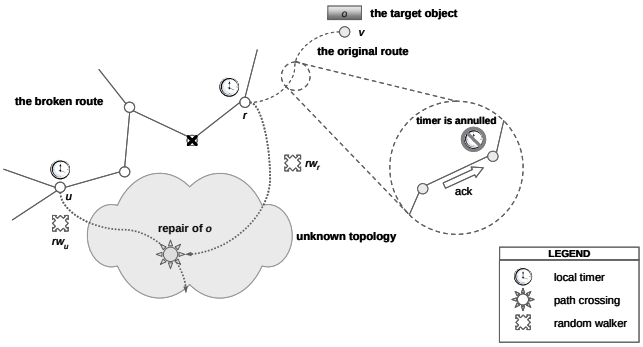
的隱私權及安全性問題，遏止垃圾郵件及監視軟體之入侵。

五、研究方法

首先，系統可靠度是指一個應用系統能否在錯誤隨時都可能發生的情況下，還能夠長時間保持在可使用且穩定的狀態。要提高系統可靠度，我們必須有容錯的機制，而錯誤偵測(failure detection)是所有容錯議題的核心。常見的錯誤偵測的型式有兩種：推動(push)和拉出(pull)，兩種型式的差別在於錯誤偵測資訊的流動方向。一般而言，拉出式的錯誤偵測比較不需要額外的控制訊息。一個分散式環境所能提供的錯誤偵測品質，會影響建構在其上的應用系統效能。所謂錯誤偵測的品質主要是指偵測時間(detection time)與準確度(accuracy)。提昇錯誤偵測的品質往往需要消耗多餘的系統資源，找出在花費代價最少的情況下提供合理偵測品質的方法，對於系統設計者來說是關鍵與重要的。在同儕網路這類的大型系統中，通常成員的數目眾多，這時如何安排錯誤偵測的架構將是相當重要的議題，因為大量的錯誤偵測會消耗過多的網路頻寬、處理時間等重要的系統資源，所以可以引進階層式錯誤偵測的概念。綜而言之，主要關聯在於提供由錯誤偵側為基礎的中介軟體。

群組成員協定的主要目的就是用來維持群組成員狀態的一致性。要研究群組成員協定，在理論基礎上必須討論的議題相當多[32-34]。首先，如上所述，對於每一個成員，我們要利用系統提供的錯誤偵測機制來更新其可能出錯(suspect)的成員名單。再來，對於負責管理群組的程式，要能夠根據即時的狀態資訊與狀態轉換圖(state transition diagram)採取適當的步驟。事實上，因為錯誤偵測所需要的基本功能之一本來就是週期性對於資料的散佈(dissemination)和匯集(aggregation)，一個明顯的例子為定期告知整體系統失去功能的成員名單。所以我們也需將訊息傳送的機制納入設計的考量。

首先，第一個子題重點在如何有效率地利用各節點的暫存資料進行錯誤回復，其基本的想法是，為了加快修復的速度與節省網路資源，希望能儘可能找到最低成本的節點來重新傳送資料。然而，相較於傳統的固接網路，MANET 的架構更需將節點與連結的暫時性失效、網路拓樸變化以及系統本身的不同步性納入考量。換句話說，因為這類網路充滿變動，所以設計演算法時要克服對系統資訊局部性的限制。本計劃將採取分散隨機式演算法來解決容錯方面的議題。簡單來說，若出現因繞路等因素引起的逾時等待或資料更新錯誤，可啟動一個以上以隨機移動為基礎的修復程序，如下圖所示。



圖一、以隨機移動為基礎的繞路修復。

其次，第二個子題重點在隱私暨安全管理，我們以垃圾郵件問題為研究標的，主要鑑於垃圾郵件已變成每日生活的一部份，為解決此迫切議題，我們檢視既有的防堵垃圾郵件之解決方案，同時並探討為何既有的方案並不能有效解決當前的垃圾信件問題。我們發現，大部分的垃圾郵件對於方法拆解(munging)及過濾(filtering)都可以規避，而對列表(listing)

及修正(shaping)則容易誤判，挑戰(challenging)則不夠方便，身份轉換(identity-hopping)則目前尚未普遍。因此，我們提出的作法具有一定的實用價值。

最後，在第三個子題—實際可行之Web應用軟體安全性驗證方面，我們所發展出的解析器為「結合樹擴張與樹剪枝之高效能解析器」。此技術已申請專利，創新性是能利用樹擴張來同時確保程式碼的完整性與有效性，再利用樹剪枝簡化不必要的節點，重組結構樹以達成本最佳化。採用上述的創新作法能讓解析器的執行速度大幅提昇，以達到對效能的要求。

六、結果與討論

在第一個子題部分，由於相關技術的進步和實際應用上的需求，無線隨意感測網路在可預見的未來將有非常快速的發展。而可靠度與可擴充性的問題在這類應用的研究上是非常關鍵的，若能掌握這方面的技術，就能在領域占有一席重要的地位。事實上，由過往發展網際網路等系統的經驗可知，完善的關鍵技術是建構高韌性與高穩定性應用系統不可或缺的核心。因為這領域的快速成長，很多重要的關鍵技術都還處於探索的初期，不夠成熟和完備，或是受限於目前的工程技術水準而難以預塑未來樣貌，因此更有進行這方面工作的必要。另外參與人員將可獲得與容錯機制設計相關的背景知識，擁有實作分散隨機式演算法和理論推導的經驗，並可學習如何使用適當的模擬工具和實驗平台來驗證成果。

在第二個子題部分，為達到有效遏阻及防堵，本計畫以多面向之防垃圾信機制，包括(1)列表合法寄件者；(2)將郵件貼上標籤以及(3)挑戰可能的垃圾郵件寄送者。我們提出的防垃圾信代理人(SRMA)與既有的郵件轉送代理程式(MTA)拋棄式郵件位址(DEA)合作。此多面向整合的解決方案可以有效將垃圾郵件寄送者阻擋在系統之外。

在第三個子題部分，軟體驗證技術粗略可分為靜態分析與動態分析兩種方法。靜態分析之優點在於效率，不影響程式之執行；但是由於必須在編譯期(compile-time)預估程式在執行時(runtime)所有可能的狀態，因此常受限於狀態擴張(state explosion)之問題而無法有效驗證較大之程式碼。此問題使得許多靜態軟體驗證技術無法取得實際之應用。動態驗證是在程式執行之同時執行驗證，比較準確並且沒有狀態擴張之問題；其缺點則是會減緩程式之執行速度。在分析 Web 應用程式之程式碼之前，我們先將目前 Web 應用程式之弱點正規化(formalize)為安全資料流(secure information flow)之問題。這種作法讓我們將複雜的 Web 程式碼資安漏洞正規成以一種自動狀態機，即 Latice 模型，此乃資訊安全中之典型問題。

本年度至目前討論的結果為止完成之工作項目包含下列各項：

1. 在無線感測網路上導入自我組織機制。
2. 發展模擬器以初步評估演算法的效能並持續修正不足之處。
3. 瞭解多面向防垃圾信件之機制的系統可行度及實作細節。
4. 瞭解傳統軟體工程正規驗證演算法
5. 分析並測試各種網頁應用程式相關安全協定及標準。

下年度之計畫預計將研究如何瞭解

各種錯誤偵測和容錯功能如何與網路其它層級協同運作。，其目標如下：

1. 設計無線隨意網路上錯誤修復的分散隨機式演算法。
2. 以模擬器來驗證所建構的容錯機制帶來的增益。
3. 設計多面向防垃圾郵件之機制。
4. 探討並評估傳統軟體工程正規驗證演算法。
5. 瞭解多面向防垃圾信件之機制的系統可行度及實作細節。

七、參考文獻

[1] M. K. Aguilera, W. Chen, and S. Toueg, "Failure detection and consensus in the crash-recovery model," *Distributed Computing*, 13(2), pp. 99-125, Apr. 2000.

[2] I. Gupta, T. D. Chandra, and G. S. Goldszmidt, "On scalable and efficient distributed failure detectors," *Proc. 20th Ann. ACM Symposium on Principles of Distributed Computing* (*PODC*), Aug. 2001.

[3] W. Chen, S. Toueg and M. K. Aguilera, "On the quality of service of failure detectors," *Proc. 30th Int'l Conf. Dependable Systems and Networks* (*DSN*), June 2000.

[4] A. Fekete , N. Lynch, and A. Shvartsman, "Specifying and using a partitionable group communication service," *Proc. 16th Ann. ACM Symposium on Principles of Distributed Computing* (*PODC*) pp.53-62, August, 1997.

[5] L. M. Feeney, M. Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment," *IEEE INFOCOM 2001*, pp. 1548–1557, 2001.

[6] I. Stojmenovic and X. Lin, "Power-aware Localized Routing in Wireless Networks," *IEEE International Parallel and Distributed Processing Symposium*, 2000.

[7] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks," *IEEE Journals on Selected Areas in Communications*, 17(8):1333-1344, 1999.

[8] L. Li and J. Halpern, "Minimum Energy Mobile Wireless Networks Revised," *IEEE International Conference on Communications* (*ICC 2001*), June 2001.

[9] X.-Y. Li and P.-J. Wan , "Constructing Minimum Energy Mobile Wireless Networks," *ACM Symposium on Mobile Ad Hoc Networking and Computing* (*MobiHoc*), Long Beach, California, October 2001.

[10] A. E. F. Clementi, P. Penna, and R. Silvestri, "On the Power Assignment Problem in Radio Networks," *Electronic Colloquium on Computational Complexity* (*ECCC*), 2000.

[11] L. Kirousis, E. Kranakis, D. krizanc, and A. Pelc, "Power Consumption in Packet Radio Networks," *Symposium on Theoretical Aspects of Computer Science* (*STACS*), 1997.

[12] G. Calinescu, I. Mandoiu, and A. Zelikovsky, "Symmetric Connectivity with Minimum Power Consumption in Radio Networks," *IFIP-TCS*, 2002.

[13] N. Li, J. Hou, and L. Sha, "Design and Analysis of an MST-Based Distributed Topology Control Algorithm," *IEEE INFOCOM 2003*, June 2003.

[14] J. Hromkovic, R. Klasing, B. Monien, and R. Peine, "Dissemination of Information in Interconnection Networks (Broadcasting and Gossiping)," *Combinatorial Network Theory*, pp. 125-212, 1996.

[15] T. D. Chandra and S. Toueg, "Unreliable Failure Detectors for Reliable Distributed Systems," *Journal of the ACM*, 43(2), pp. 225-267, Mar. 1996.

[16] I. Gupta, T. D. Chandra, and G. S. Goldszmidt. "On Scalable and Efficient Distributed Failure Detectors," *Proc. 20th Ann. ACM Symposium on Principles of Distributed Computing* (*PODC 2001*), Newport, Rhode Island, USA, Aug. 2001.

[17] R. van Renesse, Y. Minsky, and M. Hayden. "A Gossip-Style Failure Detection Service," *Proc. of Middleware'98*, Sep. 1998.

[18] M. J. Lin and K. Marzullo, "Directional Gossip: Gossip in a Wide Area Network," *European Dependable Computing Conference*, pp. 364-379, 1999.

[19] S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *Proc. Conf. Mobile Computing, MOBICOM*, pp. 151-162, Aug. 1999.

[20] J. Wu and H. Li, “A Dominating Set Based Routing Scheme in Ad Hoc Wireless Networks,” *Proc. Third Int’l Workshop Discrete Algorithms and Methods for Mobile Computing and Comm.* (*DIALM*), pp. 7-14, Aug. 1999.

[21] L. Yin and G. Cao, “Supporting cooperative caching in ad hoc networks,” *IEEE INFOCOM 2004*, March 2004.

[22] E. Cohen, S. Shenker, “Replication strategies in unstructured peer-to-peer networks,” *Proceedings of ACM SIGCOMM*, August 19-23, 2002, Pittsburgh, Pennsylvania, USA.

[23] Q. Lv , P. Cao , E. Cohen , K. Li , S. Shenker, “Search and replication in unstructured peer-to-peer networks,” *Proceedings of the 16th international conference on Supercomputing*, June 22-26, 2002, New York, New York, USA.

[24] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup service for internet applications,” *ACM SIGCOMM*, San Diego, CA, Aug. 2001.

[25] Q. Zhang, F. Yang, W. Zhu, and Y.-Q. Zhang, "A construction of locality-aware overlay network: mOverlay and its performance," *IEEE Journal on Selected Areas in Communications (JSAC)*, 22(1):18-28, January 2004.

[26] S. Mukhopadhyay, D. Panigrahi and S. Dey, “Data aware, low cost error correction for wireless sensor networks,” *Proceedings WCNC 2004*, Atlanta, 21-25 March 2004.

[27] R. Albert, H. Jeong, and A. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378-382, 2000.

[28] K.P. Birman et al., “Bimodal Multicast,” *ACM Transactions on Computer Systems*, vol. 17, no. 2, 1999, pp. 41-88.

[29] P.T. Eugster et al., “Lightweight Probabilistic Broadcast,” *ACM Transactions on Computer Systems*, vol. 21, no. 4, 2003, pp. 341-374.

[30] Ahn, L. von, Blum, M., Hopper, N.J., and Langford, J. (2003). CAPTCHA: Telling humans and computers apart. In Advances in Cryptology, Eurocrypt '03, volume 2656 of Lecture Notes in Computer Science, pp. 294-311

[31] Androutsopoulos, I., Koutsias, J., Chandrinos, K. V., Paliouras, G., and Spyropoulos, C. D. (2000a). An evaluation of Naive Bayesian anti-spam filtering. In Proceedings of the workshop on Machine Learning in the New Information Age, pp. 9-17.

[32] Carreras, X. and Marquez, L. (2001). Boosting trees for anti-spam e-mail filtering. In Proceedings of RANLP-01, 4th International Conference on Recent Advances in Natural Language Processing.

[33] Cranor, L. F. and LaMacchia, B. A., (1998). Spam! Communications of the ACM. 41(8), pp. 74-83.

[34] Dean, D. and Stubblefield, A. (2001, Aug.). Using client puzzles to protect TLS. In Proceddings of the 10th USENIX Security Symposium.

[35] Dwork, C. and Naor, M. (1993). Pricing via processing or combatting junk mail. In Lecture Notes in Computer Science 740 (Proceedings of CRYPTO'92), pp. 139-147.

[36] Dwork, C., Goldberg, A., and Naor, M. (2003). On memory-bound functions for fighting spam. In Lecture Notes in Computer Science 2729 (Proceedings of CRYPTO'03), pp. 426-444.

[37] Franklin, M. and Malkhi, D. (1998). Auditable metering with lightweight security. The Journal of Computer Security, 6(4):237--255.

[38] Gburzynski, P. and Maitan, J. (2003, Apr.). A comprehensive approach to eliminating spam. Proceedings of EUROMEDIA'03, Plymouth, UK.

[39] Gburzynski, P. (2004) SFM: an Implementation of the Challenge-Response Paradigm in Electronic Mail for Spam Avoidance. Working Paper.

[40] Gburzynski, P. and Maitan, J. (2004). Fighting the spam wars: A remailer approach with restrictive aliasing. ACM Transactions on Internet Technology, vol. 4, no. 1, pp. 1-30.

[41] Gross, Grant (2003). Spam hearing: E-mail tax, international treaty proposed. InfoWorld, May 21, 2003.

http://www.infoworld.com/article/03/05/21/HNspamtax_1.html

[42] Hird, S. (2002, Sep.). Technical solutions for controlling spam. In Proceedings of Australian UNIX and Open Systems Users Group (AUUG'02), Melbourne.

[43] Jacob, P. The spam problem: moving beyond RBLs. Available: http://theory.whirlycott.com/~phil/antispam/rbl-bad/rbl-bad.html

[44] Jacobsson, M. and Juels, A. (1999). Proofs of Work and Bread Pudding Protocols. In Proceedings of the IFIP TC6 and TC11 JointWorking Conference on Communications and Multimedia Security (CMS '99), Kluwer.

[45] Joachims, T. (1998). Text categorization with support vector machines: Learning with many relevant features. In Proceedings of the 10th European Conference on Machine Learning, number 1398 in LNCS. Springer Verlag, Heidelberg, DE.

[46] Juels, A. and Brainard J. (1999). Client puzzles: a cryptographic defense against connection depletion. In Proceedings of NDSS-1999 (Networks and Distributed Security Systems), pp. 151-164.

[47] Kohavi, R. (1995). A study of cross-validation and bootstrap for accuracy estimation and model selection. In Proceeding of the 12th International Joint Conference on Artificial Intelligence (IJCAI-1995), Morgan Kaufmann, pp. 1137-1143.

[48] Krim, Jonathan (2003). “A spammer speaks out: In Hill testimony, bulk e-mailer says Internet providers use same tactics,” Washington Post, May 22, 2003, p. A01.

[49] Lakshminarayanan, K., Adkins, D., Perrig, A., and Stoica, I. (2003, Nov.). Taming IP packet flooding attacks. 2nd Workshop on Hot Topics in Networks (HotNets-II)

[50] Laurie, B. and Clayton, R. (2004, May). "Proof-of-Work" Proves Not to Work. The Third Annual Workshop on Economics and Information Security (WEIS04).

[51] Li, K., Pu, C., and Ahamad, M. (2004, Jul.). Resisting spam delivery by TCP damping. In the first Conference on Email and Anti-Spam (CEAS 2004), Mountain View, CA.

[52] Massey, B., Thomure, M., Budrevich, R., and Long, S. (2003). Learning spam: simple techniques for freely-available software. In Proceedings of the USENIX 2003 Annual Technical Conference (FREENIX Track), pp. 63-76, San Antonio, TX.

[53] Mori, G. and Malik, J. (2003, Jun.) Recognizing objects in adversarial clutter - Breaking a visual CAPTCHA. In Proceedings of the Conference on Computer Vision and Pattern Recognition.

[54] Schneider, K.-M. (2003). A comparison of event models for Naive Bayes anti-spam e-mail filtering. In Proceedings of the 10th Conference of the European Chapter of the Association for Computational Linguistics. Budapest, Hungary, pp. 307–314.

[55] Serjantov, A. and Lewis, S. (2003, Oct.). Puzzles in P2P systems. 8th CaberNet Radicals Workshop, Corsica.

[56] Turner, D. and Havey, D. (2004). Controlling spam through lightweight currency. In Proceedings of the Hawaii International Conference on Computer Sciences, Honolulu, HI.

[57] Ashcraft, K., Engler, D. "Using Programmer-Written Compiler Extensions to Catch Security Holes." In Proceedings of the 2002 IEEE Symposium on Security and Privacy, pages 131-147, Oakland, California, 2002.

[58] Banerjee, A., Naumann, D.A. "Secure Information Flow and Pointer confinement in a Java-Like Language." In: Proceedings of the 15th Computer Security Foundations Workshop, pages 239-253, Nova Scotia, Canada, 2002.

[59] Bobbitt, M. "Bulletproof Web Security." Network Security Magazine, TechTarget Storage Media, May 2002. http://infosecuritymag.techtarget.com/2002/may/bulletproof.shtml

[60] CERT. “CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.” http://www.cgisecurity.com/articles/xss-faq.shtml

[61] Cowan, C., D. Maier, C. Pu, Walpole, J., Bakke, P., Beattie, S., Grier, A., Wagle, P., Zhang, Q., Hinton, H. “StackGuard: Automatic adaptive detection and prevention of buffer-overflow attacks.” In

Proceedings of the 7th USENIX Security Conference, pages 63--78, San Antonio, Texas, Jan 1998.

[62] Cowan, C. "Software Security for Open-Source Systems." IEEE Security and Privacy, 1(1):38-45, 2003.

[63] Curphey, M., Endler, D., Hau, W., Taylor, S., Smith, T., Russell, A., McKenna, G., Parke, R., McLaughlin, K., Tranter, N., Klien, A., Groves, D., By-Gad, I., Huseby, S., Eizner, M., McNamara, R. "A Guide to Building Secure Web Applications." The Open Web Application Security Project, v.1.1.1, Sep 2002.

[64] Denning, D. E. "A Lattice Model of Secure Information Flow." Communications of the ACM, 19(5):236-243, 1976.

[65] Dharmapurikar, S., Krishnamurthy, P., Sproull, T., and Lockwood, J. "Deep Packet Inspection Using Parallel Bloom Filters." In Proceedings of the 11th Symposium on High Performance Interconnects, pages 44-51, Stanford, California, 2003.

[66] Federal Trade Commission. "Security Check: Reducing Risks to your Computer Systems." 2003. http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm

[67] Foster, J. S., Fähndrich, M., Aiken, A. "A Theory of Type Qualifiers." In Proceedings of the ACM SIGPLAN 1999 Conference on Programming Language Design and Implementation, pages 192--203, volume 34(5) of ACM SIGPLAN Notices, Atlanta, Georgia, May 1-4, 1999.

[68] Goguen, J. A., Meseguer, J. "Security Policies and Security Models." In Proceedings of the IEEE Symposium on Security and Privacy, pages 11-20, Oakland, California, Apr 1982.

[69] Hallem, S., Chelf, B., Xie, Y., Engler, D. "A System and Language for Building System-Specific, Static Analyses." In Proceedings of the ACM SIGPLAN 2002 Conference on Programming Language Design and Implementation, pages 69-82, Berlin, Germany, 2002.

[70] Higgins, M., Ahmad, D., Arnold, C. L., Dunphy, B., Prosser, M., and Weafer, V., "Symantec Internet Security Threat Report—Attack Trends for Q3 and Q4 2002," Symantec, Feb 2003.

[71] Holzmann, G. J. "The Logic of Bugs." In Proceedings of the 10th ACM SIGSOFT Symposium on Foundations of Software Engineering, pages 81-87, Charleston, South Carolina, 2002.

[72] Huang, Y. W., Huang, S. K., Lin, T. P., Tsai, C. H. "Web Application Security Assessment by Fault Injection and Behavior Monitoring." In Proceedings of the Twelfth International World Wide Web Conference, 148-159, Budapest, Hungary, May 21-25, 2003.

[73] Huang, Y. W., Yu, F., Hang, C., Tsai, C. H., Lee, D. T., Kuo, S. Y. "Securing Web Application Code by Static Analysis and Runtime Protection." In *Proceedings of the Thirteenth International World Wide Web Conference (WWW2004)*, pages 40-52, New York, May 17-22, 2004.

[74] Huang, Y. W., Yu, F., Hang, C., Tsai, C. H., Lee, D. T., Kuo, S. Y. "Verifying Web Applications Using Bounded Model Checking." In *Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN2004)*, pages 199-208, Florence, Italy, Jun 28-Jul 1, 2004.

[75] Hughes, F. "PHP: Most Popular Server-Side Web Scripting Technology." LWN.net. http://lwn.net/Articles/1433/

[76] Kavado, Inc. "InterDo Version 3.0." Kavado Whitepaper, 2003.

[77] Krishnamurthy, A. "Hotmail, Yahoo in the run to rectify filter flaw." TechTree.com, March 24, 2004. http://www.techtree.com/techtree/jsp/showstory.jsp?storyid=5038

[78] Meier, J.D., Mackman, A., Vasireddy, S. Dunner, M., Escamilla, R., Murukan, A. "Inproving Web Application Security—Threats and Countermeasures." Microsoft Corporation, 2003.

[79] Microsoft. "Scriptlet Security." Getting Started with Scriptlets, MSDN Library, 1997 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnindhtm/html/instantdhtmlscriptlets.asp

[80] Microsoft. "Visual C++ Compiler Options: /GS (Buffer Security Check)." MSDN Library, 2003. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore/html/vclrfGSBufferSecurity.asp

[81] Myers, A. C. "JFlow: Practical Mostly-Static Information Flow Control." In: Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, pages 228-241, San Antonio, Texas, 1999.

[82] Netscape. "JavaScript Security in Communicator 4.x."

http://developer.netscape.com/docs/manuals/communicator/jssec/contents.htm#1023448

[83] Neumann, P. G. "Risks to the Public in Computers and Related Systems." *ACM SIGSOFT Software Engineering Notes*, 25(3), p.15-23, 2000.

[84] Ohmaki, K. "Open Source Software Research Activities in AIST towards Secure Open Systems." *In Proc. 7th IEEE Int'l Symp. High Assurance Systems Engineering (HASE'02)*, p.37, Tokyo, Japan, Oct 23-25, 2002.

[85] OWASP. "The Ten Most Critical Web Application Security Vulnerabilities." OWASP Whitepaper, version 1.0, 2003.

[86] Sanctum Inc. "Web Application Security Testing – AppScan 3.5." http://www.sanctuminc.com

[87] Sanctum Inc. "AppShield 4.0 Whitepaper." 2002. http://www.sanctuminc.com

[88] Sandhu, R. S. "Lattice-Based Access Control Models." IEEE Computer, 26(11):9-19, 1993.

[89] Scott, D., Sharp, R. "Abstracting Application-Level Web Security." In: The 11th International Conference on the World Wide Web (Honolulu, Hawaii, May 2002), 396-407.

[90] Scott, D., Sharp, R. "Developing Secure Web Applications." IEEE Internet Computing, 6(6), 38-45, Nov 2,002.

[91] Secure Software, Inc. "RATS—Rough Auditing Tool for Security." http://www.securesoftware.com/

[92] Shankar, U., Talwar, K., Foster, J. S., Wagner, D. "Detecting Format String Vulnerabilities with Type Qualifiers." In Proceedings of the 10th USENIX Security Symposium, pages 201-220, Washington DC, Aug 2002.

[93] SPI Dynamics. "Web Application Security Assessment." SPI Dynamics Whitepaper, 2003.

[94] Stiennon, R., "Magic Quadrant for Enterprise Firewalls, 1H03." Research Note. M-20-0110, Gartner, Inc., 2003.

[95] Varghese, S. "Microsoft patches critical Hotmail hole." TheAge.com, March 24, 2004. http://www.theage.com.au/articles/2004/03/24/1079939690076.html

[96] Visa U.S.A. "Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting as of 8/8/2003." Version 2.2, 2003.

[97] Volpano, D., Smith, G., Irvine, C. "A Sound Type System For Secure Flow Analysis." Journal of Computer Security, 4(3):167-187, 1996.

[98] Park, J. S., Sandhu, R. "Role-Based Access Control on the Web." ACM Transactions on Information and System Security 4(1):37-71, 2001.

[99] Pottier, F., Simonet, V. "Information Flow Inference for ML." ACM Transactions on Programming Languages and Systems, 25(1):117-158, 2003.

[100] Sabelfeld, A., Myers, A. C. "Language-Based Information-Flow Security." IEEE Journal on Selected Areas in Communications, 21(1):5-19, 2003.

八、計畫成果自評

本計畫以高可靠無線網路暨安全訊息通訊之研究為目的，從三個面向探討此主題，包括：(1)提高移動無線網路環境下可靠度與可擴充性；(2)評估並解決隱私暨安全管理，以及(3)實際可行之 Web 應用軟體安全性驗證。三個子題所提出之作法皆具創新性與技術深度，目前已被接受之研究論文即達九篇(條列如後)，成果頗為豐碩。

(1) Ming-Wei Wu, Yennun Huang, Ing-Yi Chen, Shyue-Kung Lu and Sy-Yen Kuo, “A Multi-Faced Approach towards Spam-Resistible Mail,” IEEE The 11th International Symposium on Pacific Rim Dependable Computing (PRDC 2005), Dec.12-14, 2005.

(2) Ming-Wei Wu, Yennun Huang, and Sy-Yen Kuo, “A Multi-Faced Approach towards Spam-Resistible Mail.” IEEE DSN 2005 Fast Abstracts, Jul. 2005.

(3) Yi-Min Wang, Roussi Roussev, Chad Verbowski, Aaron Johnson, Ming-Wei Wu, Yennun Huang, Sy-Yen Kuo, “Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management”. USENIX LISA 2004: 33-46

(4) Yao-Wen Huang, Chung-Hung Tsai, Tsung-Po Lin, Shih-Kun Huang, D. T. Lee, Sy-Yen Kuo, “A testing framework for Web application security assessment.” IEEE Computer Networks 48(5): 739-761 (2005)

(5) Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, D. T. Lee, Sy-Yen Kuo, “Verifying Web Applications Using Bounded Model Checking.” IEEE DSN 2004: 199-208

(6) Yao-Wen Huang, Chung-Hung Tsai, D. T. Lee, Sy-Yen Kuo, “Non-Detrimental Web Application Security Scanning.” ISSRE 2004: 219-230

(7) Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo, “Securing web application code by static analysis and runtime protection.” WWW 2004: 40-52

(8) Hong-Zu Chou, Szu-Chi Wang, Ing-Yi Chen, and Sy-Yen Kuo, “Randomized and Distributed Methods for Reliable Peer-to-Peer Data Communications in Wireless Ad Hoc Networks,” to appear in IET Communications (formerly IEE Proceedings Communications)

(9) Hong-Zu Chou, S. C. Wang, and Sy-Yen Kuo, " Randomized Distributed Algorithm for Peer-to-Peer Data Replication," Fast Abstract of IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2007.