

基於安全的網路服務與 RFID 之商車營運系統

黃映瑞、曹偉駿

E-mail: 9511122@mail.dyu.edu.tw

摘要

近年來，網路的普及最直接影響的就是帶動了電子商務的發展，而其所帶來的效益不僅能將企業上、下的供應鏈做有效的管理，也讓企業與消費者之間有了新的通路管道，使得「速度」成為左右企業生存的必要手段及產業競爭力的關鍵。而隨著物流、宅配業的興起，消費者對服務速度的要求也更加嚴苛，如何讓實體商品快速、安全且有效率地送達客戶手中，是物流、宅配服務業者最重要的課題。然而，交通問題一直是現代人的噩夢之一，雖然政府已逐步開始推動智慧型運輸系統，但對於商業運輸業者而言，但其重點仍放在規劃遞送路線，縮短運輸動線距離，達成降低運輸成本的目標，並未考量物流配送過程中交通狀況、車輛狀況、司機行駛狀況及貨品運送過程是否遭到非法盜竊等問題，而這些問題正是消費者能否信賴電子商務的關鍵因素。因此，本論文將結合RFID與XML金鑰管理規範，以建構一個安全的商車營運系統平台，提供供應鏈成員安全又有效率的物流資訊，同時提升商車營運系統的多元服務。

關鍵詞：商車營運系統；XML金鑰管理；網路服務

目錄

封面內頁 簽名頁 授權書.....	iii	中文摘要.....	vi	英文摘要.....	vii
誌謝.....	viii	目錄.....	ix	圖目錄.....	xi
表目錄.....	xiii	第一章 緒論.....	1	1.1 研究動機與背景.....	1
		1.2 研究目的.....	2	1.3 研究流程.....	3
		1.4 研究範圍與限制.....	6	1.5 論文架構.....	6
		第二章 文獻探討.....	8	2.1 無線射頻識別.....	8
		2.1.1 RFID的運作原理.....	9	2.1.2 RFID現有安全議題.....	10
		2.1.3 RFID應用現況.....	11	2.2 網路服務.....	12
		2.2.1 XML加密.....	14	2.2.2 XML簽章.....	15
		2.2.3 XML金鑰管理規範.....	15	2.3 智慧型運輸系統.....	20
		2.3.1 智慧型運輸系統之相關技術探討.....	21	2.3.2 現有商用車輛營運系統運作方式.....	25
		2.3.2 小結.....	27	第三章 建構安全商車營運系統.....	28
		3.1 系統分析.....	28	3.1.1 訂貨階段.....	30
		3.1.2 物流階段.....	33	3.1.3 營運交易統計階段.....	37
		3.2 系統設計.....	39	3.2.1 訂貨階段.....	43
		3.2.2 營運交易統計階段.....	59	第四章 安全性與效能分析.....	63
		4.1 安全性分析.....	63	4.2 效能分析.....	65
		4.3 綜合討論.....	67	第五章 系統實作與模擬.....	70
		5.1 系統開發環境.....	70	5.2 系統實作與測試.....	71
		第六章 結論.....	86	參考文獻.....	88

參考文獻

- [1] 交通部運輸研究所, <http://www.iot.gov.tw>.
- [2] 交通部電信總局, <http://www.dgt.gov.tw>.
- [3] 林志鴻、許晉嘉,「宅配業車輛路線規劃問題之探討」,中華民國第七屆網路研討會,民國91年。
- [4] 陳一昌、黃運貴、張芳旭、蕭偉政、卓訓榮、王晉元、王國材、李永駿、王東祺、林佩憶,「台灣地區發展智慧型運輸系統(ITS)系統架構之研究」,交通部運輸研究所,2000。
- [5] 陳宏宇,「RFID系統入門-無線射頻系統」,松崗出版社,2004年。
- [6] 鄭同柏,「RFID EPC無線射頻辨識完全剖析」,博碩文化,2004年。
- [7] R. L. Courtney, "A Broad View of ITS Standards in the U.S.," IEEE Conference: Intelligent Transportation System, pp.529-536,1997.
- [8] EPCglobal, [9] H. Haddingh, "Developing AFC Systems," Proceeding of the IEEE: Intelligent Transportation Systems, pp. 1167-1170, 2001.
- [10] T. Kanazawa, and A. Sugiura, "Direction Detector System of An Emergency Vehicle for ITS by Using Code Division Multiple Access," IEEE Workshop: Signal Processing Systems, pp. 532-539, 1999.
- [11] J. Kim and K. Moon, "Design of Unified Key Management Model using XKMS," Advanced Communication Technology, 2005, ICACT 2005. Vol. 1, pp. 77-80, 2005.

- [12] C. C. Lin, Y. J. Lin, and Y. D. Lin, " The Economic Effects of Center-to-center Directs on Hub-and-spoke Networks for Air Express Common Carriers, " *Journal of Air Transport Management*, Vol. 9, pp. 255-265, 2003.
- [13] C.L. Liu, " Best-path Planning for Public Transportation System, " *The IEEE 5th International Conference: Intelligent Transportation System*, pp.834-839, 2002.
- [14] K. Michael, L. McCathie, " The Pros and Cons of RFID in Supply Chain Management, " *Proceedings of the International Conference on Mobile Business*, 2005.
- [15] W. Leavitt, " Speed Reading: RFID for Fleets, " *Fleet Owner Overland Park*, Vol. 99, p.82, 2004.
- [16] J. L. Overholt, W. K. Krill, and K. C. Cheok, " Determining and Controlling Emergent Behavior in Intelligent Transportation Systems, " *Digital Avionics Systems Conference: 17th DASC*, Vol. 2, pp. 1-5, 1998.
- [17] C. H. Park and D. H. Cho, " An Adaptive Logical Link Control for Wireless Internet Service in ITS, " *Vehicular Technology Conference: IEEE VTS 50th*, pp. 2213-2217, 1999.
- [18] N. Park, K. Moon, S. Sohn, " A study on the XKMS-based Key Management System for Secure Global XML Web Services, " *Advanced Communication Technology*, 2004. *The 6th International Conference*, Vol. 1, pp. 492-495, 2004.
- [19] N. Park, K. Moon, S. Sohn, " XML Key Management System for Web-based Business Application, " *Network Operations and Management Symposium 2004. NOMS 2004. IEEE/IFIP*, Vol. 1, pp. 903-904, 2004.
- [20] S. Sandoval-Reyes, J. L. Soberanes Perez, " Mobile RFID Reader with Database Wireless Synchronization, " *2nd International Conference on Electrical and Electronics Engineering*, pp. 7-9, 2005.
- [21] M. Shawky, S. Bonnet, S. Favard and P. Crubille, " A Computing Platform and ITS Tools for Features Extraction from On-Vehicle Image Sequences, " *Proceeding of The IEEE: Intelligent Transportation Systems*, pp. 39-45, 2000.
- [22] A. Slater, " Specification for a Dynamic Vehicle Routing and Scheduling System, " *International Journal of Transport Management*, Vol.1, pp.29-40, 2002.
- [23] W. Stallings, " *Cryptography and Network Security*, " 3rd ed. New Jersey: Prentice Hall, 2003.
- [24] K. Toyota, T. Fuji, T. Kimoto and M. Tanimoto, " A Proposal of HIR (Human-Oriented Image Restructuring) System for ITS, " *Proceedings of the IEEE: Intelligent Vehicles Symposium*, pp. 540-544, 2000.
- [25] W3C XML Encryption, , 2001.
- [26] Y. N. Wang, R. G. Thompson and I. Bishop, " A Gis Based Information Integration Framework for Dynamic Vehicle Routing and Scheduling, " *Proceedings of the IEEE International:Vehicle Electronics Conference*, Vol. 1, pp. 474-479, 1999.
- [27] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, " Security and Privacy Aspects of Low-cost Radio Identification Systems, " *Proc. International Conference on Security in Pervasive Computing*, pp. 454-469, 2003.
- [28] XML Key Management Specification , [29] XML Key Management Specification (XKMS), , 2001.
- [30] K. Yamada and M. Soga, " A Compact Integrated Visual Motion Sensor for ITS Applications, " *Proceeding of the IEEE: Intelligent Vehicles Symposium*, pp. 650-655, 2000.
- [31] S. Yoo, K. Lee, and K. Lee, " An XML-based mediation framework for seamless access to heterogeneous internet resources, " *Lecture Notes in Computer Science*, Vol. 797, pp.396-405, 2003.
- [32] M. Zolotarev, S. Farrell, " XML and PKI — What ' s the story? , " *Network Security*, Vol. 9, pp. 7-10, 2001.