# 適用車載網路之具容錯能力的可鑑別群體金鑰轉移機制

**蔡欣潔、NOTE**

E-mail: 345147@mail.dyu.edu.tw

## 摘 要

車載網路(Vehicular Ad-hoc Networks, VANETs)的應用範圍非常廣泛，如交通疏導、事故通知、防止碰撞，甚至救災通訊等等，若此車載網路遭受入侵攻擊，將會造成伺服器中斷服務，以及車輛間無法正常通訊，致使影響使用者的權利，故VANETs之通訊安全是一個非常重要的議題。為了保護VANETs通訊之安全，須要有安全的群體金鑰產生機制，但傳統群體金鑰產生機制大部分交由使用者建立，再傳送給所屬群組裡的其他使用者，此作法會造成使用者車輛之資源大量消耗。雖然亦有部份學者提出利用認證中心建立群體金鑰，再傳送給群組內的使用者，但其傳輸方式採逐一傳遞，故效率不佳，且由於車輛移動速度較快，當群組內成員皆收到群體金鑰時，群組部分成員早已脫離該群組。此外，該作法並無法達到使用者之間彼此的身份驗證，以及亦不能提供驗證群體金鑰是否正確，且該作法也無法針對封包在傳輸中發生缺漏或損毀時，提出有效機制維護使用者權利。因此，本論文提出可鑑別之群體金鑰轉移機制，由可信任的認證中心產生群體金鑰，並透過廣播方式轉移給群體內的使用者，同時亦可驗證使用者身分，以有效的提高通訊效率與防護通訊安全。此外，本機制亦具有容錯能力，能有效率排除惡意使用者，以及在封包損毀或不完整之情況下，本機制仍能正常運作而不影響使用者權利。

關鍵詞 : 金鑰認證、秘密分享、容錯機制、資訊安全、車載網路

## 目錄

### 參考文獻

Bernardos, C. J., Soto, I., Calderon, M., Boavida, F., & Azcorra, A. (2007), “ VARON: Vehicular Ad hoc Route Optimisation for NEMO, ” Computer Communications, 30, 1765-1784. Blakley, G. R. (1979), “ Safeguarding Cryptographic Keys, ” Proc. Am. Federation of Information Processing Soc. (AFIPS ’ 79) Nat ’ l Computer Conf., 48, 313-317. Chim, T. W., Yiu, S. M., Hui, L. C. K. & Li, V. O. K. (2011), “ SPECS: Secure and privacy enhancing communications schemes for VANETs, ” Ad Hoc Networks, 9, 189-203. Daeinabi, A., Rahbar, A. G. P. & Khademzadeh, A. (2011), “ VWCA: An efficient clustering algorithm in vehicular ad hoc networks, ” Journal of Network and Computer Applications, 34, 207-222. Diffie, W., & Hellman, M. E. (1976), “ New directions in cryptography, ” IEEE Transactions on Information Theory, 22(6), 644-654. ElGamal, T. (1985), “ A public key cryptosystem and a signature scheme based on discrete logarithms, ” IEEE Transactions on Information Theory, 31(4), 469-472. Ghosh, M., Varghese, A., Gupta, A., Kherani, A. A. & Muthaiah, S. N. (2010), “ Detecting misbehaviors in VANET with integrated root-cause analysis, ” Ad Hoc Networks, 8, 778-790. Housley, R., Ford, W., Polk, W. & Solo, D. (1999), “ Internet X.509 public key infrastructure certificate and CRL profile, ” IETF, RFC2459. Hubaux, J. P., Capkun, S. & Luo, J. (2004), “ The security and privacy of smart vehicles, ” IEEE Security & Privacy Magazine, 2(3), 49-55. Huang, D. & Verma, M. (2009), “ ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks, ” Ad Hoc Networks, 7, 1526-1535. Huang, K. H., Chung, Y. F., Lee, H. H., Lai, F. & Chen, T. S.

(2009), “ A conference key agreement protocol with fault-tolerant capability, ” Computer Standards & Interfaces, 31, 401-405. Isaac, J. T., Zeadally, S., Ca ’ mara, J. S. (2010), “ Security attacks and solutions for vehicular ad hoc networks, ” IET Communications, 4(7), 894-903. Jiang, Y., Lin, C., Shi, M., Shen, X. & Chu, X. (2007), “ A DoS and fault-tolerant authentication protocol for group communications in ad hoc networks, ” Computer Communications, 30, 2428-2441. Koblitz, N. (1987), “ Elliptic curve cryptosystems, ” Mathematics of Computation, 48(17), 203-209. Li, C. T., Hwang, M. S. & Chu, Y. P. (2008), “ A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, ” Computer Communications, 31, 2803-2814. Luo, J. & Hubaux, J. P. (2004), “ A survey of inter-vehicle communication, ” EPFL Technical Report IC, 24. Miller, V. S. (1986), “ Use of elliptic curves in cryptography, ” Proceedings of Advances in Cryptology: Crypto ’ 85, Springer- Verlag, 417-426. Oh, H., Yae, C., Ahn, D. & Cho, H. (1999), “ 5.8 GHz DSRC packet communication system for ITS services, ” in: Proceedings of the IEEE VTC ’ 99, September, 2223-2227. Patwardhan, A., Parker, J., Iorga, M., Joshi, A., Karygiannis, T. & Yesha, Y. (2008), “ Threshold-based intrusion detection in ad hoc networks and secure AODV, ” Ad Hoc Networks, 6, 578-599. Rivest, R., Shamir, A., & Adleman, L. (1978), “ A method for obtaining digital structures and public-key cryptosystem, ” Communication of ACM, 21(2), 120 – 126. Samara, G., Al-Salihy, W. A. H. & Sures, R. (2010), “ Security analysis of vehicular ad hoc networks (VANET), ” Second International Conference on Network Applications, Protocols and Services, 55-60. Seba, H., (2006), “ FTKM: A fault-tolerant key management protocol for multicast communications, ” computers & security, 25, 426-434. Shamir, A. (1979), “ How to Share a Secret, ” Comm. ACM, 22(11), 612-613. Sun, J. & Fang, Y. (2009), “ Defense against misbehavior in anonymous vehicular ad hoc networks, ” Ad Hoc Networks, 7, 1515-1525. Tsaur, W. J. (2005), “ Several security schemes constructed using ECC-based self-certified public key cryptosystems, ” Applied Mathematics and Computation, 168(1), 447-464. Wang, N. W., Huang, Y. M. & Chen, W. M. (2008), “ A novel secure communication scheme in vehicular ad hoc networks, ” Computer Communications, 31, 2827-2837. Yeh, L. Y., Chen, Y. C. & Huang, J. L. (2010), “ PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks, ” Computer Communications, 34(3), 447-456. Zhou, L., Zheng, B., Geller, B., Wei, A., Xu, S. & Li, Y. (2008), “ Cross-layer rate control, medium access control and routing design in cooperative VANET, ” Computer Communications, 31, 2870-2882.