Authenticated group key transfer scheme with fault-tolerant capability for vehicular ad hoc networks

蔡欣潔、NOTE

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

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) have a wide variety of applications, such as traffic control, incident notification, collision prevention, disaster relief communication, etc. While the VANETs have been attacked, inter-vehicle communications and the service of servers will be interrupted. In order to protect the communication security of VANETs, it is crucial to develop a group key generation scheme. The traditional group key generation scheme establishes a group key by a specific user, and then transmits it to other users in the group. This will result in huge resources consumption of the user vehicles. In addition, some scholars proposed establishing the group key with the help of the trusted authority (TA), and then transmitted it to other users within the group. However, the group key is transmitted to whole members one by one, so the above-mentioned schemes are inefficient. Furthermore, since the vehicles are moved so fast, some members have left the group when the group members receive the group key. In addition, the aforementioned schemes cannot achieve mutual authentication among users in the group, verify the correctness of the group key, and preserve users ’ rights when packets loss or damage in transmission occurs. Therefore, this paper proposes the authenticated group key transfer scheme to generate groups keys by TA, and then to broadcast to the whole group members. The proposed scheme cannot only verify the user ’ s identity, but also improve communication efficiency and enhance security protection. Moreover, our scheme also possesses the fault-tolerant ability, which can remove malicious users effectively and still operate well when the packets damage or loss occurs.

Keywords : Key Authentication、Secret Sharing、Fault-tolerant、Information Security、Vehicular Ad-hoc Networks

Table of Contents

摘要 .....i ...目錄 .....ii 圖目錄 .....iv 表目錄 .....v 第一章 緒論.....1 1.1 研究背景.....1 1.2 研究動機與目的.....3 1.3 研究流程.....5 1.4 研究架構.....6 第二章 文獻探討.....8 2.1 VANETs探討.....8 2.1.1 VANETs特性.....9 2.1.2 VANETs應用.....12 2.1.3 VANETs群體金鑰之相關研究.....14 2.2 公開金鑰密碼系統.....15 2.2.1 ECC為基礎的自我認證公開金鑰密碼系統.....16 2.3 秘密分享.....19 2.4 容錯機制.....21 第三章 車載網路環境之可鑑別的群體金鑰轉移機制...24 3.1 符號定義.....24 3.2 可鑑別群體金鑰轉移機制.....26 第四章 安全性與效能分析.....33 4.1 安全性分析.....33 4.2 效能分析.....39 第五章 結論與未來發展.....45 5.1 結論.....45 5.2 未來發展方向.....46 參考文獻.....47

REFERENCES

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.