階層群集式行動隨意網路之可證明安全的需求導向路由

白浩廷、曹偉駿

E-mail: 9608093@mail.dyu.edu.tw

摘 要

行動隨意網路（Mobile Ad Hoc Networks, MANETs）是一個臨時的、特殊的與無基礎設備的網路，由一群無線行動裝置，動態地建立其網路拓蹼，而不依靠任何集中式的管理裝置。在MANETs環境中，設備與設備之間必須執行路由協定來進行通訊，而且必須確保路由是安全的，如此才能保障較高層的通訊協定，不至於因底層的路由被瓦解而無法運作。因此，設計安全的路由是MANETs相當重要的議題。最近，已有許多學者提出相關的安全路由機制。然而，這些方法並不能夠確實地抵禦各式各樣的攻擊。因此，本論文基於階層群集式的架構，首先發展動態的群體金鑰管理機制，隨後基於所提之動態群體金鑰機制，建構出高安全的路由機制。此外，本論文利用可證明安全理論驗證所提之安全路由機制的安全性，並探討其優越性。總括來說，本論文所提機制在提升行動隨意網路的路由安全上是相當有用的。

關鍵詞 : 行動隨意網路，路由安全，金鑰管理，階層式群集，密碼系統，資訊安全

目錄

參考文獻

Acs, G., Buttyan, L., & Vajda, I. (2006). Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, 5 (11), 1533-1546. Argyroudis, P.G., & O'Mahony, D. (2005). Secure routing for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 7 (3), 2-21. Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002). An on-demand secure routing protocol resilient to byzantine failures. In D. Maughan & N.H. Vaidya (Eds.), Proceedings of the 3rd ACM workshop on Wireless security (pp. 21-30), Atlanta: ACM. Bellare, M., Canetti, R., & Krawczyk, H. (1998). Modular approach to the design and analysis of authentication and key exchange protocols. In J. Vitter (Eds.), Proceedings of the Annual ACM Symposium on Theory of Computing (pp. 419-428), Dallas: ACM. Brown, M., Hankerson, D., Lopez, J., & Menezes, A. (2001). Software implementation of the NIST elliptic curves over prime fields. In D. Naccache (Ed.), Proceedings of Progress in Cryptology - CT-RSA 2001: The Cryptographers' Track at RSA Conference, Lecture Notes in Computer Science (pp. 255-265), New York: Springer-Verlag. Burrows, J.H. (2000). Federal Information Processing Standard 186-2: Digital Signatur eStandard (DSS)

[Online]. Available: http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf [2007, January 10]. Burrows, M., Abadi, M., & Needham, R. (1990). Logic of authentication. ACM Transactions on Computer Systems, 8 (1), 18-36. Chatterjee, M., Das, S.K., & Turgut, D. (2000). On-demand weighted clustering algorithm (WCA) for ad hoc networks. In H. Krawczyk (Ed.), Proceedings of IEEE Global Telecommunications Conference (1697-1701), San Francisco: IEEE. Deng, H., Li, W., & Agrawal, D.P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40 (10), 70-75. Desmedt, Y., & Frankel, Y. (1993). Threshold cryptosystems. In N. Koblitz (Ed.), Proceedings of AUSCRYPT '92, Lecture Notes in Computer Science (pp. 1-14), New York: Springer-Verlag. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22 (3), 644-654. Djenouri, D., Khelladi, L., & Badache, N. (2005). A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys & Tutorials, 7 (4), 2-28. Douceur, J.R. (2002). The Sybil attack. In P. Druschel, M. F. Kaashoek, & A.I.T. Rowstron (Eds.), Proceedings of Peer-to-Peer Systems: First Interna-tional Workshop (IPTPS), Lecture Notes in Computer Science (pp. 251-260), New York: Springer-Verlag. Girault, M. (1992). Self-certified public keys. In D. Davies (Ed.), Proceedings of EUROCRYPT ’ 91, Lecture Notes in Computer Science (pp. 490-497), New York: Springer-Verlag. Gupta, V., Gupta, S., Chang, S., & Stebila, D. (2002). In D. Maughan & N. H. Vaidya (Eds.), Performance analysis of elliptic curve cryptography for SSL. Proceedings of the Workshop on Wireless Security (pp. 87-94), Atlanta: ACM. Hong, F., Hong, L., & Fu, C. (2005). Secure OLSR. In V. Varadharajan (Ed.), Proceedings of International Conference on Advanced Information Networking and Applications (pp. 713-718), New York: IEEE. Hu, Y.C., Johnson, D.B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1 (1), 175-192. Hu, Y.C., & Perrig, A. (2004). A survey of secure wireless ad hoc routing. IEEE Security and Privacy, 2 (3), 28-39. Hu, Y.C., Perrig, A., & Johnson, D.B (2003). Packet leashes: A defense against wormhole attacks in wireless networks. In E. Shi (Ed.), Proceedings of IEEE INFOCOM (pp. 1976-1986), New York: IEEE. Hu, Y.C., Perrig, A., & Johnson, D.B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 11 (1-2), 21-38. Hu, Y.C., Perrig, A., & Johnson, D.B. (2006). Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications, 24 (2), 370-380. Imielinski, T., & Navas, J.C. (1999). GPS-Based Geographic Addressing, Routing, and Resource Discovery. Communications of the ACM, 42 (4), 86-92. Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., & Viennot, L. (2001). Optimized link state routing protocol for ad hoc networks. In D. Davies (Ed.), Proceedings of IEEE International Topic Conference (pp. 62-28), New York: IEEE. Jeng, F.G., & Wang, C.M. (2006). An efficient key-management scheme for hierarchical access control based on elliptic curve cryptosystem. Journal of Systems and Software, 79 (8), 1161-1167. Ji, X.J., Tian, C. & Zhang, Y.S. (2006). Secure DSR routing protocol analysis and design. Tongxin Xuebao/Journal on Communication, 27 (3), 136-140. Johnson, D.B., Maltz, D.A., Hu, Y. & Jetcheva, J.G. (2002). IETF Internet Draft: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt[2007, January 11]. Kanayama, N., Kobayashi, T., Saito, T., & Uchiyama, S. (2000). Remarks on elliptic curve discrete logarithm problems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E83-A (1), 17-23. Keung, S., & Siu, K.Y. (1995). Efficient protocols secure against guessing and replay attacks. In H. Krawczyk (Ed.), Proceedings of the International Conference on Computer Communications and Networks (pp. 105-112), New Jersey : IEEE. Kim, J., & Tsudik, G. (2005). SRDP: Securing route discovery in DSR. In D.B. Johnson & Z. Haas (Eds.), Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (pp. 247-258), New York: IEEE. Lauter, K. (2004). The advantages of elliptic curve cryptography for wireless security. IEEE Wireless Communications, 11 (1), 62-67. Marti, S., Giuli, T.J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In R. Pickholtz, S. K. Das, R. Caceres, & J. J. Garcia-Luna-Aceves (Eds.), Proceedings of the Annual International Conference on Mobile Computing and Networking (pp. 255-265), Boston: ACM. Milanovic, N., Malek, M., Davidson, A., & Milutinovic, V. (2004). Routing and security in mobile ad hoc networks. Computer, 37 (2), 61-65. Murphy, S. (2002). IETF Internet Draft: Routing protocol threat analysis [Online]. Available: http://www.ietf.org/ internet- drafts / draft-murphy-threat-00.txt [2007, January 11]. Papadimitratos, P., & Haas, Z.J. (2005). Secure on-demand distance vector routing in ad hoc networks. In P. Druschel & M.F. Kaashoek (Eds.), Proceedings of IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication (pp. 168-171), New York: IEEE. Performance of RSA on ARM and Palm [Online]. Available: http://www.digisec.se/mcrypt_performance.htm [2007, January 12]. Perkins, C.E., & Bhagwat, P. (1994). Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In J. Crowcroft (Ed.), Proceedings of the conference on Communications architectures, protocols and applications (pp. 234-244), London: ACM. Perkins, C.E., & Royer, E.M. (1999). Ad-hoc on-demand distance vector routing. In I.F. Akyildiz, J.Y.B. Lin, & R. Jain (Eds.), Proceedings of second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100), New Orleans: IEEE. Perrig, A., Canetti, R., Tygar, J.D., & Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. In D.T. Lee & B.S. Lin (Eds.), Proceedings of the IEEE Symposium on Security and Privacy (pp. 56-73), New Jersey: IEEE. Pfitzmann, B., & Waidner, M. (2001). A model for asynchronous reactive systems and its application to secure message transmission. In S. K. Das & R. Caceres (Eds.), Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy (pp. 184-200), Oakland: IEEE. Rafaeli, S., & Hutchison, D. (2003). A survey of key management for secure group communication. ACM Computing Surveys, 35 (3), 309-329. Ramanujan, R., Ahamad, A., Bonney, J., Hagelstrom, R., & Thurber, K. (2000). Techniques for Intrusion-resistant Ad Hoc Routing Algorithms (TIARA). In J. Forlizzi, J. Lee, & S. Hudson (Eds.), Proceedings of IEEE Military Communications Conference MILCOM (pp. 660-664). New York: IEEE. Royer, E.M., & Toh, C.K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications, 2 (6), 46-55. Sanzgiri, K., Laflamme, D., Dahill, B., Levine, B.N., Shields, C., & Belding-Royer, E.M. (2005). Authenticated routing for ad hoc networks. IEEE Journal on Selected Areas in Communications, 23 (3), 598-609.

Shamir, A. (1979). How to share a secret. Communications of the ACM, 22 (11), 612-613. Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In S. Cui, P. Duan, & C.W. Chan (Eds.), Proceedings of CRYPTO 84, Lecture Notes in Computer Science (pp. 47-53), New York: Springer-Verlag. Solinas, J. (1999). Generalized mersenne numbers [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/1999 /corr99-39.ps [2007, January 12]. Stallings, W. (2005). Cryptography and Network Security Principles and Practices (4rd ed.). New York: Prentice Hall. Tsaur, W.J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. Applied Mathematics and Computation, 168 (1), 447-464. Valle, G., & Cardenas, R.G. (2005). Overview the key management in ad hoc networks. In L. Xu & L. Korba (Eds.), Proceedings of Advanced Distributed Systems, Lecture Notes in Computer Science (pp. 397-406), New York: Springer-Verlag. Wu, B., Wu, J., Fernandez, E.B., Ilyas, M., & Magliveras, S. (2007). Secure and efficient key management in mobile ad hoc networks. Journal of Network and Computer Applications, 30 (3), 937-954. Wu, J., & Stojmenovic, I. (2004). Ad Hoc Networks. Computer, 37(2), 29-31. Wu, K.P., Ruan, S.J., & Tseng, C.K. (2001). Hierarchical access control using the secure filter. IEICE Transactions on Information and Systems, E84-D (6), 700-708. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks challenges and solutions. IEEE Wireless Communications, 11 (1), 38-47. Yi, S., Naldurg, P., & Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. In N.H. Vaidya, M.S. Corson, & S.R. Das (Eds.), Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing (pp. 299-302). Long Beach: ACM. Yu, J.Y., & Chong, P.H.J. (2005). A survey of clustering schemes for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 7 (1), 32-48. Zhang, C., Zhou, M.C., & Yu, M. (2006). Ad hoc network routing and security: a review. International Journal of Communication Systems, Article in Press. Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Securing mobile ad hoc networks with certificateless public keys. IEEE Transactions on Dependable and Secure Computing, 3 (4), 386-399. Zhen, J., & Srinivas, S. (2003). Preventing replay attacks for secure routing in ad hoc networks. In J. Pieprzyk & H. Ghodosi (Eds.), Proceedings of Ad-Hoc, Mobile, and Wireless Networks, Lecture Notes in Computer Science (pp. 140-150), New York: Springer-Verlag.