階層叢集式行動隨意網路之動態存取控制機制

黃南翔、曹偉駿

E-mail: 9806282@mail.dyu.edu.tw

摘 要

群組計算及通訊的應用，刺激行動隨意網路對群組存取控制的需求。由於動態的成員關係以及缺乏認證中心，這些因素造成行動隨意網路的存取控制更具挑戰。近年來，一些學者試圖以驗證門檻式簽章的方法，提出應用於行動隨意網路的群組存取控制機制。然而鄰近節點數量若小於機制所定的門檻值，則無法使用門檻式簽章，導致未能滿足行動隨意網路的動態環境。本研究基於高彈性的階層叢集式架構，並且結合有效率的橢圓曲線密碼系統(Elliptic curve cryptosystem, ECC)及安全的濾器技術 (Secure Filter)，提出一套適用於行動隨意網路的群組存取機制，以解決現有使用門檻式簽章的存取控制機制所遭遇之困難。在我們所提的機制中，當群組的成員關係發生改變時，藉由更新少數叢集頭的安全過濾器即可達成安全的群組存取控制。換句話說，本機制確保資料只有經認證的使用者才能存取，且叢集頭能存取其下層群組之資料，亦即，最重要的是能防止權限低的節點存取權限高的節點內容。

關鍵詞 : 網路安全、群組存取控制、階層式叢集、行動隨意網路

目錄

參考文獻

Akl, S.G., & Taylor, P.D. (1983). Cryptographic Solution to a Problem of Access Control in a Hierarchy. ACM Transactions on Computer Systems, 1(3), 239 – 247.Balachandran, R. K., Zou, X. K., Ramamurthy, B., Thukral, A., & Variyam, V. N. (2008). An Efficient and

Attack-resistant Key Agreement Scheme for Secure Group Communications in Mobile Ad-hoc Networks. Wireless Communications & Mobile Computing, 8(10), 1297-1312.Chang, C. C., Lin, I. C., Tsai, H. M., & Wang, H. H. (2004). A key assignment scheme for controlling access in partially ordered user hierarchies. Proceedings of the 18th IEEE International Conference on Advanced Information Networking and Applications (pp. 376 – 379).Chang, C.C., Hwang, R.J., & Wu, T.C. (1992). Cryptographic key Assignment Scheme for Access Control in a Hierarchy. Information Systems, 17(3), 243 – 247.Chang, C.C., & Buehrer, D.J. (1993). Access Control in a Hierarchy Using a One-way Trapdoor Function. Computers and Mathematics with Applications, 26(5), 71 – 76.Cheng, B. C., Chen, H., & Tseng, R. Y. (2008). A Good IDS Response Protocol of MANET Containment Strategies. IEICE Transactions on Communications, E91B(11), 3657-3666.Chick, G.C., & Tavares, S.E. (1990). Flexible Access Control With Master Keys. Lecture Notes in Computer Science, 3295 , 316 – 322.Chou, J. S., Chen, Y. L., & Chen, T. H. (2008). An Efficient Session key Generation for NTDR Networks Based on Bilinear Paring. Computer Communications, 31(14), 3113-3123.Chung, Y. F., Lee, H. H., Lai, F. P., & Chen, T. S. (2008). Access control in user hierarchy based on elliptic curve cryptosystem. Information Sciences, 178, 230-243.Fourati, A., & Al Agha, K. (2008). Detecting Forged Routing Messages in Ad Hoc Networks. Telecommunication Systems, 39(3-4), 205-214.Frey, G., & Ruck, H. (1994). A Remark Concerning m-divisibility and the Discrete Logarithm in The Divisor Class Group of Curves. Mathematics of Computation, 62, 865-874.Hwang, M. S., & Yang, W. P. (2003). Controlling access in large partially-ordered hierarchies using cryptographic keys. Journal of Systems and Software, 67(2), 99 – 107.Jarecki, S., Saxena, N., & Yi. J. H. (2004). An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (pp. 1-9).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, 1161 – 1167.Kannhavong, B., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). A Study of a Routing Attack in OLSR-based Mobile Ad Hoc Networks. International Journal of Communication Systems, 20(11), 1245-1261.Kim, Y., Mazzocchi, D., & Tsudik, G. (2003). Admission Control in Peer Groups. Proceedings of Second IEEE International Symposium on Network Computing and Applications (pp. 131-139).Kong, J., Luo, H., Xu, K., Gu, D.L., Gerla, M., & Lu, S. (2002). Adaptive Security for Multilevel Ad Hoc Networks. Wireless Communications and Mobile Computing, 2(5), 533-547.Lu, F., & Zhou, T. (2006). Research on Identity-based Cluster Access Control Model with Dynamic Trust Agent for Mobile Ad Hoc Networks. Processdings of International Conference on Wireless Communications, Networking and Mobile Computing (pp. 1-5).Luo, H. Y., Kong, J. J., Zerfos, P., Lu, S. W., & Zhang, L. X. (2004). URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks. IEEE-ACM Transactions on Networking, 12(6), 1049-1063.Mackinnon, S.T., Taylor, P.D., Meijer, H., & Akl, S.G. (1985). An Optimal Algorithm for Assigning Cryptographic Keys to Control Access in a Hierarchy. IEEE Transactions on Computers, C-34(9), 797 – 802.Menezes, A., Okamoto, T., Vanstone, S. (1993). Reducing Elliptic Curve Logarithms to Logarithms in a Finite-field. IEEE Transactions on Information Theory, 39(5), 1639-1646.Oorschot, P., & Wiener, M. (1999). Parallel Collision Search With Cryptanalysis Applications. Journal of Cryptology, 12, 1-28.Otrok, H., Mohammed, N., Wang, L. Y., Debbabi, M., & Bhattacharya, P. (2008). A Game-theoretic Intrusion Detection Model for Mobile Ad Hoc Networks. Computer Communications, 31(4), 708-721.Peng, W. X., Wang, Y. L., Park, E. K., & Makki, K. (2007). Dynamic Key Management for Secure Routing in MANET. Wireless Communications & Mobile Computing, 7(10), 1233-1241.Pollard, J. M. (1978). Monte Carlo Methods for Index Computation mod P. Mathematics of Computation, 32, 918-924.Pohlig, S. C., & Hellman M. E. (1978). An Improved Algorithm Over GF(p) and its Eryptographie Significance. IEEE Transaction on Information Theory, 24, 106-110.Pucha, H., Das, S. M., & Hu, Y. C. (2007). The Performance Impact of Traffic Patterns on Routing Protocols in Mobile Ad Hoc Networks. Computer Networks, 51(12), 3595-3616.Satoh, T. & Araki, K. (1998). Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves. Commentarii Mathematici Universitatis Sancti Pauli, 47, 81-92.Saxena, N., Tsudik, G., & Yi, J. H. (2005). Identity-based Access Control for Ad Hoc Groups. Lecture Notes in Computer Science, 3056, 326- 379.Saxena, N., Tsudik, G., & Yi, J. H. (2009). Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs. IEEE Transactions on Parallel and Distributed Systems, 20(2), 158-170.Semaev, I. (1998). Evaluation of Discrete Logarithm of Group if p-torsion Points of An Elliptic Curve in Characteristic p. Mathematics of Computation, 67, 353-356.Smart, N. (1999). The Discrete Logarithm Problem on Elliptic Curves of Trace Ons. Journal of Cryptology, 12, 193-196Trung, H. D., Benjapolakul, W., & Duc, P. M. (2007). Performance Evaluation and Comparison of Different Ad Hoc Routing Protocols. Computer Communications, 30(11-12), 2478-2496.Tsaur, W.J. (2005). Several Security Schemes Constructed Using ECC-based Self-certified Public Key Cryptosystems. Applied Mathematics and Computation, 168 (1), 447-464.Tsaur, W. J., & Pai, H. T. (2007). Dynamic Key Management Schemes for Secure Group Communication Based on Hierarchical Clustering in Mobile Ad Hoc Networks. Lecture Notes in Computer Science, 4743, 475 – 484.Tsaur, W. J., & Pai, H. T. (2007). A Secure On-Demand Source Routing Scheme Using Hierarchical Clustering in Mobile Ad Hoc Networks. Lecture Notes in Computer Science, 4743, 513 – 522.Tzeng, W. G. (2002). A Time-bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy. IEEE Trandactions on Knowledge and Data Engineering, 14(1), 182-188.Wang , N. C., & Fang, S. Z. (2007). A Hierarchical Key Management Scheme for Secure Group Communications in Mobile Ad Hoc Networks. Journal of Systems and Software, 80, 1667 – 1677.Wang, S. M., Tao, R., Xu, K., & Wang, Y. (2008). A New Key Management Protocol to MANET. Chinese Journal of Electronics, 17(3), 513-519.Wu, J., & Stojmenovic, I. (2004). Ad Hoc Networks. Computer, 37(2), 29-31.Wu, K. P., Ruan, S. J., Tseng, C. K., & Lai, F. P., (2001). Hierarchical Access Control Using the Secure Filter. IEICE Transactions on Information & Systems, E84-D(6), 700 – 707.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., & Wei, R. (2006). An access control scheme for partially ordered set hierarchy with provable security. Lecture Notes in Computer Science, 3897,

221-232.Yang, H., Luo, H. Y., Ye, F., Lu, S. W., & Zhang, L. X. (2004). Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, 11(1), 38-47.Yeh, J. H. (2008). A Secure Time-bound Hierarchical Key Assignment Scheme Based on RSA Public Key Cryptosystem. Information Processing Letters, 105, 117 – 120.Yi, P., Jiang, X. H., Wu, Y., & Liu, N. (2008). Distributed Intrusion Detection for Mobile Ad Hoc Networks. Journal of Systems Engineering and Electronics, 19(4), 851-859.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, 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.Zhou, L., & Haas, Z. J. (1999). Securing Ad Hoc Networks, IEEE Network, 13(6), 24-30.