A Small-World Key Management for Wireless Sensor Networks

Yung-Tsung Hou*, Chia-Mei Chen, and Bingchiang Jeng

Department of Information Management,

National Sun Yat-Sen University,

Kaohsiung, Taiwan

yungtsung.hou@gmail.com, {cmchen, jeng}@mis.nsysu.edu.tw

Received 9 December 2008; Revised 6 March 2009; Accepted 29 March 2009

Abstract. Most of wireless sensor networks (WSNs) are deployed in hostile environments where communication between sensors may be monitored. For applications that require higher data security, employing some cryptographic scheme is therefore necessary in the networks. However, key management in WSNs is a challenging task due to resource constraints on sensor nodes. In this paper, based on the concept of small worlds, we present a group-based key pre-distribution scheme which enables any pair of sensors to establish a unique shared key. The proposed method for key path establishment uses only local information with logarithmic memory overhead to the number of groups. We also evaluate other performance aspects, including communication and computing overhead. The analysis and simulation results show that the proposed key management method performs better than other known methods.

Keywords: key management, key pre-distribution, small worlds, sensor networks

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, 2002.

[2] L. Eschenauer and V. Gligor, "A Key-management Scheme for Distributed Sensor Networks," *Proceedings of the 9th ACM Conference on Computer and Communication Security*, Washington, DC, USA, pp. 41-47, 2002.

[3] H. Chan, A. Perrig, D. Song, "Random Key Pre-distribution Schemes for Sensor Networks," *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, California, USA, pp. 197-213, 2003.

[4] W. Du, J. Deng, Y. S. Han, S. Chen, P. Varshney, "A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge," *Proceedings of IEEE INFOCOM* 2004, pp. 590-597, 2004.

[5] D. Huang, M. Mehta, D. Medhi, L. Harn, "Location-aware Key Management Scheme for Wireless Sensor Networks," *Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks*, pp. 29-42, 2004.

[6] Z. Yu and Y. Guan, "A Key Pre-distribution Scheme using Deployment Knowledge for Wireless Sensor Networks," *Proceedings of ACM/IEEE International Conference on Information Processing in Sensor Networks*, pp. 261-268, 2005.

[7] S. Milgram, "The Small World Problem," *Psychology Today*, Vol. 61, No. 1, pp. 60-67, 1967.

[8] D. Watts and S. Strogatz, "Collective Dynamics of Small-world Networks," *Nature*, Vol. 393, pp. 440-442, 1998.

[9] S. A. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, Vol. 15, No. 2, pp. 346-358, 2007.

[10] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 2, pp. 228-258, 2005.

[11] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 1, pp. 41-77, 2005.

* Correspondence author

[12] D. Liu, P. Ning, W. Du, "Group-based Key Predistribution for Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, Vol. 4, No. 2, 2008.

[13] H. Chan and A. Perrig, "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks," *Proceedings of IEEE INFOCOM 2005*, Miami, USA, pp. 524-535, 2005.

[14] C. Korte and S. Milgram, "Acquaintance Networks between Racial Groups: Application of the Small World Method," *Journal of Personality and Social Psychology*, Vol. 15, No. 2, pp. 101-108, 1978.

[15] J. Travers and S. Milgram, "An Experimental Study of the Small World Problem," *Sociometry*, Vol. 32, No. 4, pp. 425-443, 1969.

[16] L. A. N. Amaral, A. Scala, M. Barthelemy, H. E. Stanley, "Classes of Small World Networks," *PNAS*, Vol. 97, No. 21, pp. 11149-11152, 2000.

[17] J. Kleinberg, "The Small-world Phenomenon: An Algorithm Perspective," *Proceedings of 32nd ACM Symposium on Theory of Computing*, Portland, Oregon, USA, pp. 163-170, 2000.

[18] B. Ghosh, "Random Distances within a Rectangle and between Two Rectangles," *Bulletin of the Calcutta Mathematical Society*, Vol. 43, pp. 17-24, 1951.

[19] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *Proceedings of the 6th Annual International Conference on Mobile Computing and Networkin*g, pp.56-67, 2000.

[20] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," *Proceedings of the Sixth International Conference on Mobile Computing and Networking*, Boston, Massachusetts, USA, pp. 243-254, 2000.