KYBERNETIKA — VOLUME 44 (2008), NUMBER 4, PAGES 522-533

A Chaos-Based Secure Cluster Protocol for Wireless Sensor Networks

Qian Fang; Ying Liu; Xiaoqun Zhao

Abstract: Security mechanisms for wireless sensor networks (WSN) face a great challenge due to the restriction of their small sizes and limited energy. Hence, many protocols for WSN are not designed with the consideration of security. Chaotic cryptosystems have the advantages of high security and little cost of time and space, so this paper proposes a secure cluster routing protocol based on chaotic encryption as well as a conventional symmetric encryption scheme. First, a principal-subordinate chaotic function called N-Logistic-tent is proposed. Data range is thus enlarged as compared to the basic Logistic map and the security is enhanced. In addition, the computation is easier, which does not take much resource. Then, a secure protocol is designed based on it. Most of communication data are encrypted by chaotic keys except the initialization by the base station. Analysis shows that the security of the protocol is improved with a low cost, and it has a balance between resource and security.

Keywords: wireless sensor network; security; chaotic encryption; cluster;

AMS Subject Classification: 90B18; 74H65; 68M12;

References

[1] G. Huang and Y. Zhou: MANET security communication model based on multistage chaotic encryption. Comput. Engrg. Appl. 3 (2006), 136–139.

[2] K. Kelber: General design rules for chaos-based encryption systems. Internat. Symposium on Nonlinear Theory and its Applications 1 (2005), 465–468.

[3] S. Liu, F. Liang, and G. Xin: Chaos and Fractal in Natural Science. Beijing: Publishing House of Beijing University 2003, pp. 16–53.

[4] J. Luo and H. Shi: Research of chaos encryption algorithm based on logistic mapping. In: Internat. Conference Intelligent Information Hiding and Multimedia Signal Processing 2006, pp. 381–383.

[5] J. Lv, J. Lu, and S. Chen: Chaos Time Series Analysis and its Applications. Wuhan: Publishing House of Wuhan University 2002, pp. 72–92.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar: SPINS: Security protocols for sensor networks. Wireless Networks 8 (2002), 5, 521–534.

[7] G. Plitsis: Performance of the application of chaotic signals in IEEE 802.11b and wireless sensor networks. In: Proc. Seventh IEEE Internat. Symposium on Computer Networks. 2006.

[8] Y. Wang, G. Attebury, and B. Ramamurthy: A survey of security issues in wireless sensor networks. IEEE Comm. Surveys & Tutorials 8 (2006), 2, 2–23.

[9] H. Yu, P. Zeng, and W. Liang: Intelligent Wireless Sensor Network System. Beijing: Publishing House of Science 2006, pp. 126–132.

[10] C. Zhu and Z. Chen: A fast combined chaotic cryptographic method fitting mobile computing. Comput. Engrg. 31 (2005), 1, 138–140.