P.O.Box 8718, Beijing 100080, China	Journal of Software May 2007,18(5):1232-1245
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2006 by *Journal of Software*

A Reliable Pairwise Key-Updating Scheme for Sensor Networks

WEN Mi, CHEN Ke-Fei, ZHENG Yan-Fei, LI Hui

Full-Text PDF Submission Back

WEN Mi1, CHEN Ke-Fei1,2, ZHENG Yan-Fei1,2, LI Hui1,
1(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)
2(School of Information Security and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)
Authors information: WEN Mi was born in 1979. She is a Ph.D. student of Shanghai Jiaotong University. Her current research areas are security in wireless sensor networks, etc. CHEN Ke-Fei was born in 1959. He is a professor of Shanghai Jiaotong University. His research areas are classical and modern cryptography, etc. ZHENG Yan-Fei was born in 1976. She is a lecturer of Shanghai Jiaotong University. Her research areas are wireless sensor networks, etc. LI Hui was born in 1977. He is a Ph.D. student of Shanghai Jiaotong University. His current research areas are wireless sensor networks, etc.
Corresponding author: WEN Mi, Phn: +86-21-34205539, Fax: +86-21-34204405, E-mail: superwm@sjtu.edu.cn, http://cis.sjtu.edu.cn
Received 2006-12-29; Accepted 2007-02-14

Abstract
This paper proposes a reliable pairwise key-updating (RPKU) scheme for clustered WSNs via predistribution and local collaboration approaches. Based on the modified version of Blom's matrix construction, this scheme can extend and shrink the pairwise keys in WSNs with the network topology changes. This scheme also presents a hierarchical key distribution method in the clustered WSNs, guaranteeing that any pair of neighboring nodes can find a common secret key between themselves. Comparison and simulation results show that the proposed scheme outperforms most of the existing pairwise key establishment schemes in terms of network security, key connectivity and scalability.

Wen M, Chen KF, Zheng YF, Li H. A reliable pairwise key-updating scheme for sensor networks. *Journal of Software*, 2007,18(5):1232-1245.
DOI: 10.1360/jos181232
http://www.jos.org.cn/1000-9825/18/1232.htm

摘要
提出了一种基于预分发和协作的可靠的对密钥更新方案RPKU(reliable pairwise key-updating).借助于一种改进的Blom密钥矩阵构造方法,该方案能够随着网络的动态变化而动态伸缩各个节点的密钥信息,从而解决了由于节点被攻击所导致的密钥泄漏和密钥连通性下降等问题.该方案还提出了一种基于分簇型传感器网络结构的密钥预分发方法,使得任意两个相邻节点间都能建立一个对密钥.仿真结果表明,与已有的密钥方案相比,该方案在安全性、密钥连通性和扩展性等方面都具有明显的优势.

基金项目：Supported by the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant No.20050248043 (高等学校博士学科点专项科研基金)

References:

[1] Tilak S, Abu-Ghazaleh NB, Heinzelman W. A taxonomy of wireless microsensor network models. ACM Mobile Computing and Communications Review, 2002,6(2):28-36.

[2] Blom R. An optimal class of symmetric key generation systems. In: Beth T, Cot N, Ingemarsson I, eds. Advances in Cryptology—EUROCRYPT'84. LNCS 209, Berlin, Heidelberg: Springer-Verlag, 1985. 335-338.

[3] Blundo C, Santis AD, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-Secure key distribution for dynamic conferences. LNCS 740, Berlin, Heidelberg: Springer-Verlag, 1993. 471-486.

[4] Choi1 SJ, Youn1 HY. An efficient key predistribution scheme for secure distributed sensor networks. In: Enokido T, et al., eds. EUC Workshops 2005. IFIP Int'l Federation for Information Processing. LNCS 3823, 2005. 1088-1097.

[5] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conf. on Computer and Communication security. Washington: ACM Press. 2002. 41-47.

[6] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proc. of the 2003 IEEE Symp. on Security and Privacy (SP 2003). Berkeley, 2003. 197-213.

[7] Du W, Deng J, Han YS, Varshney PK. A pairwise key pre-distribution scheme for wireless sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washingtion: ACM Press, 2003. 42-51.

[8] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. ACM Trans. on Information and System Security, 2005, 8 (1):41-77.

[9] MacWilliams FJ, Sloane N. The Theory of Error-Correcting Codes. North Holland, 1997.

[10] Du W, Deng J, Han YS, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge. In: Proc. of the IEEE INFOCOM 2004. Hong Kong: IEEE Press, 2004. 586-597.

[11] Camtepe SA, Yener B. Key distribution mechanisms for wireless sensor networks: A Survey. Technical Report, TR-05-07, Rensselaer Polytechnic Institute, 2005.

[12] Carman D, Kruus P, Matt B. Constraints and approaches for distributed sensor networks security. Technical Report, 00-010. NAI Labs, 2000.

[13] Wang G, Zhang W, Cao G, La Porta T. On supporting distributed collaboration in sensor networks. In: Proc. of the IEEE Military Communications Conf. (MILCOM). Boston: IEEE Press, 2003. 752-757.

[14] Shaneck M, Mahadevan K, Kher V, Kim YD. Remote software-based attestation for wireless sensors. In: Proc. of the 2nd European Workshop (ESAS 2005). LNCS 3813, Visegrad: Springer-Verlag, 2005. 27-41.

[15] Jolly G, Kuscu MC, Kokate P, Yuonis M. A low-energy management protocol for wireless sensor networks. In: Proc. of the 8th IEEE Int'l Symp. on Computers and Communication (ISCC 2003). Turkey, 2003. 335-340.

[16] Zhao YJ, Govindan R, Estrin D. Residual energy scans for monitoring wireless sensor networks. In: Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC 2002). Orlando: IEEE Press, 2002. 356-362.

[17] Ren FY, Huang HN, Lin C. Wireless sensor networks. Journal of Software, 2003,14(7):1282-1291 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm

[18] Cheng Y, Agrawal DP. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. Ad Hoc Networks, 2007,5(1):35-48.

附中文参考文献:

[17] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282-1291. http://www.jos.org.cn/1000-9825/14/1282.htm