Mathematical Problems of Computer Science 33, 127–134, 2010.

Data Encryption, Authentication and Key Predistribution Schemes for Wireless Sensor Networks

Ara Alexanian, Hakob Aslanyan and Armen Soghoyan

Yerevan State University

Abstract

This paper investigates some security aspects of wireless sensor networks. Particularly symmetric encryption, authentication and key predistribution schemes are proposed. Encryption and authentication schemes are based on a secret key which is a table of strong generators of a permutation group (as per Sims algorithm). The ciphertext of a plaintext of size N is a single permutation over $n = 2N + 1$ elements. Encryption/Decryption processes are simple and easy to perform for a wireless node with limited abilities.

Key predistribution scheme deals with all the node and network limitations and requirements existing in wireless sensor networks and gives a secure key predistribution scheme under the assumption that nodes are not physically captured for t_0 time after being deployed, where t_0 is time necessary for invoking the key establishment phase of proposed scheme, which is in practice should be some seconds.

References

[1] Yee Wei Law, Jeroen Doumen and Pieter Hartel, "Survey and benchmark of block ciphers for wireless sensor networks", *ACM Transactions on Sensor Networks TOSN*, vol. 2, number 1, pp. 65-93, 2006.

[2] R. Rivest, "The RC5 Encryption Algorithm", 1994 Leuven Workshop on Fast Software Encryption, Springer-Verlag, pp. 86-96, 1995.

[3] R. Rivest, M. Robshaw, R. Sidney and Y. Yin, "The RC6^{TM} Block Cipher. Specification version 1.1", 1998.

[4] J. Daemen and V. Rijmen, AES Proposal: Rijndael, 1999.

[5] M. Matsui, "New Block Encryption Algorithm MISTY", *Fast Software Encryption, 4th International Workshop, FSE 97*, vol. 1267 of LNCS.,Springer-Verlag, pp. 54-68, 1997.

[6] 3rd Generation Partnership Project, "Specification of the 3GPP Confidentiality and Integrity Algorithms Document 2", KASUMI Specification. ETSI/SAGE, Specification Version: 1.0, 1999.

[7] K. Aoki, T. Ichikawa, M. Matsui, S. Moriai, J. Nakajima and T. Tokita, "Specification of Camellia. A 128-Bit Block Cipher", Nippon Telegraph and Telephone Corporation and Mitsubishi Electric Corporation, Specification Version 2.0, 2001.

[8] A. Perrig, R. Szewczyk , V. Wen and et al., "SPINS: security protocols for sensor networks", *Journal of Wireless Networks*, vol. 8, number 2, pp. 521-534, 2002.

[9] C. Karlof ,N. Sastry and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", *Proceedings of the 2nd International Conference & Embedded Networked Sensor Systems*, Baltimore, USA, 2004.

[10] J.N. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: A survey", *IEEE Wireless Communications.*, vol. 11, number 6, pp. 6-28, 2004.

[11] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, number 6, pp. 644-654, 1976..

[12] R. L. Rivest, A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, number 2, pages 120-126, 1978.

[13] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks", *Proceedings of the 9th ACM Conference on Computer and Communication Security*, pages 41-47, 2002.

[14] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pp. 197-213, 2003.

[15] S. A. Camtepe and B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, *IEEE/ACM Transactions on Networking (TON)*, vol. 15, number 2, pp. 346-358, 2007.

[16] Y. Xiao, V. Krishna Rayi, Bo Sun, X. Du, Fei Hu and M. Galloway, "A survey of key management schemes in wireless sensor networks", *Computer Communications*, vol. 30, number 11-12, pp. 2314-2341, 2007.

[17] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks', *Wireless Sensor Networks*, T. Znati et al., eds, 2004.

[18] A. Alexanyan, Algebra (Groups, Rings, Fields), Yerevan University Publisher, In Armenian, 2006,.

[19] M. Brown, D. Cheung, D. Hankerson, J. L. Hernandez, M. Kirkup and A. Menezes, "PGP in constrained wireless devices", *9th USENIX Security Symposium*, 2000.

[20] D. W. Carman, P.S. Kruus and B. J. Matt., "Constraints and approaches for distributed sensor networks security", NAI Lab, September, number 00-010, 2000.

[21] Serege Lang, Algebra, Springer Science+Business Media, Inc., 2002.

[22] B.L Van der Varden, Algebra, Springer Verlag, 1968.

Անլար սենսորային ցանցերի տվյալների ծածկագրման, ինքնության հաստատման և բանալիների բաշխման սխեմաներ համար

Ա. Ալեքսանյան, Հ. Ասլանյան և Ա. Սողոյան

Ամփոփում

Աշխատանքում դիտարկված են անլար սենսորային ցանցերի ապահովությանը վերաբերող որոշ խնդիրներ: Մասնավորապես առաջարկվում են տվյալների սիմետրիկ ծածկագրման, ինքնության հաստատման և բանալիների բաժանման սխեմաներ: Ծածկագրման և ինքնության հաստատման սխեմաների բանալի է հանդիսանում տեղադրությունների խմբի ուժեղ ծնիչների բազմության աղյուսակը (ինչպես Սիմսի ալգորիթմում): Մուտքային տվյալների N չափանի (N բայթ պարունակող) բլոկը ծածկագրելուց ստացվում է $n = 2N + 1$ տարրերից կազմված մեկ տեղադրություն: Ծածկագրման և վերծանման գործողությունները պարզ են և կարող են կատարվել սահմանափակ հնարավորություններ ունեցող անլար սենսորային հանգույցի կողմից: Բանալիների բաժանման սխեման հաշվի է առնում անլար սենսորային ցանցերում առկա բոլոր սահմանափակումներն ու պահանջները և տալիս է բանալիներ բաժանման ապահով սխեմա անելով միայն մեկ ենթադրություն, այն է՝ հանգույցները տեղադրվելուց հետո t_0 ժամանակի ընթացքում չեն ենթարկվում ֆիզիկական հարձակման: Այստեղ t_0 -ն ցանցի հանգույցների միջև հաղորդակցման բանալիների հաստատման համար անհրաժեշտ ժամանակն է, որը իրականում տևում է վայրկյաններ: