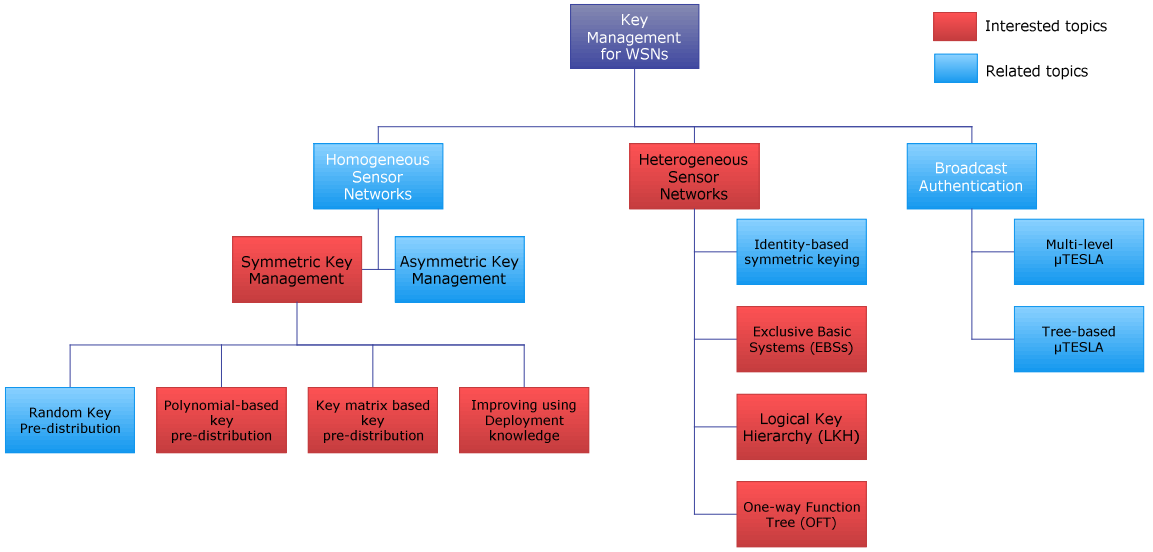
Research Taxonomy

by

Ngo Trong Canh, Master Student

u-Security Research Group
ntcanh@oslab.khu.ac.kr



Bibliography

1. General

[1.1] S. Rafaeli, D. Hutchison. “A survey of key management for secure group communication”, In ACM Computing Surveys, Vol. 35, No. 3, September 2003, pp. 309–329.

[1.2] B. C. Lai, D. D. Hwang, S. P. Kim, I. Verbauwhede. "Reducing radio energy consumption of key management protocols for wireless sensor networks", In Proceedings of the 2004 international symposium on Low power electronics and design, August 2004.

[1.3] D. Huang, D. Medhi. "A byzantine resilient multi-path key establishment scheme and its robustness analysis for sensor networks", In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, April 2005.

[1.4] S.A. Camtepe and B. Yener. “Key Distribution Mechanisms for Wireless Sensor Networks: a Survey”, In Technical Report TR-05-07 (March 23, 2005).

[1.5] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan. "On the distribution and revocation of cryptographic keys in sensor networks", In Dependable and Secure Computing, IEEE Transactions, 2005

[1.6] P. Kotzanikolaou1, D. D. Vergados2 and G. Stergiou. "Performance analysis of a hybrid key establishment protocol for wireless sensor networks", In Proceedings of the Seventh IEEE International Symposium on Multimedia, December 2005.

[1.7] Y.S Hwang, S.W Han, T.Y Nam. "The expansion of key infection model for dynamic sensor network", In : Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, February 2006.

[1.8] A.M. Hegland, E. Winjum, S. Mjølsnes, C. Rong, Kure, And P. Spilling "A survey of key management in ad hoc networks", In IEEE Communications Surveys & Tutorials, 3rd Quarter 2006.

2. Key Management for Homogeneous Wireless Sensor Networks

[2.1] L. Eschenauer, V. D. Gligor. "A key-management scheme for distributed sensor networks", In Proceedings of the 9th ACM conference on Computer and communications security, November 2002.

[2.2] H. Chan, A. Perrig, D. Song. "Random key predistribution schemes for sensor networks" In Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 2003.

[2.3] R. Pietro, L. Mancini, A. Mei. “Random key-assignment for secure Wireless Sensor Networks”, In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03, Octorber 2003.

[2.4] S. Zhu, S. Xu, S. Setia, S. Jajodia. “Establishing Pairwise Keys for Secure Communication in Ad Hoc Networks: A Probabilistic Approach”, In Proceedings of the 11th IEEE International Conference on Network Protocols, Nov2003.

[2.5] D. Hwang,B. Lai,and I. Verbauwhede. "Energy-memory-security tradeoffs in distributed sensor networks", In 3rd International Conference on Ad-Hoc Networks and Wireless(ADHOC-NOW 2004).

[2.6] J. Hwang, Y. Kim. "Revisiting random key pre-distribution for sensor networks", In ACM Workshop on Security of AdHoc and Sensor Networks(SASN04).

[2.7] D. Liu, P.Ning. "Establishing pairwise keys in distributed sensor networks", In ACM Transactions on Information and System Security, February 2003.

[2.8] P.J Chuang, T. H Chao, and B. Y Li. "A scalable grouping random key predistribution scheme for large scale distributed sensor networks", In Proceedings of the Third International Conference on Information Technology and Applications, July 2005.

[2.9] A.Price, K. Kristie. "A key pre-distribution scheme for wireless sensor networks", In Wireless Telecommunications Symposium, April 2005.

[2.10] H. Fu, S. Kawamura, M. Zhang, L. Zhang. "Replication attack on random key pre-distribution schemes for wireless sensor networks", In Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE, June 2005.

[2.11] R. Blom, ”An optimal class of symmetric key generation systems”, In Proc of EUROCRYPT ’84, pages 334-338, 1985.

[2.12] R. Blom, “An optimal class of symmetric key generation systems”, In Proc of EUROCRYPT ’84, pp. 334-338, 1985.

[2.13] W. Du, J. Deng, Y. S. Han, P. K. Varshney. "A pairwise key predistribution scheme for wireless sensor networks", In ACM Transactions on Information and System Security, May 2005

[2.14] S. Camtepe, and B. Yener. "Combinatorial design of key distribution mechanisms for wireless sensor networks. In 9th European Symposium on Research Computer Security, 2004.

[2.15] J. Lee, and D. Stinson. "A combinatorial approach to key pre-distributed sensor networks", http://www.cacr.math.uwaterloo.ca/~dstinson/pubs.html, 2004.

[2.16] D. S. Sánchez, H. Baldus. "A deterministic pairwise key pre-distribution scheme for mobile sensor networks", In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, September 2005.

[2.17] G. Li, J. He, Y. Fu. "A hexagon-based key predistribution scheme in sensor networks", In Proceedings of the 2006 International Conference on Parallel Processing Workshops, 2006.

[2.18] W. Du; J. Deng; Y. S. Han; S. Chen; P.K Varshney. ”A key management scheme for wireless sensor networks using deployment knowledge”, In 23rd AnnualJoint Conference of the IEEE Computer and Communications Societies (Infocom’04), Hong Khong, China, March 21-25, 2004.

[2.19] C. Yang; J. Xiao. “Location-Based Pairwise Key Establishment and Data Authentication for Wireless Sensor Networks”, In EEE Information Assurance Workshop, June 21-23, 2006.

[2.20] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. ”Perfect-secure key distribution of dynamic conferences”, In Advances in Cryptography – CRYPTO ’92, LNCS 740, pp. 471-486, 1993.

[2.21] D. Liu; P. Ning. “Location-based pairwise key establishments for static sensor networks”, In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN '03), October 2003

[2.22] Y. Zhou, Y. Zhang, and Y. Fang. "LLK: A link-layer key establishment scheme for wireless sensor networks", In Wireless Communications and Networking Conference IEEE, March 2005

[2.23] A. Kumar Das, A. Das, S. Mohapatra, S. Vavilapalli, "A location-aware scheme for key establishment in wireless sensor networks", In Communication System

[2.24] H. Chan, A. Perrig. "PIKE: peer intermediaries for key establishment in sensor networks", In Dependable and Secure Computing, IEEE Transactions, Jan.-March 2006.

[2.25] D. Liu, P.Ning. "Improving Key Predistribution with Deployment Knowledge in Static Sensor Networks", In ACM Transactions on Sensor Networks, Vol. 1, No. 2, November 2005, pp. 204-239.

[2.26] W. Du, J. Deng, Y. S. Han, P. Varshney. "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge". In IEEE Transactions on Dependable and Secure Computing, Volume 3 , Issue 1 (January 2006).

3. Key Management for Heterogeneous Wireless Sensor Networks

[3.1] Sandro Rafaeli And David Hutchison. ”A Survey of Key Management for Secure Group Communication”, In ACM Computing Surveys, Vol. 35, No. 3, September 2003, pp. 309–329.

[3.2] Yacine Challal, Hamida Seba. ”Group Key Management Protocols: A Novel Taxonomy”, In International Journal Of Information Technology, Vol. 2 No. 1, 2005.

[3.3] L.B. Oliveira, H.C. Wong, M. Bern, R. Dahab, A.A.F. Loureiro. "SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks",Fifth IEEE International Symposium on Network Computing and Applications, July 2006.

[3.4] M. F. Younis, K. Ghumman, M. Eltoweissy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks", In Ieee Transactions On Parallel And Distributed Systems, August 2006.

[3.5] G. Jolly, M.C. Kuscu, P. Kokate, and M. Younis. "A low-energy key management protocol for wireless sensor networks", In Proceedings of the Eighth IEEE International Symposium on Computers and Communication, Jun-July 2003.

[3.6] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy. "Scalable cryptographic key management in wireless sensor networks", In Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference, March 2004.

[3.7] "Robust security in large-scale wireless actuator and sensor networks: a low energy two-level implementation", In Networking, Sensing and Control, 2005. Proceedings. 2005 IEEE, March 2005.

[3.8] M. Chorzempa, J.-M. Park, M. Eltoweissy. "SECK: survivable and efficient clustered keying for wireless sensor networks", In : Performance, Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International, April 2005.

[3.9] F. Hu, X. Cao. "Security in wireless actor & sensor networks (WASN): towards a hierarchical re-keying design", Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference, April 2005.

[3.10] M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic key management in sensor networks", In Communications Magazine, IEEE, April 2006.

[3.11] Z. Qingguang, C. Yanling, L. Juan. "A Lightweight Key Management Protocol for Hierarchical Sensor Networks", In Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference, December 2006.

[3.12] X. Chen, J. Drissi. ”An efficient key management scheme in hierarchical sensor networks", In : Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference, November 2005.

[3.13] Biswajit Panja and Sanjay Madria. ”Energy-Efficient Group Key Management Protocols for Hierarchical Sensor Networks”, International Journal of Distributed Sensor Networks, 3:2, 201 – 223

[3.14] Alan T. Sherman and David A. McGrew, ”Key Establishment in Large Dynamic GroupsUsing One-Way Function Trees,” In IEEE Trans on Software Engineering, Vol. 29, No. 5, May 2003

[3.15] Yinian Mao, Yan (Lindsay) Sun, Min Wu, and K. J. Ray Liu. ”JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management”, In ACM/IEEE Trans on Networking, Vol. 14, No. 5, Oct 2006.

[3.16] Seyit A. Çamtepe and Bülent Yener, ”Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks”, In IEEE/ACM Trans on Networking, Vol. 15, No. 2, April 2007.

4. Broadcast authentication

[4.1] A. Perrig, R. Canetti, D. Song, and D. Tygar. ”Efficient authentication and signing of multicast streams over lossy channel”, In Proceedings of the 2000 IEEE Symposium on Security and Privacy, May 2000.

[4.2] A. Perrig, R. Canetti, D. Song, and D. Tygar. ”Efficient and secure source authentication for multicast”, In Proceedings of Network and Distributed System Security Symposium, Feb 2001.