Daftar Pustaka

[1] Ahmed, A. S. An evaluation of security protocols on wireless sensor network. In *TKK T-110.5190 Seminar on Internetworking* (2009).

[2] Alkhurayyif, Y. Security in wireless sensor network. *International Journal of Computing Science and Information Technology 1*, 3 (7 2013), 10–17.

[3] Asokan, N., Niemi, V., and Nyberg, K. Man-in-the-middle in tunnelled authentication protocols. In *International Workshop on Security Protocols* (2003), Springer, pp. 28–41.

[4] Dargie, W., and Poellabauer, C. *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons, 2010.

[5] Deepakumara, J., Heys, H. M., and Venkatesan, R. Performance comparison of message authentication code (mac) algorithms for internet protocol security (ipsec). In *Proc. Newfoundland Electrical and Computer Engineering Conf* (2003).

[6] Dener, D. Optimum packet length over data transmission for wireless sensor networks. In *Proceedings of the 8th International Conference on Sensing Technology* (2014), pp. 52–56.

[7] Denis, T. S. Libtomcrypt. *available online at libtom. org* (2004).

[8] Dodis, Y., Ristenpart, T., Steinberger, J., and Tessaro, S. To hash or not to hash, again. *On the Indifferentiability of the Second Iterate and HMAC* (2012).

[9] Gong, Z., Hartel, P., Nikova, S., and Zhu, B. Towards secure and practical macs for body sensor networks. In *International Conference on Cryptology in India* (2009), Springer, pp. 182–198.

[10] Guo, J., Sasaki, Y., Wang, L., Wang, M., and Wen, L. Equivalent key recovery attacks against hmac and nmac with whirlpool reduced to 7 rounds. In *International Workshop on Fast Software Encryption* (2014), Springer, pp. 571–590.

[11] Gupta, G. S., and Mukhopdhyay, S. C. *Smart Sensors and Sensing Technology*. Springer, 2008.

[12] Hu, F., and Cao, X. *Wireless sensor networks: principles and practice*. CRC Press, 2010.

[13] Hu, F., Ziobro, J., Tillett, J., and Sharma, N. K. Secure wireless sensor networks: Problems and solutions. *Rochester Institute of Technology, Rochester, New York, USA* (2004).

[14] Jorstad, N. D., and Landgrave, T. Cryptographic algorithm metrics. In *20th National Information Systems Security Conference* (1997).

[15] López, J., and Zhou, J. *Wireless sensor network security*, vol. 1. Ios Press, 2008.

[16] Luk, M., Mezzour, G., Perrig, A., and Gligor, V. Minisec: a secure sensor network communication architecture. In *Proceedings of the 6th international conference on Information processing in sensor networks* (2007), ACM, pp. 479–488.

[17] Muhammad, A. Implementation and verification of skipjack algorithm using verilog.

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

[19] Pricop, E., and Stamatescu, G. *Recent Advances in Systems Safety and Security*, vol. 62. Springer, 2016.

[20] Rivest, R. L. The rc5 encryption algorithm. In *International Workshop on Fast Software Encryption* (1994), Springer, pp. 86–96.

[21] Rogaway, P., Bellare, M., and Black, J. Ocb: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC) 6*, 3 (2003), 365–403.

[22] Sbrusch, R. *Authenticated messaging in wireless sensor networks used for surveillance*. ProQuest, 2008.

[23] Sen, J. *Routing security issues in wireless sensor networks: attacks and defenses*. INTECH Open Access Publisher, 2010.

[24] Shah, V., and Sharma, S. Evaluation of encryption method of snep for implementing security in wireless sensor network using spins framework. *International Journal of Grid and Distributed Computing 7*, 5 (2014), 43–52.

[25] Sharma, R., Chaba, Y., and Singh, Y. Analysis of security protocols in wireless sensor network. *International journal of advanced networking and applications 2*, 3 (2010), 707–713.

[26] Stavroulakis, P., and Stamp, M. *Handbook of information and communication security*. Springer Science & Business Media, 2010.

[27] Sumathy, S., and Kumar, B. U. Secure key exchange and encryption mechanism for group communication in wireless ad hoc networks. *arXiv preprint arXiv:1003.3564* (2010).