REFERENCES

1. AES, NIST 2001, Advanced encryption standard, Federal Information Processing Standard, FIPS-197, pp. 12.

2. Ahmed, MR, Huang, X & Sharma, D 2012, 'A taxonomy of internal attacks in wireless sensor network', International Scholarly and Scientific Research & Innovation, vol. 6, no. 2, pp. 393-396.

3. Ahmed, N, Kanhere, SS & Jha, S 2005, 'The holes problem in wireless sensor networks: a survey', ACM SIGMOBILE mobile computing and communications review, vol. 9, no. 2, pp. 4-18.

4. Akkaya, K & Younis, M 2005, 'A survey on routing protocols for wireless sensor networks', Journal of Adhoc Networks, vol. 3, no. 3, pp. 325-349.

5. Akyildiz, IF, Su, W, Sankarasubramaniam, Y & Cayirci, E 2002, 'Wireless sensor networks: a survey', Journal of Computer Networks, vol. 38, no. 4, pp. 393-422.

6. Alanazi, H, Zaidan, BB, Zaidan, AA, Jalab, HA, Shabbir, M & Al-Nabhani, Y 2010, 'New comparative study between DES, 3DES and AES within nine factors', Journal Of Computing, vol. 2, no. 3, pp. 152-157.

7. Alcaraz, C, Lopez, J, Roman, R & Chen, HH 2012, 'Selecting key management schemes for WSN applications', Journal of Computers & Security, vol. 31, no. 38, pp. 956-966.

8. Ali, M, Bohm, A & Jonsson, M 2008, 'Wireless sensor networks for surveillance applications–a comparative survey of MAC protocols', Proceedings of the fourth IEEE conference on wireless and mobile communications, pp. 399-403.

9. Al-Karaki, JN & Kamal, AE 2004, 'Routing techniques in wireless sensor networks: a survey', IEEE Wireless Communications, vol. 11, no.6, pp. 6-28.

10. Alliance, Z 2006, 'ZigBee security specification overview', http://www. zigbee.org/en/ events/doeuments/ December2005_ Open_ House_Presentation/Zigbee_Security_Layer_Technical_Overview.pdf.

11. Alzaid, H, Foo, E & Nieto, JG 2008, 'Secure data aggregation in wireless sensor network: a survey', Proceedings of the sixth australian conference on information security, vol. 81, pp. 93-105.

12. Anoop, MS 2007, 'Elliptic curve cryptography an implementation guide', http:// www. infosecwriters. com/text_ resources/ pdf/Elliptic_ Curve_ AnnopMS.pdf.

13. Arazi, B, Elhanany, I, Arazi, O & Qi, H 2005, 'Revisiting public-key cryptography for wireless sensor networks', Journal of Computer, vol. 38, no.11, pp. 103-105.

14. Bellovin, SM & Blaze, M 2001, 'Cryptographic modes of operation for the internet', Proceedings of the second NIST workshop on modes of operation, pp.1-6.

15. Bellovin, SM 1996, 'Problem areas for the IP security protocols', Journal of USENIX Security.

16. Bernstein, D, Birkner, P, Lange, T & Peters, C 2013, 'ECM using Edwards Curves', Journal of Mathematics of Computation, vol. 82, no. 282, pp. 1139-1179.

17. Bernstein, DJ & Lange, T 2011, 'A complete set of addition laws for incomplete Edwards curves', Journal of Number Theory, vol. 131, no.5, pp. 858-872.

18. Bernstein, DJ, Birkner, P, Joye, M, Lange, T & Peters, C 2008, 'Twisted edwards curves', In Progress in Cryptology, Springer Berlin Heidelberg, pp. 389-405.

19. Blake, IF, Seroussi, G & Smart, N 1999, 'Elliptic curves in cryptography', London Mathematical Society Lecture Note Series 265, Cambridge university press.

20. Blom, R 1985, 'An optimal class of symmetric key generation systems', In Advances in cryptology, Springer Berlin Heidelberg, pp. 335-338.

21. Blundo, C, De Santis, A, Herzberg, A, Kutten, S, Vaccaro, U & Yung, M 1993, 'Perfectly-secure key distribution for dynamic conferences', Advances in cryptology—CRYPTO'92, Springer Berlin Heidelberg, pp. 471-486.

22. Boukerche, A 2008, Algorithms and Protocols for Wireless Sensor Networks, John Wiley & Sons, vol. 62.

23. Boyle, DE & Newe, T 2009, 'On the implementation and evaluation of an elliptic curve based cryptosystem for Java enabled wireless sensor networks', Journal of Sensors and Actuators A: Physical, vol. 156, no. 2, pp. 394-405.

24. Brickell, EF, Denning, DE, Kent, ST, Maher, DP & Tuchmann, W 1993, 'The SKIPJACK Algorithm', pp. 1-7. [28 July 1993].

25. Brooks, R, Govindaraju, PY, Pirretti, M, Vijaykrishnan, N & Kandemir, MT 2007, 'On the detection of clones in sensor networks using random key predistribution', IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 37, no. 6, pp. 1246-1258.

26. Castelluccia, C, Mykletun, E & Tsudik, G 2005, 'Efficient aggregation of encrypted data in wireless sensor networks', proceedings in the second annual IEEE international conference on mobile and ubiquitous systems: networking and services, pp. 109-117.

27. Chan, H & Perrig, A 2003, 'Security and privacy in sensor networks', Journal of Computer, vol. 36, no.10, pp. 103-105.

28. Chan, H, Perrig, A & Song, D 2003, 'Random key predistribution schemes for sensor networks', Proceedings of the IEEE symposium in Security and Privacy, pp. 197-213.

29. Chaves, R, Kuzmanov, G, Sousa, L & Vassiliadis, S 2008, 'Cost-efficient SHA hardware accelerators', IEEE Transactions on Very Large Scale Integration Systems, vol. 16, no. 8, pp. 999-1008.

30. Chen, X, Makki, K, Yen, K & Pissinou, N 2009, 'Sensor network security: a survey', IEEE Journal of Communications Surveys & Tutorials, vol. 11, no. 2, pp. 52-73.

31. Cho, K, Jo, M, Kwon, T, Chen, HH & Lee, DH 2013, 'Classification and experimental analysis for clone detection approaches in wireless sensor networks', IEEE Journal of Systems, vol. 7, no. 1, pp. 26-35.

32. Choi, H, Zhu, S & LaPorta, TF 2007, 'SET: Detecting node clones in sensor networks', Proceedings in the third IEEE international conference on security and privacy in communications networks, pp. 341-350.

33. Chu, D, Großschädl, J, Liu, Z, Müller, V & Zhang, Y 2013, 'Twisted Edwards-form elliptic curve cryptography for 8-bit AVR-based sensor nodes', Proceedings in the first ACM workshop on Asia public-key cryptography, pp. 39-44.

34. Coleman, RA, Browne, M & Theobalds, T 2004, 'Aggregation as a defense: limpet tenacity changes in response to simulated predator attack', Journal of Ecology, vol. 85, no.4, pp. 1153-1159.

35. Conti, M, Di Pietro, R, Mancini, LV & Mei, A 2011, 'Distributed detection of clone attacks in wireless sensor networks", IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685-698.

36. Crosby, GV, Hester, L & Pissinou, N 2011, 'Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks', International Journal of Network Security, vol. 12, no. 2, pp. 107-117.

37. Crosby, GV, Pissinou, N & Gadze, J 2006, 'A framework for trust-based cluster head election in wireless sensor networks', Proceedings in the IEEE workshop on dependability and security in sensor networks and systems, pp. 10-22.

38. Culler, D, Hill, J, Horton, M, Pister, K, Szewczyk, R & Woo, A 2002, 'Mica: The commercialization of microsensor motes', Sensors Magazine, vol. 19, no. 4, pp. 40-48.

39. Das, AK 2011, 'An efficient random key distribution scheme for large-scale distributed sensor networks', Journal of Security and Communication Networks, vol. 4, no. 2, pp. 162-180.

40. Das, AK, Sharma, P, Chatterjee, S & Sing, JK 2012, 'A dynamic password-based user authentication scheme for hierarchical wireless sensor networks', Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646-1656.

41. Ding, M, Cheng, X & Xue, G 2003, 'Aggregation tree construction in sensor networks', Proceedings in the IEEE 58th conference on vehicular technology, vol. 4, pp. 2168-2172.

42. Doyle, B, Bell, S, Smeaton, AF, McCusker, K & O'Connor, NE 2006, 'Security considerations and key negotiation techniques for power constrained sensor networks', Journal of Computer, vol. 49, no. 4, pp. 443-453.

43. Du, X & Chen, W 2004, 'Sequential optimization and reliability assessment method for efficient probabilistic design', Journal of Mechanical Design, vol. 126, no. 2, pp. 225-233.

44. Du, X, Guizani, M, Xiao, Y & Chen, HH 2009, 'Transactions papers a routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks', IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1223-1229.

45. Dutertre, B, Cheung, S & Levy, J 2004, 'Lightweight key management in wireless sensor networks by leveraging initial trust', Technical Report SRI-SDL-04-02, SRI International.

46. Eastlake, D & Jones, P 2001, 'US secure hash algorithm 1 (SHA1)', RFC 3174, [September 2001].

47. Egea-Lopez, E, Vales-Alonso, J, Martinez-Sala, AS, Pavon-Marino, P & García-Haro, J 2005, 'Simulation tools for wireless sensor networks', Proceedings in the conference on summer simulation multiconference - SPECTS 2005, pp. 2-9.

48. ElGamal, T 1985, 'A public key cryptosystem and a signature scheme based on discrete logarithms', Lecture Notes in Computer Science, ed. George Robert Blakley & David Chaum, In Advances in Cryptology, Springer Berlin Heidelberg, vol. 196, pp. 10-18.

49. Eltoweissy, M, Moharrum, M & Mukkamala, R 2006, 'Dynamic key management in sensor networks', IEEE Communications Magazine, vol. 44, no. 4, pp. 122-130.

50. Emam, SA & Emami, SS 2007, 'Design and implementation of a fast, combined SHA-512 on FPGA", International Journal of Computer Science and Network Security, vol.7, pp.165-168.

51. Eschenauer, L & Gligor, VD 2002, 'A key-management scheme for distributed sensor networks', Proceedings of the 9th ACM conference on computer and communications security, pp. 41-47.

52. FIPS Publication 1999, '46-3: Data Encryption Standard (DES)', National Institute of Standards and Technology, vol. 25, no.10.

53. Forouzan, BA 2007, Cryptography & Network Security. McGraw-Hill, Inc.

54. Fouchal, S, Mansouri, D, Mokdad, L & Iouallalen, M 2013, 'Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks', International Journal of Communication Systems, vol. 28, no. 2, pp. 309-324.

55. Fu, F, Liu, J & Yin, X 2007, 'Space-time related pairwise key predistribution scheme for wireless sensor networks', proceedings of the international conference on wireless communication, networking and mobile computing, pp. 2692-2696.

56. Galindo, D, Roman, R & Lopez, J 2012, 'On the energy cost of authenticated key agreement in wireless sensor networks', Wireless Communications and Mobile Computing, vol. 12, no. 1, pp. 133-143.

57. Ganeriwal, S, Balzano, LK & Srivastava, MB 2008, 'Reputation-based framework for high integrity sensor networks', ACM Transactions on Sensor Networks, vol. 4, no. 3, pp. 1-5.

58. Garg, P & Tiwari N 2012, 'Evolution of Sha-176 algorithm', IOSR Journal of Computer Engineering, vol. 2, no. 2, pp. 18-22.

59. Gay, D, Levis, P, Culler, D & Brewer, E 2009, Nesc 1.3 language reference manual, Available from: <https:// fenix. tecnico. ulisboa. pt/downloadFile /3779579586689/nesc-1.3.1.pdf> [July 2009].

60. Gay, D, Levis, P, Von Behren, R, Welsh, M, Brewer, E & Culler, D 2003, 'The nesC language: A holistic approach to networked embedded systems', In ACM Sigplan Notices, vol. 38, no. 5, pp. 1-11.

61. Girao, J, Westhoff, D, Mykletun, E & Araki, T 2007, 'TinyPEDS: Tiny persistent encrypted data storage in asynchronous wireless sensor networks', Journal of Ad Hoc Networks, vol. 5, no. 7, pp. 1073-1089.

62. Good, T & Benaissa, M 2007, 'Hardware results for selected stream cipher candidates', State of the Art of Stream Ciphers, pp. 191-204.

63. Guo, MH & Deng, DJ 2011, 'Centralized conference key mechanism with elliptic curve cryptography and Lagrange interpolation for sensor networks', IET Communications, vol. 5, no. 12, pp. 1727-1731.

64. Hankerson, D, Hernandez, JL & Menezes, A 2000, 'Software implementation of elliptic curve cryptography over binary fields', in Cryptographic Hardware and Embedded Systems-CHES 2000, proceedings of the Second International Workshop Worcester, eds. Çetin K. Koç & Christof Paar, USA, Springer Berlin Heidelberg, pp. 1-24.

65. Hankerson, D, Menezes, A & Vanstone, S 2004, Guide to Elliptic Curve Cryptography", Springer Verlog, New York, ISBN 0-387-95273-X, pp.1-305.

66. Haque, MM, Pathan, ASK, Hong, CS & Huh, EN 2008, 'An asymmetric key-based security architecture for wireless sensor networks', KSII Transactions On Internet And Information Systems, vol. 2, no. 5, pp. 265-279.

67. Hassan, A & Bach, C 2014, 'Improving security connection in wireless sensor networks', International Journal of Innovation and Scientific Research, vol. 2, no. 2, pp. 301-307.

68. Hisil, H, Wong, KKH, Carter, G & Dawson, E 2008, 'Twisted Edwards curves revisited', Advances in Cryptology-ASIACRYPT 2008, ed. Josef Pieprzyk, Proceedings of 14th international conference on the theory and application of cryptology and information security, Melbourne, Australia, Springer Berlin Heidelberg, pp. 326-343.

69. Hoffstein, J, Pipher, J & Silverman, JH 1998, 'NTRU: A ring-based public key cryptosystem', In Algorithmic number theory, proceedings of the Third International Symposiun, ANTS-III ed. Joe P. Buhler, USA, Springer Berlin Heidelberg, pp. 267-288.

70. http://csrc.nist.gov/publications/nistpubs/800-56A/ SP80056A_ Revision1 Mar08 2007.pdf

71. Huang, X, Sharma, D & Shah, PG 2011, 'Dynamic window with fuzzy controller in wireless sensor networks for elliptic curve cryptography', Proceedings in the IEEE international conference on in fuzzy systems pp. 2342-2349.

72. Hussain, S & Rahman, MS 2009, 'Using received signal strength indicator to detect node replacement and replication attacks in wireless sensor networks', Proceedings of SPIE 7344, data mining, intrusion detection, information security and assurance, and data networks security, vol. 7344.

73. Hwang, J & Kim, Y 2004, 'Revisiting random key pre-distribution schemes for wireless sensor networks', Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 43-52.

74. Intanagonwiwat, C, Govindan, R & Estrin, D 2000, 'Directed diffusion: a scalable and robust communication paradigm for sensor networks', Proceedings of the 6th ACM annual international conference on mobile computing and networking, pp. 56-67.

75. Intanagonwiwat, C. Govindan, R, Estrin, D, Heidemann, J & Silva, F 2003, 'Directed diffusion for wireless sensor networking', IEEE/ACM Transactions on Networking, vol. 11, no. 1, pp. 2-16.

76. Janakiraman, VS, Ganesan, R & Gobi, M 2007, 'Hybrid cryptographic algorithm for robust network security', International Journal on Computer Network and Internet Research, vol. 7, no. 1, pp. 1-11.

77. Jha, MK & Sharma, TP 2011, 'Secure data aggregation in wireless sensor network: a survey', International Journal of Engineering Science and Technology, vol. 81, pp. 93-105.

78. Jing, L, Liu, F & Li, Y 2011, 'Energy saving routing algorithm based on SPIN protocol in WSN', Proceedings of the IEEE international conference on image analysis and signal processing (IASP), pp. 416-419.

79. Karl, H & Willig, A 2007, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons.

80. Karlof, C & Wagner, D 2003, 'Secure routing in wireless sensor networks: Attacks and countermeasures' Journal of Adhoc Networks, vol. 1, no. 2, pp. 293-315.

81. Karlof, C, Sastry, N & Wagner, D 2004, 'TinySec: link layer encryption for tiny devices", In ACM SenSys, pp.3-5.

82. Khalique, A, Singh, K & Sood, S 2010, 'Implementation of elliptic curve digital signature algorithm', International Journal of Computer Applications, vol. 2, no. 2, pp. 21-27.

83. Klaoudatou, E, Konstantinou, E, Kambourakis, G & Gritzalis, S 2009, 'A cluster-based framework for the security of medical sensor environments', in Trust, Privacy and Security in Digital Business, proceedings of the 6th International Conference on TrustBus 2009, eds. Simone Fischer-Hübner, Costas Lambrinoudakis & Günther Pernul, Austria, Springer Berlin Heidelberg, pp. 52-62.

84. Klaoudatou, E, Konstantinou, E, Kambourakis, G & Gritzalis, S 2011, 'A survey on cluster-based group key agreement protocols for WSNs', IEEE Communications Surveys & Tutorials, vol. 13, no. 3, pp. 429-442.

85. Koblitz, N 1987, 'Elliptic curve cryptosystems', Journal of Mathematics of Computation, vol. 48, no. 177, pp. 203-209.

86. Koc, CK 1994, 'High-speed RSA implementation', Technical Report, RSA Laboratories.

87. Koc, CK 1995, 'RSA hardware implementation', RSA Laboratories. [August 1995].

88. Kodali, RK & Chougule, SK 2013, 'Hierarchical key agreement protocol for wireless sensor networks', International Journal on Recent Trends in Engineering & Technology, vol. 9, no. 1, pp. 25-33.

89. Koo, WK, Lee, H, Kim, YH & Lee, DH 2008, 'Implementation and analysis of new lightweight cryptographic algorithm suitable for wireless sensor networks', Proceedings of the IEEE international conference on information security and assurance, pp. 73-76.

90. Krishnamachari, B & Heidemann, J 2004, 'Application-specific modelling of information routing in wireless sensor networks', Proceedings of the IEEE international conference on performance, computing, and communications, pp. 717-722.

91. Labraoui, N, Gueroui, M & Aliouat, M 2012, 'Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks', Transactions on Emerging Telecommunications Technologies, vol. 23, no. 4, pp. 303-316.

92. Lee, J & Stinson, DR 2005, 'Deterministic key predistribution schemes for distributed sensor networks', proceedings of the 11th international workshop on selected areas in cryptography, ed. Helena Handschuh & M. Anwar Hasan, Canada, Springer Berlin Heidelberg, pp. 294-307

93. Lee, JC, Leung, VC, Wong, KH, Cao, J & Chan, HC 2007, 'Key management issues in wireless sensor networks: current proposals and future developments', IEEE Transaction on Wireless Communications, vol. 14, no. 5, pp. 76-84.

94. Leong, MP, Cheung, OY, Tsoi, KH & Leong, PHW 2000, 'A bit-serial implementation of the international data encryption algorithm IDEA', Proceedings of the IEEE symposium on field-programmable custom computing machines, pp. 122-131.

95. Levis, P, Lee, N, Welsh, M & Culler, D 2003, 'TOSSIM: Accurate and scalable simulation of entire TinyOS applications', Proceedings of the 1st ACM international conference on Embedded networked sensor systems, pp. 126-137.

96. Li, J, Li, Y, Ren, J & Wu, J 2014, 'Hop-by-Hop message authentication and source privacy in wireless sensor networks', IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1223-1232.

97. Lin, X 2009, 'CAT: Building couples to early detect node compromise attack in wireless sensor networks', Proceedings of the IEEE Conference on Global Telecommunications, pp. 1-6.

98. Liu, A & Ning, P 2008, 'TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks', Proceedings of the IEEE international conference on information processing in sensor networks, IPSN'08, pp. 245-256.

99. Liu, D, Ning, P & Li, R 2005, 'Establishing pairwise keys in distributed sensor networks', ACM Transactions on Information and System Security, vol. 8, no. 1, pp. 41-77.

100. López, J & Zhou, J 2008, Wireless Sensor Network Security, IOS Press, vol. 1, Netherland.

101. Lopez, J, Roman, R, Agudo, I & Fernandez-Gago, C 2010, 'Trust management systems for wireless sensor networks: Best practices', Journal of Computer Communications, vol. 33, no. 9, pp. 1086-1093.

102. Lou, Y, Zhang, Y & Liu, S 2012, 'Single hop detection of node clone attacks in mobile wireless sensor networks', Procedia Engineering, vol. 29, pp. 2798-2803.

103. Lu, H, Li, J & Guizani, M 2014, 'Secure and efficient data transmission for cluster-based wireless sensor networks', IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 750-761.

104. Lukosius, A 2006, Context routing in wireless sensor networks, Communication Networks, Master project, University of Bremen.

105. Lv, S, Wang, X, Zhao, X & Zhou, X 2008, 'Detecting the sybil attack cooperatively in wireless sensor networks', Proceedings of the IEEE international conference on computational intelligence and security, CIS'08, vol. 1, pp. 442-446.

106. Makin, BA & Padha, DA 2010, 'A trust-based secure data aggregation protocol for wireless sensor networks', IUP Journal of Information Technology, vol. 6, no. 3, pp. 7-22.

107. Malan, DJ, Welsh, M & Smith, MD 2004, 'A public-key infrastructure for key distribution in Tinyos based on elliptic curve cryptography', Proceedings of the first annual IEEE communications society conference on sensor and ad hoc communications and network, pp.71-80.

108. Malan, DJ, Welsh, M & Smith, MD 2008, 'Implementing public-key infrastructure for sensor networks', ACM Transactions on Sensor Networks, vol. 4, no. 4, pp. 22.

109. Martínez, VG, Encinas, LH & Ávila, CS 2010, 'A survey of the elliptic curve integrated encryption scheme', A Journal of Computer Science and Engineering, vol. 2, no. 2, pp. 7-13.

110. Mascolo, C & Musolesi, M 2006, 'SCAR: context-aware adaptive routing in delay tolerant mobile sensor networks', Proceedings of the 2006 ACM international conference on wireless communications and mobile computing, pp.533-538.

111. Menezes, AJ, Oorschot, PCV & Vanstone, SA 2010, Handbook of Applied Cryptography, CRC press.

112. Mishra, AK & Turuk, AK 2013, 'A zone-based node replica detection scheme for wireless sensor networks', Journal of Wireless Personal Communications, vol. 69, no. 2, pp. 601-621.

113. Moniruzzaman, M, Arafeen, MJ & Bose, S 2009, 'overview of wireless sensor networks-detection of cloned node using RM, LSN, SET, Bloom filter and AICN protocol and comparing their performances', International Journal of Digital Content Technology and its Applications, vol. 3, no. 3, pp. 103-108.

114. Moon, D, Hwang, K, Lee, W, Lee, S & Lim, J 2002, 'Impossible differential cryptanalysis of reduced round XTEA and TEA', in fast software encryption, proceedings of the 9th international workshop on fast software encryption, ed. Joan Daemen & Vincent Rijmen, Belgium, Springer Berlin Heidelberg, pp. 49-60.

115. Mykletun, E, Girao, J & Westhoff, D 2006, 'Public key based cryptoschemes for data concealment in wireless sensor networks', Proceedings of the IEEE International Conference on Communications, vol. 5, pp. 2288-2295.

116. Okeya, K & Sakurai, K 2000, 'Power analysis breaks elliptic curve cryptosystems even secure against the timing attack', Progress in cryptology—INDOCRYPT, Springer Berlin Heidelberg, pp. 178-190.

117. Ozdemir, S & Xiao, Y 2009, 'Secure data aggregation in wireless sensor networks: A comprehensive overview', Journal of Computer Networks, vol. 53, no. 12, pp. 2022-2037.

118. Ozdemir, S & Xiao, Y 2011, 'Integrity protecting hierarchical concealed data aggregation for wireless sensor networks', Journal of Computer Networks, vol. 55, no. 8, pp. 1735-1746.

119. Ozdemir, S & Xiao, Y 2013, 'FTDA: outlier detection-based fault-tolerant data aggregation for wireless sensor networks', Journal of Security and Communication Networks, vol. 6, no. 6, pp. 702-710.

120. Ozdemir, S 2008, 'Functional reputation based reliable data aggregation and transmission for wireless sensor networks', Journal of Computer Communications, vol. 31, no. 17, pp. 3941-3953.

121. Padmavathi, DG & Shanmugapriya, M 2009, 'A survey of attacks, security mechanisms and challenges in wireless sensor networks', International Journal of Computer Science and Information Security, vol. 4, no. 1 & 2, arXiv preprint arXiv:0909.0576.

122. Padmavathi, G, Shanmugapriya, D & Kalaivani, M 2010, 'A study on vehicle detection and tracking using wireless sensor networks', Journal of Wireless Sensor Network, vol. 2, no. 2, pp. 173-185.

123. Pandey, A & Tripathi, RC 2010, 'A survey on wireless sensor networks security', International Journal of Computer Applications, vol. 3, no 2, pp. 8887-8975.

124. Parno, B, Perrig, A & Gligor, V 2005, 'Distributed detection of node replication attacks in sensor networks', Proceedings of the IEEE symposium on security and privacy, pp. 49-63.

125. Perrig, A, Stankovic, J & Wagner, D 2004, 'Security in wireless sensor networks', ACM Communications, vol. 47, no. 6, pp. 53-57.

126. Piotrowski, K, Langendoerfer, P & Peter, S 2006, 'How public key cryptography influences wireless sensor node lifetime', Proceedings of the fourth ACM workshop on security of ad hoc and sensor networks, pp.169-176.

127. Potlapally, NR, Ravi, S, Raghunathan, A & Jha, NK 2003, 'Analyzing the energy consumption of security protocols', Proceedings of the ACM international symposium on low power electronics and design, pp. 30-35.

128. Potlapally, NR, Ravi, S, Raghunathan, A, & Jha, NK 2006, 'A study of the energy consumption characteristics of cryptographic algorithms and security protocols', IEEE Transactions on Mobile Computing, vol. 5, no. 2, pp. 128-143.

129. Prasithsangaree, P & Krishnamurthy, P 2004, 'On a framework for energy-efficient security protocols in wireless networks', Journal of Computer Communications, vol. 27, no 17, pp. 1716-1729.

130. Preneel, B & Rijmen, V 2008, The status of stream ciphers after the eSTREAM, Project, < http://www.ecrypt.eu.org/stream/portfolio.pdf>.

131. Rabin, MO 1979, 'Digitalized signatures and public-key functions as intractable as factorization', ACM digital library, Technical report.

132. Raymond, DR & Midkiff, SF 2008, 'Denial-of-service in wireless sensor networks: Attacks and defenses', IEEE Journal of Pervasive Computing, vol. 7, no. 1, pp. 74-81.

133. Roberts, PH & Zobel, RN 2004, 'A discussion of elliptic curve cryptography and configurable ecc system design with application to distributed simulation', International Journal of Simulation, vol. 5, no. 1-2, pp. 47-57.

134. Sahingoz, OK 2013, 'Large scale wireless sensor networks with multi-level dynamic key management scheme', Journal of Systems Architecture, vol. 59, no. 9, pp. 801-807.

135. Sanchez, DS & Baldus, H 2005, 'A deterministic pairwise key pre-distribution scheme for mobile sensor networks', Proceedings of the first IEEE international conference on security and privacy for emerging areas in communications networks, SecureComm 2005, pp. 277-288.

136. Sastry, N & Wagner, D 2004, 'Security considerations for IEEE 802.15. 4 networks', Proceedings of the 3rd ACM workshop on wireless security, pp. 32-42.

137. Shah, PG, Huang, X & Sharma, D 2010, 'Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes', Proceeding of the international conference on wireless communication and sensor computing, pp. 1-6.

138. Shaikh, RA, Jameel, H, d'Auriol, BJ, Lee, H, Lee, S & Song, YJ 2009, 'Group-based trust management scheme for clustered wireless sensor networks', IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 11, pp. 1698-1712.

139. Sharma, K & Ghose, MK 2010, 'Wireless sensor networks: An overview on its security threats', IJCA Special Issue on Mobile Ad-hoc Networks, pp. 42-45.

140. Shen, AN, Guo, S, Chien, HY & Guo, M 2009, 'A scalable key pre-distribution mechanism for large-scale wireless sensor networks', Research article on concurrency and computation: practice and experience, vol. 21, no. 10, pp. 1373-1387.

141. Shim, KA, Lee, YR & Park, CM 2013, 'EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks', Journal of Ad Hoc Networks, vol. 11, no. 1, pp. 182-189.

142. Ssu, KF, Wang, WT & Chang, WC 2009, 'Detecting sybil attacks in wireless sensor networks using neighboring information', Journal of Computer Networks, vol. 53, no. 18, pp. 3042-3056.

143. Tague, P & Poovendran, R 2007, 'A canonical seed assignment model for key predistribution in wireless sensor networks', ACM Transactions on Sensor Networks, vol. 3, no.4, article. 19.

144. Tan, H, Zic, J, Jha, SK & Ostry, D 2011, 'Secure multihop network programming with multiple one-way key chains', IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp. 16-31.

145. Tan, HÖ & Körpeoğlu, I 2003, 'Power efficient data gathering and aggregation in wireless sensor networks', ACM Sigmod Record, vol. 32, no. 4, pp. 66-71.

146. Tobarra, L, Cazorla, D, Cuartero, F, Diaz, G & Cambronero, E 2007, 'Model checking wireless sensor network security protocols: Tinysec+ LEAP', Proceedings of the Wireless Sensor and Actor Networks, Springer US, pp. 95-106.

147. Ugus, O, Hessler, A & Westhoff, D 2007, 'Performance of additive homomorphic EC-Elgamal encryption for TinyPEDS', <http://137.226.34.227/ftp/pub/ publications/ rwth/informatik/ 2007/ 2007-11.pdf#page=61>.

148. Umakanth, B & Damodhar, J 2013, 'Detection of Energy draining attack using EWMA in wireless ad hoc sensor networks', International Journal of Engineering Trends and Technology, vol. 4, no. 8, pp. 3691-3695.

149. Vaidyanathan, K, Sur, S, Narravula, S & Sinha, P 2004, 'Data aggregation techniques in sensor networks', Technical Report, The Ohio State University.

150. Venugopalan, R, Ganesan, P, Peddabachagari, P, Dean, A, Mueller, F & Sichitiu, M 2003, 'Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis', Proceedings of the ACM international conference on compilers, architecture and synthesis for embedded systems, pp. 188-197.

151. Verma, OP, Agarwal, R, Dafouti, D & Tyagi, S 2011, 'Performance analysis of data encryption algorithms'. Proceedings of the IEEE 3rd international conference on electronics computer technology, vol. 5, pp. 399-403.

152. Wang, J, Yang, G, Sun, Y & Chen, S 2007, 'Sybil attack detection based on RSSI for wireless sensor network' Proceedings of the IEEE international conference on wireless communications, networking and mobile computing, pp. 2684-2687.

153. Watro, R, Kong, D, Cuti, SF, Gardiner, C, Lynn, C & Kruus, P 2004, 'TinyPK: securing sensor networks with public key technology' Proceedings of the 2nd ACM workshop on Security of adhoc and sensor networks, pp. 59-64.

154. Wei-hong, W, Yu-bing, L & Tie-ming, C 2008, 'The study and application of elliptic curve cryptography library on wireless sensor network', Proceedings of the 11th IEEE international conference on communication technology, pp. 785-788.

155. Wen, H, Luo, J & Zhou, L 2011, 'Lightweight and effective detection scheme for node clone attack in wireless sensor networks', IET Wireless Sensor Systems, vol. 1, no. 3, pp. 137-143.

156. Westhoff, D, Girao, J & Acharya, M 2006, 'Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation', IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1417-1431.

157. Wheeler, DJ & Needham, RM 1995, 'TEA, a tiny encryption algorithm', Proceeding of the Fast Software Encryption, Springer Berlin Heidelberg, pp. 363-366.

158. Win, ED, Mister, S, Preneel, B & Wiener, M 1998, 'On the performance of signature schemes based on elliptic curves', in Algorithmic Number Theory: proceedings of Third International Symposium, ed. Joe P. Buhler, USA, Springer Berlin Heidelberg, pp. 252-266.

159. Wolf, C & Preneel, B 2005, 'Taxonomy of public key schemes based on the problem of multivariate quadratic equations', IACR Cryptology ePrint Archive, no. 77.

160. Wood, AD & Stankovic, JA 2004, A taxonomy for denial-of-service attacks in wireless sensor networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, pp. 739-763.

161. Xiao, Y, Chen, HH, Sun, B, Wang, R & Sethi, S 2006, 'MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks', EURASIP Journal on Wireless Communications and Networking.

162. Xiao, Y, Rayi, VK, Sun, B, Du, X, Hu, F & Galloway, M 2007, 'A survey of key management schemes in wireless sensor networks', Journal of Computer Communications, vol. 30, no. 11, pp. 2314-2341.

163. Xue, K, Ma, C, Hong, P & Ding, R 2013, 'A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks', Journal of Network and Computer Applications, vol. 36, no. 1, pp.316-323.

164. Ya-nan, L, Jian, W, He, D & Li-jun, S 2013, 'Intra-cluster key sharing in hierarchical sensor networks', IET Wireless Sensor Systems, vol.3, no.3, pp. 172-182.

165. Yang, Y, Wang, X, Zhu, S & Cao, G 2008, 'SDAP: A secure hop-by-hop data aggregation protocol for sensor networks', ACM Transactions on Information and System Security, vol. 11, no.4, article. 18.

166. Ye, W, Heidemann, J & Estrin, D 2002, 'An energy-efficient MAC protocol for wireless sensor networks', Proceedings of 21st IEEE annual joint conference of the IEEE computer and communications societies. vol. 3, pp. 1567-1576.

167. Yeh, HL, Chen, TH, Liu, PC, Kim, TH & Wei, HW 2011, 'A secured authentication protocol for wireless sensor networks using elliptic curves cryptography', Journal of Sensors, vol. 11, no. 5, pp. 4767-4779.

168. Yick, J, Mukherjee, B & Ghosal, D 2008, 'Wireless sensor network survey', Journal of Computer Networks, vol. 52, no. 12, pp. 2292-2330.

169. Younis, M, Ghumman, K & Eltoweissy, M 2006, 'Location-aware combinatorial key management scheme for clustered sensor networks', IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 8, pp. 865-882.

170. Younis, O & Fahmy, S 2004, 'HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks', IEEE Transactions on Mobile Computing, vol. 3, no. 4, pp. 366-379.

171. Yu, Y, Li, K, Zhou, W & Li, P 2012, 'Trust mechanisms in wireless sensor networks: attack analysis and countermeasures', Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880.

172. Zeng, Y, Cao, J, Zhang, S, Guo, S & Xie, L 2010, 'Random-walk based approach to detect clone attacks in wireless sensor networks', IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677-691.

173. Zhang, J & Varadharajan, V 2010, 'Wireless sensor network key management survey and taxonomy', Journal of Network and Computer Applications, vol. 33, no. 2, pp. 63-75.

174. Zhang, X, He, J & Wei, Q 2011, 'EDDK: energy-efficient distributed deterministic key management for wireless sensor networks', EURASIP Journal on Wireless Communications and Networking, article. 12.

175. Zhou, Y, Fang, Y & Zhang, Y 2008, 'Securing wireless sensor networks: a survey', IEEE Journal of Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6-28.

176. Zhu, B, Setia, S, Jajodia, S, Roy, S & Wang, L 2010, 'Localized multicast: efficient and distributed replica detection in large-scale sensor networks', IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913-926.

177. Zhu, S, Setia, S & Jajodia, S 2006, 'LEAP+: Efficient security mechanisms for large-scale distributed sensor networks', ACM Transactions on Sensor Networks, vol. 2, no. 4, pp. 500-528.