References

1. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 29, pp. 656–715, 1949.
2. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, pp. 1355–1387, Oct. 1975.
3. I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, pp. 339–348, May 1978.
4. A.O. Hero, "Secure space-time communication," IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
5. X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," J. Commun., vol. 2, no. 3, pp. 24–32, May 2007.
6. H. Kim and J. D. Villasenor, "Secure MIMO communications in a system with equal numbers of transmit and receive antennas," IEEE Commun. Lett., vol. 12, no. 5, pp. 386–388, May, 2008.
7. U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, Mar. 1993.
8. S. Wolf, Theoretically and computationally secure key agreement in cryptography, Ph. D Dissertation, 1999.
9. I. Csiszar and P. Narayan, "Common randomness in information theory and cryptography, part I: Secret sharing," IEEE Trans. Inf. Theory, vol. 39, pp. 1121–1132, July 1993.
10. A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
11. M. Nloch, J. Barros and M. R. D. Rodrigues, "Wireless information theoretic security," IEEE Trans. Inform. Theory, vol. 54, no. 6, pp. 2515–2534, June, 2008.
12. J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," IEICE Trans. Fund. Elec. Comm. Comp., vol. E89-A, no. 7, pp. 2036–2046, July 2006.
13. M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in Proceedings of 41st Annual Conference on Information Sciences and Systems, Baltimore, MD, Mar. 2007.
14. E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2735–2751, June, 2008.
15. L. Lai, H. El Gamal and H. V. Poor, "The Wiretap channel with feedback: encryption over the channel," http://www.ece.osu.edu/helgamal/publications.html.

H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4614-6510-2, © The Author(s) 2013

16. C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding: Turbo codes," in Proceedings of IEEE Int. Conf. Communications, Geneva, Switzerland, 1993, pp. 1064–1070.
17. R. G. Gallager, "Low density parity check codes," Cambridge, MA: MIT Press, 1963.
18. D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," IEEE Trans. Inf. Theory, vol. 45, no. 3, pp. 399–431, Mar. 1999.
19. L. Bazzi, T. J. Richardson and R. L. Urbanke, "Exact thresholds and optimal codes for the binary-symmetric channel and gallager's decoding algorithm A," IEEE Trans. Inf. Theory, vol. 50, no. 9, pp. 2010–2021, Sep. 2004.
20. B. Marco, C. Giovanni, and C. Franco, "Variable rate LDPC codes for wireless applications," in Proceedings of Software in Telecommunications and Computer Networks International Conference on Sept. 29–Oct. 1, pp. 301–305, 2006.
21. H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," IEEE Trans. Inform. Theory, vol. 57, no. 10, pp. 6428–6443, 2011.
22. A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth ldpc codes," IEEE Trans. Inform. Forensics and Secur., vol. 6, no.3, pp. 585–594, 2011.
23. H. Ahmadi, R. Safavi-Naini, "Secret keys from channel noise," Eurocry 2011, pp. 266–283, 2011.
24. K. Zeng and D. Wu, A. Chan and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," IEEEINFOCOM 2010, pp. 1–9, 2010.
25. H. Behairy, S.-C. Chang, "Parallel concatenated gallager codes," Electron.Lett., vol. 36, no. 24, pp. 2025–2026, 2000.
26. H. Wen, G. Gong and P-H. Ho, "Build-in wiretap channel I with feedback and LDPC codes," J. Commun. Netw., vol. 11, no. 6, pp. 538–643, Dec. 2009.
27. Hong Wen, Pin-Han Ho and Xiao-Hong Jiang, "On achieving unconditional secure communications over binary symmetric channels (BSC)," IEEE Wirel. Commun. Lett., vol. 1, no. 2, pp. 49–52, 2012.
28. S. Lin and D. J. Costello, Jr., Error control coding: fundamentals and applications. Englewood Cliffs, NJ: Prentice-Hall, 1983.
29. H. Koorapaty, A. A. Hassan, S. Chennakeshu, "Secure information transmission for mobile radio," IEEE Trans. Wirel. Commun., vol. 2, no. 7, pp. 52–55, 2003.
30. Y. Zhang and H. Dai, "A real orthogonal space-time coded UWB scheme for wireless secure communications," EURASIP J. Wirel Commun. Netw., vol. 6, no. 3, pp. 1–8, 2009.
31. Y. Hua, S. An and Y. Xiang, "Blind identification of FIR MIMO channels by decorrelation subchannels," IEEE Trans. Signal Process., vol. 51, no. 5, pp. 1143–1155, 2003.
32. T. Liu, S. Shamai Shitz, "A note on the secrecy capacity of the multiantenna wiretap channel," IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547–2553, 2009.
33. Y. Nawaz and G. Gong, "WG: A family of stream ciphers with designed randomness properties," Inf. Sci., vol. 178, no. 7, pp. 1903–1916, 2008.
34. N. Courtois, "Higher order correlation attacks, XL algorithm and cryptanalysis of toyocrypt", In Proceedings of ICISC 2002, LNCS: vol. 2587, Berlin: Springer, pp. 182–199, 2003.
35. V. Tarokh, H. Jafarkhani, A. R. Calderbank, "Space time block codes from orthogonal designs," IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 744–765, 1999.
36. IEEE P802.11n, Draft standard for information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements, Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. 802.11 Working Group of the 802 Committee, 2009.
37. S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," IEEE Journal on Selected Areas in Communications, vol. 16, no.8, pp. 1451–1458, 1998.

38. V. Tarokh, A. Naguib, N. Seshadri, A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criteria in the presence of channel estimation errors, mobility, and multiple paths," IEEE Trans. Commun., vol. 17, no. 2, pp. 199–207, 1999.
39. H. Wen, G. Gong, S. Lv and P. Ho, "Framework for MIMO cross-layer secure communication based on STBC," Telecommun. Syst. J., pp. 1–9, August 2011.
40. H. Wen, P. Ho and G. Gong, "A framework of physical layer technique assisted authentication for vehicular communication networks," Sci China Ser F-Inf Sci, vol. 53, no. 10, pp. 1996–2004, 2010.
41. H. Wen, P. Ho, C. Qi and G. Gong, "Physical layer assisted authentication for distributed Ad-Hoc wireless sensor networks," IEEE Inf. Secur., vol. 4, issue 4, pp. 390–396, 2010.
42. H. Wen, P. Ho, "Physical layer technique to assist authentication based on PKI for vehicular xommunication networks," KSII Trans. Internet Inf. Syst.," vol. 5, issue 5, pp. 440–456, Feb. 2011.
43. H. Wen, J. Luo and L. Zhou, "Lightweight and effective detection scheme for node clone attack in WSNs," IET Wireless Sensor Systems, vol. 1, no. 3, pp. 137–143, Sept. 2011.
44. H. Wen, P. Ho and X. Jiang, "On achieving unconditional secure communications over binary symmetric channels (BSC)," IEEE Wirel. Commun. Lett., vol. 1, no. 2, pp.49–52, 2012.
45. L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," IEEE Trans. Wirel. Commun., vol. 7, issue 7, pp. 2571–2579, July 2008.
46. L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," in Proceedings of IEEE International Conference on Communications, pp. 4646–4651, 24–28 June 2007.
47. L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in Proceedings of IEEE International Conference on Communications, pp. 1520–1524, 19–23 May 2008.
48. P. L. Yu, J. S. Baras, B. M. Sadler, "Physical-layer authentication," IEEE Trans. Inf. Forensics and Secur., vol. 3, no. 1, pp. 38–51, Mar. 2008.
49. P. A. Bello, "Characterization of randomly time-variant linear channels," IEEE Trans. Comm. Syst., vol. 11, pp. 360–393, 1963.
50. O. Edfors, M. Sandell, J. J. van de Beek, S. K. Wilson, and P. O. Borjesson, "OFDM xhannel estimation by singular value decomposition," IEEE Trans. Comm., vol. 46, no. 7, pp. 931–939, July 1998.
51. P. Hoeher, S. Kaiser, and P. Robertson, "Pilot-symbol-aided channel estimation in time and frequency," in Proceedings of IEEE Global Telecommunications, pp. 90–96, Nov. 1997.
52. Y. Li, L. J. Cimini, Jr. and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," IEEE Trans. Commun., vol. 46, no. 7, pp. 902–915, July 1998.
53. S. Coleri, M. Ergen, A. Puri, A. Bahai, "A Study of channel estimation in OFDM systems," in Proceedings of IEEE VTC, vol. 2, pp. 894–898, Vancouver, Canada, Sept. 2002.
54. Y. Qiao, S. Yu, P. Su, and L. Zhang, "Research on an iterative algorithm of LS Channel estimation in MIMO OFDM systems," IEEE Trans. Broadcast, vol. 51, no. 1, pp. 149–153, Mar. 2005.
55. A. Wald, "Sequential tests of statistical hypotheses," Ann. Math. Stat. 16 (2): 117–186, June 1945.
56. "Dedicated Short Range Communications (DSRC)," [Online] Available: http://grouper.ieee.org/ groups /scc32/dsrc/index.html, 2007.
57. Task Group p, "IEEE P802.11p: Draft standard for information technology telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE Computer Society, Jun. 2009.

58. J.P. Hubaux, “The security and privacy of smart vehicles,” IEEE Secur. Priv., vol. 2, pp. 49–55, 2004.
59. M. Raya and J. P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007.
60. F. Dotzer, “Privacy issues in vehicular Ad Hoc networks,” in Proceedings of ACM Workshop on Vehicular Ad Hoc Networks, Sept. 2006.
61. H. Moustafa, G. Bourdon, and Y. Gourhant, “AAA in vehicular communication on highways with Ad Hoc networking support: a proposed architecture,” in Proceedings of ACM workshop on Vehicular ad hoc networks, pp. 79–80, 2005.
62. C. Zhang, R. Lu, X. Lin, Pin-Han Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” in Proceedings of IEEE INFOCOM, pp. 246–250, 2008.
63. X. Lin, X. Sun, X. Wang, C. Zhang, Pin-Han Ho, X. Shen, “TSVC: timed efficient and secure vehicular communications with privacy preserving,” IEEE Trans. Wirel. Commun., vol. 7, no. 12, pp. 4987–4998, 2009.
64. C. Zhang, X. Lin, R. Lu and P. H. Ho, “RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks,” in Proceedings of ICC’08, pp. 1451–1457, May 19–23, 2008.
65. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: security protocols for sensor netowrks,” in Proceedings of the 7th annual international conference on Mobile computing and networking, July 2001, Rome, Italy, p. 189–199.
66. Donggang Liu and Peng Ning, “Multilevel μTESLA: broadcast authentication for distributed sensor networks,” ACM Trans. Embed. Comput. Syst., vol. 3, no. 3, Nov. 2004, pp. 800–836.
67. M. Demirbas, Youngwhan Song, “An RSSI-based scheme for Sybil attack detection in wireless sensor networks,” in Proceedings of WoWMoM 2006, pp. 566–570, 2006.
68. R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, 1978, pp. 120–126.
69. U. S. National Institute of Standards and Technology (NIST), Digital Signature Standard (DSS), Federal Register 56. FIPS PUB 186, Aug. 1991.
70. U. S. National Institute of Standards and Technology (NIST). DES Model of Operation. Federal Information Processing Standards Publication 81 (FIPS PUB 81).
71. S. P. Miller, C. Neuman, J. I. Schiller, and J. H. Saltzer, “Kerberos authentication and authorization system,” In Project Athena Technical Plan, page section E.2.1, 1987.
72. IEEE LAN/MAN Standards Committee, “IEEE 802.16a: air interface for fixed broadband wireless access systems,” 2003.
73. Wireless InSite software, http://www.remcom.com/wirelessinsite/.
74. J. Daemen and V. Rijmen. AES proposal: Rijndael, Mar. 1999.
75. IEEE P802 LAN/MAN Committee, “The working group for wireless local area networks (WLANs),” http://grouper.ieee.org/groups/802/11/index.html.
76. B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 49–63, 2005.
77. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” In Proceedings of First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127, 2003.
78. Anthony D. Wood and John A. Stankovic. A Taxonomy for denial-of-service attacks in wireless sensor networks. Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, 2004.
79. Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location-based compromise-tolerant security mechanisms for wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 247–260, 2006.

80. R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, and Cybern., Part C: Applications and Reviews, vol. 37, no. 6, pp. 1246–1258, 2007.
81. C. Bekara and M. Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against nodes replication attacks," in Proceedings of Third IEEE International Conference on Wireless and Mobile Computing, Netw. Commun. (WiMOB 2007), 2007, pp. 59–59.
82. Zhijun Li and Guang Gong, "DHT-based detection of node clone in wireless sensor networks," in Proceedings of First International Conference on Ad Hoc Networks (ADHOCNETS 2009), Sept. 23–25, 2009, Niagara Falls, Ontario, Canada, LNICST 28, pp. 240–255.
83. Zhijun Li and Guang Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," in Proceedings of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS '09), Oct. 12–15, 2009, Macau SAR, P.R.C, pp. 1030–1035.
84. T. Suen and A. Yasinsac, "Ad Hoc network security: peer identification and authentication using signal properties," In Systems, Man and Cybernetics (SMC) Information Assurance Workshop, pp. 432–433, 2005.
85. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 Mac layer spoofing using received signal strength," In Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), Apr. 2008.
86. J. Douceur, "The Sybil attack," In Proceedings of First International Workshop on Peer-to-Peer Systems, pp. 251–260, 2002.
87. Zhang Jian-Ming, Yu Qun and Wang Liang-Min, "Geographical location-based scheme for Sybil attacks detection in wireless sensor networks," J. Syst. Simul., vol. 20, no. 1, pp. 259–263, Jan. 2008.
88. J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," In Proceedings of third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259–268, 2004.
89. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proceedings of the 9th ACM Conference on Computer and communications security (CCS), Nov. 2002.
90. P. Golle, D. Greene and J. Staddon, "Detecting and correcting malicious data in VANETs," In proceedings of 1st ACM Workshop on Vehicular Ad Hoc Networks pp. 29–37, 2004.
91. Jie Yang, Yingying Chen, W. Trappe, "Detecting Sybil attacks in wireless and sensor networks using cluster analysis," In Proceedings of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2008, pp. 834–839, 2008.
92. Ren Xiu-li, Yang Wei, "Method of detecting the Sybil attack based on ranging in wireless sensor network," in Proceedings of WiCom '09, pp. 1–4, 2009.