REFERENCES

1. McHenry MA. NSF Spectrum Occupancy Measurements Project Summary. Shared Spectrum Company Report, Aug. 2005.

2. Unlicensed Operations in the TV Broadcast Bands, Second Memorandum Opinion and Order, FCC 10-174, Sep. 2010.

3. Small Entity Compliance Guide: Part 15 TV Band Devices, Second Report and Order and Memorandum Opinion and Order, FCC08-260, Nov. 2008.

4. K.M. Ali and A. Al-Khalifah, “A Comparative Study of Authentication Methods for Wi-Fi Networks”. IEEE Computer Society, pp. 190-194. DOI 10.1109/CICSyN.2011.49, 2011.

5. Unlicensed Operations in the TV Broadcast Bands, Second Memorandum Opinion and Order, FCC 10-174, Sep. 2010.

5. A. Gurtov, “Host Identity Protocol (HIP): Towards the Secure Mobile Internet,” Wiley Publishing, p. 332, 2008.

6.Small Entity Compliance Guide: Part 15 TV Band Devices, Second Report and Order and Memorandum Opinion and Order, FCC08-260, Nov. 2008.

7. Protocol to Access White-Space (PAWS) Databases draft-ietf-paws-protocol-20, 2014.

8. Mubark el at, “Fast and secure generating and exchanging a symmetric keys for TVWS Database” IJRG, 2015.

9. http://tools.ietf.org/html/rfc7238

11.G. Kbar “Improved SSL Application using Session Key based Double Key Encryption/Decryption (SDKED) ” Proceedings of the IASTED International Conference, Parallel and Distributed Computing and Networks, February 17-19,page 294-300, 2004.

12. Chun-I fan at , “Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs”, 2013.

13. Suneth Namal, Lightweight Authentication and Key Management on 802.11 with Elliptic Curve Cryptography, IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.

14. S. Pack, J. Choi, T. Kwon, and Y. Choi, “Fast Handoff Support in 802.11 Wireless Network". IEEE Communication Survey and Tutorial, 2007, pp. 1-25.

15. Pradeep K. Sinha, "Distributed Operating Systems Concepts and Design", IEEE Press, ISBN-81-2031380-1, 2009.

16. Kemal Bicakci, Bulent Tavli, “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks” Computer Standards & Interfaces Volume 31, Issue5,September, Pages 931-941, 2009.
17.Bellardo, J. and S. Savage, “802.11 Denial-Of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proceedings of the USENIX Security Symposium, Washington D.C., August 2003, 15 – 28.

18. IEEE 802.11 "Wireless LAN Security with Microsoft Windows Microsoft Corporation" Published: January 2008.
19. L. Zhou and Z. Haas. “Securing ad hoc networks.” IEEE Network, 13(6):24–30, 1999.
20. chun-I fan at , “Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs”, 2013.
21. C. He and J.C Mitchell, "Security Analysis and Improvements for IEEE 802.11i" Proceedings of the 12th Annual Network and Distributed System Security Symposium, 2005.
22. C.He, J.C.Mitchell, Security analysis and improvements for IEEE802.11i, Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05, pp.90-110), 2005.
23. IEEE 802.11 "Wireless LAN Security with Microsoft Windows Microsoft Corporation" Published: January 2008.

24. M. Beck and E. Tews, “Practical Attacks Against WEP and WPA” Proceedings of the second ACM conference on Wireless Network Security, pp. 79-86, 2009.
25. N. Bernaschi, F. Ferreri, L. Valcamonici, Access points vulnerabilities to DoS attacks in 802.11 networks, Wireless Networks, pp. 634-638, 2004.
26. Kemal Bicakci, Bulent Tavli, “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks” Computer Standards & Interfaces Volume 31, Issue5,September, Pages 931-941, 2009.
27. Qingkuan Dong, Lin Gao, A New Client-Puzzle Based DoS-Resistant Scheme of IEEE 802.11i Wireless Authentication Protocol , 2010.
28. chun-I fan at , “Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs”, 2013.
29. Suneth Namal, Lightweight Authentication and Key Management on 802.11 with Elliptic Curve Cryptography, IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.

30. E. Tews and M. Beck, “Practical attacks against WEP and WPA,” in Proceedings of the second ACM conference on Wireless network security. ACM, 2009, pp. 79–86.

31. Bellardo, J. and S. Savage, “802.11 Denial-Of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proceedings of the USENIX Security Symposium, Washington D.C., August 2003, 15 – 28.
32 Maxim, M. and D. Pollino, " Chapter 2, Wireless Threats, in Wireless Security", (McGraw-Hill Companies, 2002), 48 – 63.
33.Godber, A. and Partha Dasgupta, “Countering Rogues in Wireless Networks”, First International Workshop on Wireless Security and Privacy in conjunction with ICPP 2003,
Taiwan, October, 2003 425 – 431.
34. Wright, J., “Detecting Wireless LAN MAC Address Spoofing”, www.polarcove.com/whitepapers/, 3rd November 2003.
35. Stanley Wong, “The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards”, SANS Institute 2003.

36. C. He and J.C Mitchell, "Security Analysis and Improvements for IEEE 802.11i" Proceedings of the 12th Annual Network and Distributed System Security Symposium, 2005.
37. Rahmalia Syahputri, at “Fast and Secure Authentication in IEEE 802.11i Wireless LAN”, International Conference on Uncertainty Reasoning and Knowledge Engineering, 2012.

38. Rahmalia Syahputri, at “Fast and Secure Authentication in IEEE 802.11i Wireless LAN”, International Conference on Uncertainty Reasoning and Knowledge Engineering, 2012.
39. S. Frankel, B. Eydt, L.Owens, and K. Scarfone, "Establishing Wireless Robust Secure Network: A Guide to IEEE 802.11i". National Institute of Standards and Technology,
Technology administrations U.S, Department of Commerce, Special Publication 800 – 97, 2007.
40. JYH-CHENG CHEN el at , “WIRELESS LAN SECURITY AND IEEE 802.11i”, IEEE Wireless Communications • February 2005.
41. C.He, J.C.Mitchell, Security analysis and improvements for IEEE802.11i, Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05, pp.90-110), 2005.
42. Demian Lekomtcev, el at, Comparison of 802.11af and 802.22 standards – physical layer and cognitive functionality, elektro revue ISSN 1213-1539 VOL. 3, NO. 2, JUNE 2012.
43. Kang, H., et al., "Coexistence between 802.22 and 802.11af over TV white space", ICT Convergence (ICTC), International Conference on, September 2011, pp. 533 – 536, 2011.
44. [71] IEEE 802.11 Working Group, “IEEE 802.11af draft 4.0, Amendment 5: TV White Spaces Operation,” Apr. 2013.

45. "IEEE P802.11af™/D1.02 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 Amendment 3: TV White Spaces OperationU.S.", June 2011
46. Rahman, M. A., et al. "Channel Model Considerations for P802.11af" IEEE 11-10-0154-00-00af, Jan, 2010.
47. Barbeau,Michel.; “WiMax/802.16 Threat Analysis,” Association for Computing Machinery, pp. Oct. 2005.
48. Kolias, C.; Kambourakis, G.; Gritzalis, S., "Attacks and Countermeasures on 802.16: Analysis and Assessment," Communications Surveys & Tutorials, IEEE, No.99, pp.1-28, 2014.
49. Sidharth, Sreejesh; Sebastian, M.P., "A Revised Secure Authentication Protocol for IEEE 802.16 (e)," In proceeding of Advances in Computer Engineering (ACE), pp.34-38, 20-21 June 2010.
50. Cong Wang elt, “An enhanced authentication protocol for WRANs in TV white space”, security and communication networks , Security Comm. Networks 2015.
51. Protocol to Access White-Space (PAWS) Databases draft-ietf-paws-protocol-20
52. H. Karimi, “Geolocation databases for white space devices in the UHF TV bands: Specification of maximum permitted emission levels”, Proc. 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, May 2011.
53. R. Murty, R. Chandra, T. Moscibroda and P. Bahl, “SenseLess: A Database-Driven White Spaces Network”, Proc. 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, May 2011.
54. Jarkko Paavola and Arto Kivinen, “Device Authentication Architecture for TV White
Space Systems”, 19 international conference on cognitive radio oriented wireless networks, 2014.
55. S. Arkoulis, L. Kazatzopoulos, C. Delakouridis and G.F. Marias, “Cognitive Spectrum and its Security Issues”, Proc. The Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST 2008), Cardiff, Wales, 2008.

56. T. Brown and A. Sethi, “Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment”, Proc. 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2007), Orlando, USA, 2007.
57. Z. Chaczko, R. Wickramasooriya, R. Klempous and J. Nikodem, “Security Threats in Cognitive Radio Applications”, Proc. 14th International Conference on Intelligent Engineering Systems (INES 2010), Canary Islands, Spain, 2010.
58. S. Chen, K. Zeng and P. Mohapatra, “Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space”, Proc. The 30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011), Shanghai, China, 2011.
59. T.R. Newman, T.C. Clancy, M. McHenry and J.H. Reed, “Case Study: Security Analysis of a Dynamic Spectrum Access Radio System”, Proc. IEEE Global Communications Conference 2010 (GLOBECOM 2010), Miami, USA, 2010.
60. http://www.avispa-project.org/
61. G. Lowe. An Attack on the Needham-Schroeder Public-Key Authentication Protocol. Information Processing Letters, 56(3):131–136, November 1995.
62. J. Clark and J. Jacob. A survey of authentication protocol literature: Version 1.0., November 1997.
63. M. Burrows, M. Abadi, and R. Needham. A logic of authentication. ACM transactions on Computer Systems, 8(1):18–36, 1990.
64. L. Paulson. The inductive approach to verifying cryptographic protocols. Journal of Computer Security, 6(1):85.128, 1998.
65. F. J. T. Fábrega, J. C. Herzog, and J. D. Guttman. Strand spaces: Why a security protocol is correct? In Proceedings of the 1998 IEEE Symposium on Security and Privacy, pages 160.171. IEEE Computer Society Press, New York, May 1998.
66. C. Meadows. Open issues in formal methods for cryptographic protocol analysis. In Proceedings of the DARPA Information and Survivability

Conference and Exposition: DISCEX 2000, pages 237.250. IEEE Computer Society Press, January 2000.
67. J. R. Burch, E. M. Clarke, K. L. McMillan, D. L. Dill, and L. J. Hwang. Symbolic model
checking: 1020 states and beyond. Information and Computation, 98(2):142.170, June 1992.
68. K. L. McMillan. Symbolic model checking. Kluwer, Dordrecht, 1993.
69. Lamport. The temporal logic of actions. ACM Trans. Program. Lang. Syst., 16(3):872.923,
1994.
70. Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drieslma, J. Mantovani, S. Mödersheim, and L. Vigneron. A High Level Protocol Speci_cation Language for Industrial Security-Sensitive
Protocols. In Automated Software Engineering. Proceedings of the Workshop on Speci_cation
and Automated Processing of Security Requirements, SAPS'04, pages 193.205. Austrian Computer Society, Austria, September 2004.
71. AVISPA. Deliverable 2.1: The High-Level Protocol Speci_cation Language. Available at http: //www.avispa-project.org, 2003.
72. J. Millen and G. Denker. MuCAPSL. In DISCEX III, DARPA Information Survivability Conference and Exposition, pages 238–249. IEEE Computer Society, 2003.
73. J. Cuellar, I. Wildgruber, and D. Barnard. The temporal logic of transitions. In Formal Methods Europe, 1994.
74. G. J. Holzmann. Design and validation of computer protocols. Prentice-Hall, Inc., 1991.
75. M. Burrows, M. Abadi, and R. Needham. A logic of authentication. ACM Transactions on
Computer Systems, 8(1):18.36, 1990.
76. D. Nessett. A critique of the Burrows, Abadi and Needham logic. ACM Operating Systems

Review, 24(2):35.38, April 1990.
77. P. C. van Oorschot. An alternate explanation of two ban-logic ¨failures¨ . In EUROCRYPT '93:Workshop on the theory and application of cryptographic techniques on Advances in cryptology,pages 443.447. Springer-Verlag New York, Inc., 1994.
78. L. Paulson. The inductive approach to verifying cryptographic protocols. Journal of Computer Security, 6(1):85.128, 1998.
79. [44] L. C. Paulson. Mechanized proofs for a recursive authentication protocol. In 10th ComputerSecurity Foundations Workshop, pages 84–95. IEEE Computer Society Press, 1997.
80. L. C. Paulson. Isabelle: a Generic Theorem Prover. LNCS 828. Springer-Verlag, 1994.
81. G. Lowe. Casper: a Compiler for the Analysis of Security Protocols. Journal of Computer Security, 6(1):53–84, 1998. See http://web.comlab.ox.ac.uk/oucl/work/gavin.lowe/Security/Casper/.
82. J. K. Millen. Capsl: Common authentication protocol speci_cation language. In Proceedings of the 1996 workshop on New security paradigms, page 132, 1996.
83. A. Armando, D. Basin, M. Bouallagui, Y. Chevalier, L. Compagna, S. Mödersheim, M. Rusinowitch, M. Turuani, L. Viganò, and L. Vigneron. The aviss security protocol analysis tool. In Computer-Aided Veri_cation CAV'02, Lecture Notes in Computer Science 2404, pages 349.353. Springer-Verlag, 2002.
84. J. Millen and G. Denker. CAPSL and MuCAPSL. Journal of Telecommunications and Information Technology, (4):16–27, 2002.
85. Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drieslma, J. Mantovani, S. Mödersheim, and L. Vigneron. A High Level Protocol Speci_cation Language for Industrial Security-Sensitive
Protocols, volume 180 of Automated Software Engineering, pages 193.205. Austrian Computer
Society, Austria, September 2004.

86. Bianchi, G. Performance analysis of the IEEE 802.11 distributed coordination function. IEEE Journal on Selected Areas in Communications, 18(3), 535-547. 2000.

87. Broadcom IEEE 802.11g: the new mainstream wireless LAN standard. Retrieved May 23 2007, from http://www.54g.org/pdf/802.11g-WP104-RDS1. 2003.

88. IEEE Std. 802.16e-2004, IEEE Standard for Local and Metropolitan Area Networks, part 16, “Air Interface for Fixed Broadband Wireless Access Systems,” IEEE Press, 2004.

89. Bogdanoski, Mitko.; Latkoski, Pero.; Risteski, Aleksandar.; Popovski, Borislav.; “IEEE 802.16 Security Issues: A Survey,” In proceeding of TELFOR, 16th Telecommunications Forum, pp., 25-27 Nov. 2008

90. WiMax forum, Frequently asked questions http://www.wimaxforum.org/technology/faq/

91. Habib, M.; Mehmood, T.; Ullah, F.; Ibrahim, M., "Performance of WiMAX Security Algorithm (The Comparative Study of RSA Encryption Algorithm with ECC Encryption Algorithm)," In proceeding of Computer Technology and Development, 2009 (ICCTD '09), Vol. 2, pp.108-112, 13-15 Nov. 2009.

92. Lang Wei-min; Zhong Jing-li; Li Jian-jun; Qi Xiang-yu, "Research on the Authentication Scheme of WiMAX," In proceeding of Wireless Communications, Networking and Mobile Computing, (WiCOM '08), pp.1-4, Oct. 2008.

93. Abdul Maalik at, “Implementation of MAC Layer Security Protocol in WiMAX Using OMNET++ Simulator”, International Journal of Computer Science and Telecommunications ,Volume 4, Issue 8, August, 2013.

94. B. Sridevi, “Performance Analysis of Proposed Cost Reduction Mechanisms for authentication in Mobile WiMAX Network Entry Process”, Arab J Sci Eng, 39:4727–4735, 2014

95. Kamal Ali Alezabi, A New Tunnelled EAP based Authentication Method for WiMAX Networks, IEEE 11th Malaysia International Conference on Communications 26th - 28th November 2013, Kuala Lumpur, Malaysia, 2013.

96. A. Rai, V. Kumar, and S. Mishra, “An efficient password authenticated key exchange protocol for wlan and wimax,” in Proceedings of the In-ternational Conference & Workshop on Emerging Trends in Technology, pp. 881–885, ACM, 2011.

97. Wireless medium access control and physical layer specifications for low-rate wireless personal area networks. IEEE Standard, 802.15.4-2003.ISBN 0-7381-3677-5, May 2003.

98. IEEE P802.19/D1.02 Draft Standard for Information Technology - Telecommunications and information exchange between systems - Steve Shellhammer (Qualcomm and Chair, IEEE 802.19 WG).

100. IEEE Std. 802.22, Information Technology—Local and metropolitan area networks—Specific Requirements— Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands,
Jul. 2011; pp.1–680.
101. Cordeiro C, Challapali K, Birru D, Shankar S. IEEE 802.22: an introduction to the first wireless standard based on cognitive radios. Journal of Communications; 1(1):38–47, 2006.
102. Stevenson C, Chouinard G, Hu W, Shellhammer S, Caldwell W. IEEE2.22: the first cognitive radio wireless regional area network standard. IEEE Communication Magazine 47(1):130–138, 2009.
103. "IEEE Std 802.22™-2011 IEEE Standard for Information Technology - Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN) - Specific requirements - Part 22:
Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands", July 2011.
104. "IEEE Std 802.22™-2011 IEEE Standard for Information Technology - Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN) - Specific requirements - Part 22:Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands", July 2011.
105. “IEEE 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,” tech.rep., Dec. 2007., Tech. Rep.
106. M. Li, W. Lou, and K. Ren. “Data security and privacy in wireless body area networks.” IEEE Wireless Communications, 17(1):51–58, 2010.
107. Maithili Narasimha, "Applied Cryptography" , ISPN 1255-6858, 2010.
108. Shamima Sultana , Improved Needham-Schroeder Protocol for Secured and Efficient Key Distributions, Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009), Dhaka, Bangladesh, 21-23 December 2009.