8. REFERENCES

[1] J. Postel, "Transmission Control Protocol, RFC 793," September 1981.

[2] O. Bonaventure, M. Handley and C. Raiciu, "An overview of Multipath TCP," *login,* vol. 37, no. 5, pp. 17-23, 2012.

[3] A. Ford, C. Raiciu, M. Handley and O. Bonaventure, "RFC 6824 TCP Extensions for Multipath Operation with Multiple Addresses," 2013.

[4] O. Dharmadhikari, "5G Link Aggregation with Multipath TCP (MPTCP)," CableLabs Logo, 2019.

[5] L. Chao, C. Wu, T. Yoshinaga, W. Bao and Y. Ji., "A Brief Review of Multipath TCP for Vehicular Networks," *Sensors,* vol. 21, no. 8, p. 2793, 2021.

[6] A. Hamza, M. I. Lali, F. Javid and M. u. Din., "Study of MPTCP with Transport Layer Security," in *Proceedings of the 3rd International Conference on Engineering & Emerging Technologies (ICEET)*, Superior University, Lahore, PK, 7-8 April, 2016.

[7] A. Bittau, D. Boneh, M. Hamburg, M. Handley, D. Mazieres and Q. Slack, "Cryptographic protection of TCP Streams (tcpcrypt)," Internet-Draft draft-ietf-tcpinc-tcpcrypt-03, 2014.

[8] J. Díez, M. Bagnulo, F. Valera and I. Vidal, "Security for multipath TCP: a constructive approach.," *International Journal of Internet Protocol Technology,* vol. 6, no. (3), pp. 146-155., 2011.

[9] A. Krishnan, P. P. Amritha and M. Sethumadhavan, "Sum Chain Based Approach against Session Hijacking in MPTCP," in *7th International Conference on Advances in Computing & Communications, ICACC-2017*, Cochin, India, 2017.

[10] R. Melki, A. Hussein and A. Chehab, "Enhancing Multipath TCP Security Through Software Defined Networking," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019.

[11] G. Noh, H. Park, H. Roh and W. Lee, "Secure and Lightweight Subflow Establishment of Multipath-TCP.," *IEEE Access,* vol. 7, pp. 177438-177448, 2019.

[12] K. Popat and D. V. Kapadia, "Recent Trends in Security Threats in Multi-Homing Transport Layer Solutions," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 5641-5648, 2020.

[13] A. Kostopoulos, H. Warma, T. Levä, B. Heinrich, A. Ford and L. Eggert, "Towards multipath TCP adoption: challenges and opportunities," in *6th EURO-NGI Conference on Next Generation Internet*, 2010.

[14] "Use Multipath TCP to create backup connections for iOS," Apple, 2017.

[15] G. Detal, S. Barré, B. Peirens and O. Bonaventure, "Leveraging Multipath TCP to create Hybrid Access Networks," in *SIGCOMM*, Los Angeles, CA, USA, 2017.

[16] O. Bonaventure, "The first Multipath TCP enabled smartphones," Multipath-TCP, 10 12 2018. [Online]. Available: http://blog.multipath-tcp.org/blog/html/2018/12/10/the_first_multipath_tcp_enabled_smartphones.html. [Accessed 1 1 2022].

[17] O. Bonaventure, "Multipath TCP in the datacenter," 11 12 2018. [Online]. Available: http://blog.multipath-tcp.org/blog/html/2018/12/11/multipath_tcp_in_the_datacenter.html. [Accessed 1 1 2022].

[18] Q. Zhao, P. Du, J. Mena and M. Gerla, "Software Defined Multi-Path TCP Solution for Mobile Wireless Tactical Networks," in *2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, 2018.

[19] Q. Zhao, P. Du, J. Mena and M. Gerla, "A Multi-path TCP Solution for Software-Defined Military Heterogeneous Network," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2018.

[20] A. Ford, C. Raiciu, M. Handley and O. Bonaventure, "Architectural Guidelines for Multipath TCP Development (RFC6182)," Internet Engineering Task Force (IETF), March 2011.

[21] A. Ford, C. Raiciu, M. Handley, O. Bonaventure and C. Paasch, "TCP Extensions for Multipath Operation with Multiple Addresses RFC6824(if approved)," draft-ietf-mptcp-rfc6824bis-12, 2018.

[22] T. Wijethilake, K. Gunawardana, C. Keppitiyagama and K. De Zoyza, "Alternative Approach for Authenticating Subflows of Multipath Transmission Control Protocol using Application Level Key," in *13th International Research Conference- KDU*, At: Colombo, 2020.

[23] M. Bagnulo, C. Paasch, F. Gont, O. Bonaventure and C. Raiciu, "Analysis of residual threats and possible fixes for multipath TCP (mptcp)," (No. RFC 7430), 2015.

[24] F. DEMARIA, "Security Evaluation of Multipath TCP, Analyzing and fixing Multipath TCP vulnerabilities, contributing to the Linux Kernel implementation of the new version of the protocol (PhD Thesis)," March 2016.

[25] A. Munir, Z. Qian, Z. Shafiq, A. Liu and F. Le, "Multipath TCP traffic diversion attacks and countermeasures," in *IEEE 25th International Conference on Network Protocols (ICNP)*, Toronto, ON, Canada, 2017.

[26] V. A. Kumar, D. Das and S. M. IEEE., "Data sequence signal manipulation in multipath TCP (MPTCP): The vulnerability, attack and its detection.," *Computers & Security*, vol. 103, p. 102180, 2021.

[27] K. Popat and V. V. Kapadia, "Multipath TCP Security Issues, Challenges and Solutions," in *Information, Communication and Computing Technology.Communications in Computer and Information Science*, 2021.

[28] A. S. Almuflih, K. Popat, V. V. Kapdia, M. R. N. M. Qureshi, N. Almakayeel and a. R. E. A. Mamlook, "Efficient Key Exchange Using Identity-Based Encryption in Multipath TCP Environment," *Efficient Key Exchange Using Identity-Based Encryption in Multipath TCP Environment*, vol. 12, no. 15, p. 7575, 2022.

[29] S. Barré, C. Paasch and O. Bonaventure., "Multipath TCP: from theory to practice," in *International Conference on Research in Networking.*, Berlin, Heidelberg, 2011.

[30] K. J. Popat, J. Raval, S. Johnson and B. Patel., "Experimental Evaluation of Multipath TCP with MPI," in *In Proceedings of the Third International Symposium on Women in Computing and Informatics*, 2015.

[31] R. Khalili, N. Gast and M. Popovic, "Opportunistic linked-increases congestion control algorithm for MPTCP," 2013.

[32] Y. Cao, M. Xu and X. Fu, "Delay-based congestion control for multipath TCP," in *2012 20th IEEE international conference on network protocols (ICNP)*, 2012.

[33] C. Raiciu, M. Handley and D. Wischik, "Coupled congestion control for multipath transport protocols (RFC 6356)," Internet Engineering Task Force (IETF), 2011.

[34] B. A. Forouzan and D. Mukhopadhyay, Cryptography and network security, New York, NY, USA: Mc Graw Hill Education (India) Private Limited, 2015.

[35] G. Tihon, M. Jadin, O. Pereira and a. O. Bonaventure, "Secure MultiPath TCP: design and implementation.," 2015-2016.

[36] W. Stallings, Cryptography and network security, 4/E, Pearson Education India, 2006.

[37] R. Bhanot and R. Hans., "A review and comparative analysis of various encryption algorithms.," *nternational Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289-306, 2015.

[38] M. Harini, K. P. Gowri, C. Pavithra and M. P. Selvarani, "Comparative study and analysis of various Cryptographic Algorithms," *International Journal of Scientific & Engineering Research*, vol. 8, no. 5, p. 2229, 2017.

[39] S. Kumari, "A research Paper on Cryptography Encryption and Compression Techniques," *International Journal of Engineering and Computer Science*, vol. 6, no. 4, 2017.

[40] F. Maqsood, M. Ahmed, M. M. Ali and M. A. Shah, "Cryptography: a comparative analysis for modern techniques," *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 6, 2017.

[41] M. Jadin, G. Tihon, O. Pereira and O. Bonaventure, "Securing multipath TCP: Design & implementation," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*.

[42] F. Mallouli, A. Hellal, N. S. Saeed and F. A. Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2019.

[43] R. K. Chaturvedi and S. Chand., "Multipath TCP security over different attacks.," *Transactions on Emerging Telecommunications Technologies,* vol. 31, no. 9, p. 4081, 2020.

[44] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM journal on computing,* vol. 32, no. 3, pp. 586-615, 2003.

[45] V. Pandya, A. Saiyed and K. Patel, "Recent Advancement in Fine-Grained Access Control and Secure Data Sharing Scheme for Distributed Environment," in *Emerging Technologies for Computing, Communication and Smart Cities*, 2022.

[46] M. Bagnulo, "Threat Analysis for TCP Extensions for Multi-path Operation with Multiple Addresses," draft-ietf-mptcp-threat-08, 2011.

[47] M. Z. Shafiq, F. Le, M. Srivatsa and A. X. Liu., "Cross-path inference attacks on multipath tcp," in *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*, 2013.

[48] D.-Y. Kim and H.-K. Choi, "Efficient design for secure multipath TCP against eavesdropper in initial handshake," in *International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2016.

[49] S. Costea, M. O. Choudary, D. Gucea, B. Tackmann and C. Raiciu., "Secure opportunistic multipath key exchange," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Securit*, 2018.

[50] C. Paasch and O. Bonaventure, "Securing the MultiPath TCP handshake with external keys," Work in Progress, draft-paasch-mptcp-ssl-00, 2012.

[51] O. Bonaventure, "MPTLS : Making TLS and Multipath TCP stronger together," 2015.

[52] T. Kato, S. Cheng, R. Yamamoto, S. Ohzahata and N. Suzuki, "Protecting Eavesdropping over Multipath TCP Communication Based on Not-Every-Not-Any Protection," in *SECURWARE 2017 : The Eleventh International Conference on Emerging Security Information, Systems and Technologies*, 2017.

[53] O. Bonaventure, "Multipath TCP: An annotated bibliography.," *ICTEAM, UCL,* 2015.

[54] "Elliptic-curve cryptography," [Online]. Available: https://en.wikipedia.org/wiki/Elliptic-curve_cryptography. [Accessed 01 04 2022].

[55] M. Bagnulo, "Secure MPTCP, draft-bagnulo-mptcp-secure-00," ietf-bagnulo-mptcp-secure-00, 2014.

[56] C. a. O. B. aasch, "Securing the MultiPath TCP handshake with external keys," Work in Progress, draft-paasch-mptcp-ssl-00, 2012.

[57] V. Shah and V. Kapadia, "Load Balancing by Process Migration in Distributed Operating System.," *International Journal of Soft Computing and Engineering (IJSCE),* vol. 2, no. 1, pp. 361-363, 2012.

[58] C. D. Phung, S. Secci, B. Felix and M. Nogueira, "Can MPTCP secure Internet communications from man-in-the-middle attacks?," in *13th International Conference on Network and Service Management (CNSM),* Tokyo, Japan, 2017.

[59] C. Pearce and S. Zeadally, "Ancillary Impacts of Multipath TCP on Current and Future Network Security," *IEEE Internet Computing,* vol. 19, no. 5, pp. 58-65, 2015.

[60] S. Patil, R. Raut, R. Jhaveri*, T. Ahanger, P. Dhade, A. Kathole and K. Vhatkar, "Robust Authentication System with Privacy preservation of Biometrics," *Security and Communication Networks,* vol. 2022, p. 14, 2022.

[61] C. Patel, D. Joshi, N. Doshi, V. A. and R. Jhaveri, "An enhanced approach for three factor remote user authentication in multi - server environment," *Journal of Intelligent & Fuzzy Systems,* vol. 39, no. 6, pp. 8609-8620, 2020.

[62] J. Ma, F. Le, A. Russo and J. Lobo, "Detecting distributed signature-based intrusion: The case of multi-path routing attacks.," in *IEEE Conference on Computer Communications (INFOCOM),* 2015.

[63] V. V. Kapadia and V. K. Thakar., "Combinatorial system design for high performance memory management.," in *2013 15th International Conference on Advanced Computing Technologies (ICACT),* 2013.

[64] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh and B. Yoon, "CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment.," *IEEE Access* , vol. 10, pp. 11354-11371, 2022.

[65] O. Bonaventure, "Important Milestone for Multipath TCP," Tessares, 10 April 2020. [Online]. Available: https://www.tessares.net/important-milestone-for-multipath-tcp/. [Accessed 1 1 2022].

[66] "Opening the way to 4G / 5G Wi-Fi Convergence (NEW)," tessares, 2020.

[67] "5G & Wi-Fi: from coexistence to convergence," tessares.

[68] F. Li and M. K. Khan, "A survey of identity-based signcryption," *IETE Technical Review,* vol. 28, no. 3, pp. 265-272, 2011.