Bibliography

[1] J. G. McNeff, "The global positioning system," *IEEE Transactions on Microwave theory and techniques*, vol. 50, no. 3, pp. 645–652, 2002.

[2] K. Etemad, "Overview of mobile wimax technology and evolution," *IEEE communications magazine*, vol. 46, no. 10, pp. 31–40, 2008.

[3] E. Hajlaoui, A. Zaier, A. Khlifi, J. Ghodhbane, M. B. Hamed, and L. Sbita, "4g and 5g technologies: A comparative study," in *2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, pp. 1–6, IEEE, 2020.

[4] P. Marsch, I. Da Silva, O. Bulakci, M. Tesanovic, S. E. El Ayoubi, T. Rosowski, A. Kaloxylos, and M. Boldi, "5g radio access network architecture: Design guidelines and key considerations," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 24–32, 2016.

[5] M. G. Rahman and H. Imai, "Security in wireless communication," *Wireless personal communications*, vol. 22, no. 2, pp. 213–228, 2002.

[6] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for authentication and key establishment*, vol. 1. Springer, 2003.

[7] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 8, pp. 1608–1617, 1997.

[8] 3GPP tech. rep., TR 36.839 v11.1.0; Evolved Universal Terrestrial Radio Access (E-UTRA); Mobility Enhancements in Heterogeneous Networks (Release 11), 2012.

[9] 3GPP tech. rep., TR 38.872 v12.1.0; Small cell enhancements for E-UTRA and E-UTRAN - Physical layer aspects (Release 12), 2013.

[10] 3GPP tech. rep., TR 36.932 V12.1.0; LTE; Scenarios and requirements for small cell enhancements for E-UTRA and E-UTRAN (Release 12), 2014.

[11] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in iot," *IEEE access*, vol. 3, pp. 622–637, 2015.

[12] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2017.

[13] S. Steiniger, M. Neun, and A. Edwardes, "Foundations of location based services," *Lecture notes on LBS*, vol. 1, no. 272, p. 2, 2006.

[14] L. Sharma, A. Javali, R. Nyamangoudar, R. Priya, P. Mishra, and S. K. Routray, "An update on location based services: Current state and future prospects," in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 220–224, IEEE, 2017.

[15] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," *Wireless Personal Communications*, vol. 84, no. 2, pp. 1487–1508, 2015.

[16] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Transactions on wireless communications*, vol. 5, no. 9, pp. 2569–2577, 2006.

[17] M. K. Giluka, M. S. A. Khan, G. Krishna, T. A. Atif, V. Sathya, and B. R. Tamma, "On handovers in uplink/downlink decoupled lte hetnets," in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–6, IEEE, 2016.

[18] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE transactions on information forensics and security*, vol. 11, no. 9, pp. 2052–2064, 2016.

[19] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Transactions on industrial electronics*, vol. 63, no. 11, pp. 7124–7132, 2016.

[20] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE transactions on industrial informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.

[21] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, 2004.

[22] F. Shahzad, M. Pasha, and A. Ahmad, "A survey of active attacks on wireless sensor networks and their countermeasures," *arXiv preprint arXiv:1702.07136*, 2017.

[23] T. Jamal, P. Amaral, A. Khan, A. Zameer, K. Ullah, and S. A. Butt, "Denial of service attack in wireless lan," *ICDS 2018*, vol. 51, 2018.

[24] C. Tang and D. O. Wu, "Mobile privacy in wireless networks-revisited," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 1035–1042, 2008.

[25] D. Samfat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in *Proceedings of the 1st annual international conference on Mobile computing and networking*, pp. 26–36, 1995.

[26] S. Steinbrecher and S. Köpsell, "Modelling unlinkability," in *International workshop on privacy enhancing technologies*, pp. 32–47, Springer, 2003.

[27] Z. Chen, S. Guo, R. Duan, and S. Wang, "Security analysis on mutual authentication against man-in-the-middle attack," in *2009 First International Conference on Information Science and Engineering*, pp. 1855–1858, IEEE, 2009.

[28] A. G. Reddy, A. K. Das, E.-J. Yoon, and K.-Y. Yoo, "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography," *IEEE access*, vol. 4, pp. 4394–4407, 2016.

[29] V. Odelu, S. Banerjee, A. K. Das, S. Chattopadhyay, S. Kumari, X. Li, and A. Goswami, "A secure anonymity preserving authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2351–2387, 2017.

[30] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*, pp. 388–397, Springer, 1999.

[31] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE transactions on computers*, vol. 51, no. 5, pp. 541–552, 2002.

[32] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[33] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[34] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[35] R. Roman, C. Alcaraz, and J. Lopez, "A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes," *Mobile Networks and Applications*, vol. 12, no. 4, pp. 231–244, 2007.

[36] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, 2015.

[37] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and network security*, vol. 12. Mc Graw Hill Education (India) Private Limited New York, NY, USA:, 2015.

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

[39] Y. Watanabe, J. Shikata, and H. Imai, "Equivalence between semantic security and indistinguishability against chosen ciphertext attacks," in *International Workshop on Public Key Cryptography*, pp. 71–84, Springer, 2003.

[40] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[41] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[42] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, Springer, 1985.

[43] W. Diffie, "New direction in cryptography," *IEEE Transactions on on Information Theory*, vol. 22, pp. 472–492, 1976.

[44] R. Haakegaard and J. Lang, "The elliptic curve diffie-hellman (ecdh)," *Online at https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Haakegaard+ Lang. pdf*, 2015.

[45] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.

[46] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *computer*, vol. 35, no. 10, pp. 54–62, 2002.

[47] C. Shouqi, L. Wanrong, C. Liling, S. Qing, and H. Xin, "An improved anonymous authentication protocol for location-based service," *IEEE Access*, vol. 7, pp. 114203–114212, 2019.

[48] R. Shashidhara, S. Bojjagani, A. K. Maurya, S. Kumari, and H. Xiong, "A robust user authentication protocol with privacy-preserving for roaming service in mobility environments," *Peer-to-peer networking and applications*, vol. 13, no. 6, pp. 1943–1966, 2020.

[49] Y. Lu, G. Xu, L. Li, and Y. Yang, "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1454–1465, 2019.

[50] B. Lee and K. Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," in *International conference on information security and cryptology*, pp. 389–406, Springer, 2002.

[51] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K.-K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739–8752, 2019.

[52] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended chebyshev chaotic maps," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4815–4828, 2018.

[53] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *International workshop on public key cryptography*, pp. 65–84, Springer, 2005.

[54] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Transactions on wireless communications*, vol. 15, no. 1, pp. 357–366, 2015.

[55] D. Mohapatra and S. Suma, "Survey of location based wireless services," in *2005 IEEE International Conference on Personal Wireless Communications, 2005. ICPWC 2005.*, pp. 358–362, IEEE, 2005.

[56] C. Bae, J. Yoo, K. Kang, Y. Choe, and J. Lee, "Home server for home digital service environments," *IEEE Transactions on Consumer electronics*, vol. 49, no. 4, pp. 1129–1135, 2003.

[57] I. Han, H.-S. Park, Y.-K. Jeong, and K.-R. Park, "An integrated home server for communication, broadcast reception, and home automation," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 1, pp. 104–109, 2006.

[58] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for iot applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[59] T. Demuth and A. Rieke, "Securing the anonymity of content providers in the world wide web," in *Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 494–502, SPIE, 1999.

[60] B. Gupta, V. Prajapati, N. Nedjah, P. Vijayakumar, A. A. A. El-Latif, and X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (tmis)," *Neural Computing and Applications*, pp. 1–26, 2021.

[61] L. Meng, H. Xu, H. Xiong, X. Zhang, X. Zhou, and Z. Han, "An efficient certificateless authenticated key exchange protocol resistant to ephemeral key leakage attack for v2v communication in iov," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11736–11747, 2021.

[62] Y. Lu, L. Li, and Y. Yang, "Robust and efficient authentication scheme for session initiation protocol," *Mathematical problems in engineering*, 2015.

[63] M. Hölbl, T. Welzer, and B. Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," *Journal of Computer and System Sciences*, vol. 78, no. 1, pp. 142–150, 2012.

[64] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE transactions on wireless communications*, vol. 10, no. 2, pp. 431–436, 2010.

[65] Y. Yang, L. Zhang, Y. Zhao, K.-K. R. Choo, and Y. Zhang, "Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 317–331, 2022.

[66] C.-I. Fan, J.-J. Huang, M.-Z. Zhong, R.-H. Hsu, W.-T. Chen, and J. Lee, "Rehand: Secure region-based fast handover with user anonymity for small cell networks in mobile communications," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 927–942, 2019.

[67] D. Zhao, Z. Yan, M. Wang, P. Zhang, and B. Song, "Is 5g handover secure and private? a survey," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12855–12879, 2021.

[68] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between henb and enb in lte networks," *Computer Networks*, vol. 56, no. 8, pp. 2119–2131, 2012.

[69] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[70] D. He, S. Chan, and M. Guizani, "Handover authentication for mobile networks: security and efficiency aspects," *IEEE Network*, vol. 29, no. 3, pp. 96–103, 2015.

[71] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48–53, 2011.

[72] F. Van Den Broek, R. Verdult, and J. De Ruiter, "Defeating imsi catchers," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 340–351, 2015.

[73] S. J. Ramson and D. J. Moni, "Applications of wireless sensor networks—a survey," in *2017 international conference on innovations in electrical, electronics, instrumentation and media technology (ICEEIMT)*, pp. 325–329, IEEE, 2017.

[74] X. Shen, Z. Wang, and Y. Sun, "Wireless sensor networks for industrial applications," in *Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No. 04EX788)*, vol. 4, pp. 3636–3640, IEEE, 2004.

[75] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on industrial electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[76] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[77] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical internet of things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019.

[78] G. Inc, "Gartner identifies top 10 strategic iot technologies and trends. [online] available:https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends," 2018.

[79] L. S. Vailshery, "Internet of things (iot) and non-iot active device connections worldwide from 2010 to 2025." https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/, 2021. [Online; accessed 10-August-2022].

[80] T. Limbasiya, S. K. Sahay, and B. Sridharan, "Privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system," *Information Systems Frontiers*, vol. 23, no. 4, pp. 835–848, 2021.

[81] J. Wang, Y. Zhu, *et al.*, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5g networks," *Journal of Network and Computer Applications*, vol. 161, p. 102660, 2020.

[82] T.-Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar, and C.-M. Chen, "An authenticated key exchange protocol for multi-server architecture in 5g networks," *IEEE Access*, vol. 8, pp. 28096–28108, 2020.

[83] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5g networks using self-certified public key cryptography," *Journal of Network and Computer Applications*, vol. 131, pp. 66–74, 2019.

[84] B. Ng, A. Si, R. W. Lau, and F. W. Li, "A multi-server architecture for distributed virtual walkthrough," in *Proceedings of the ACM symposium on Virtual reality software and technology*, pp. 163–170, 2002.

[85] M. Chorzempa, J.-M. Park, M. Eltoweissy, and T. Hou, "Key management for wireless sensor networks in hostile environments," *Paper submitted to the Faculty of the Virginia Polytechnic Institute and State University*, 2006.

[86] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 39–95, 2017.

[87] J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *IEEE INFOCOM 2009*, pp. 1773–1781, IEEE, 2009.

[88] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems," *Department of Computer Science University of Colorado at Boulder*, 2005.

[89] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-wsn: Software-defined wsn management system for iot applications," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2074–2081, 2016.

[90] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 27–51, 2014.

[91] C. J. Bernardos, A. De La Oliva, P. Serrano, A. Banchs, L. M. Contreras, H. Jin, and J. C. Zúñiga, "An architecture for software defined wireless networking," *IEEE wireless communications*, vol. 21, no. 3, pp. 52–61, 2014.

[92] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, and I. Rashid, "Alam: Anonymous lightweight authentication mechanism for sdn-enabled smart homes," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9622–9633, 2020.

[93] A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untraceability for 5g-enabled softwarized industrial cyber-physical systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2316–2330, 2021.

[94] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones–a survey of attitudes and practices," *Computers & Security*, vol. 24, no. 7, pp. 519–527, 2005.

[95] N. L. Clarke and S. Furnell, "Advanced user authentication for mobile devices," *computers & security*, vol. 26, no. 2, pp. 109–119, 2007.

[96] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the pin: Enhancing user authentication for mobile devices," *Computer fraud & security*, vol. 2008, no. 8, pp. 12–17, 2008.

[97] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247–269, 2014.

[98] K. M. Shelfer and J. D. Procaccino, "Smart card evolution," *Communications of the ACM*, vol. 45, no. 7, pp. 83–88, 2002.

[99] Y. Cao, Y. Li, H. Li, and X. Wang, "An anonymous authentication protocol for privacy protection in location based services," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–5, IEEE, 2008.

[100] C.-C. Lee, M.-S. Hwang, and I.-E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[101] C.-C. Wu, W.-B. Lee, and W.-J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722–723, 2008.

[102] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 214–222, 2012.

[103] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Computer Communications*, vol. 32, no. 4, pp. 611–618, 2009.

[104] T. Zhou and J. Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks," *Computer Networks*, vol. 55, no. 1, pp. 205–213, 2011.

[105] D. He, S. Chan, C. Chen, J. Bu, and R. Fan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 61, no. 2, pp. 465–476, 2011.

[106] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in *International workshop on fast software encryption*, pp. 371–388, Springer, 2004.

[107] Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless personal communications*, vol. 68, no. 4, pp. 1477–1491, 2013.

[108] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *International Journal of Communication Systems*, vol. 24, no. 3, pp. 347–362, 2011.

[109] Q. Xie, M. Bao, N. Dong, B. Hu, and D. S. Wong, "Secure mobile user authentication and key agreement protocol with privacy protection in global mobility networks," in *2013 International Symposium on Biometrics and Security Technologies*, pp. 124–129, IEEE, 2013.

[110] M. S. Farash, S. A. Chaudhry, M. Heydari, S. M. Sajad Sadough, S. Kumari, and M. K. Khan, "A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security," *International Journal of Communication Systems*, vol. 30, no. 4, p. e3019, 2015.

[111] F. Wu, L. Xu, S. Kumari, X. Li, M. K. Khan, and A. K. Das, "An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks," *Annals of Telecommunications*, vol. 72, no. 3, pp. 131–144, 2017.

[112] S. A. Chaudhry, A. Albeshri, N. Xiong, C. Lee, and T. Shon, "A privacy preserving authentication scheme for roaming in ubiquitous networks," *Cluster Computing*, vol. 20, no. 2, pp. 1223–1236, 2017.

[113] A. M. Rahmani, M. Mohammadi, J. Lansky, S. Mildeova, M. Safkhani, S. Kumari, S. H. T. Karim, and M. Hosseinzadeh, "Amapg: advanced mobile authentication protocol for glomonet," *IEEE Access*, vol. 9, pp. 88256–88271, 2021.

[114] J. Ryu, H. Lee, Y. Lee, and D. Won, "Smasg: Secure mobile authentication scheme for global mobility network," *IEEE Access*, vol. 10, pp. 26907–26919, 2022.

[115] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Systems Journal*, vol. 10, no. 4, pp. 1370–1379, 2016.

[116] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless communications*, vol. 11, no. 1, pp. 62–67, 2004.

[117] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical performance comparison of ecc and rsa for resource-constrained iot devices," in *2018 Global Internet of Things Summit (GIoTS)*, pp. 1–6, IEEE, 2018.

[118] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet x. 509 public key infrastructure certificate and crl profile," tech. rep., 1999.

[119] F. Wei, P. Vijayakumar, Q. Jiang, and R. Zhang, "A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 268–278, 2018.

[120] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," *Future Generation Computer Systems*, vol. 83, pp. 607–618, 2018.

[121] M. Gupta and N. S. Chaudhari, "Anonymous two factor authentication protocol for roaming service in global mobility network with security beyond traditional limit," *Ad Hoc Networks*, vol. 84, pp. 56–67, 2019.

[122] Q. Xie and L. Hwang, "Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city," *Neurocomputing*, vol. 347, pp. 131–138, 2019.

[123] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1382–1392, 2017.

[124] M. Ghahramani, R. Javidan, and M. Shojafar, "A secure biometric-based authentication protocol for global mobility networks in smart cities," *The Journal of supercomputing*, vol. 76, no. 11, pp. 8729–8755, 2020.

[125] M. Nikooghadam, H. Amintoosi, and S. Kumari, "A provably secure ecc-based roaming authentication scheme for global mobility networks," *Journal of Information Security and Applications*, vol. 54, p. 102588, 2020.

[126] S. Khatoon, T.-Y. Chen, and C.-C. Lee, "An improved user authentication and key agreement scheme for roaming service in ubiquitous network," *Annals of Telecommunications*, pp. 1–20, 2022.

[127] F. Wen, W. Susilo, and G. Yang, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks," *Wireless personal communications*, vol. 73, no. 3, pp. 993–1004, 2013.

[128] P. Gope and T. Hwang, "Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks," *Wireless Personal Communications*, vol. 82, no. 4, pp. 2231–2245, 2015.

[129] G. Zhang, D. Fan, Y. Zhang, X. Li, and X. Liu, "A privacy preserving authentication scheme for roaming services in global mobility networks," *Security and Communication Networks*, vol. 8, no. 16, pp. 2850–2859, 2015.

[130] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A novel efficient maka protocol with desynchronization for anonymous roaming service in global mobility networks," *Journal of Network and Computer Applications*, vol. 107, pp. 83–92, 2018.

[131] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, N. Kumar, Y. Park, and S. Tanwar, "Design of an anonymity-preserving group formation based authentication protocol in global mobility networks," *IEEE Access*, vol. 6, pp. 20673–20693, 2018.

[132] F. Wu, X. Li, L. Xu, S. Kumari, and A. K. Sangaiah, "A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion," *Computers & Electrical Engineering*, vol. 68, pp. 107–118, 2018.

[133] R. Shashidhara, S. K. Nayak, A. K. Das, and Y. Park, "On the design of lightweight and secure mutual authentication system for global roaming in resource-limited mobility networks," *IEEE Access*, vol. 9, pp. 12879–12895, 2021.

[134] M. M. Sohail, M. Hassan, K. Mansoor, A. Ghani, and K. Jawad, "An improved authentication protocol for global mobility network (glomonet)," in *2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 401–406, IEEE, 2020.

[135] D. Kang, H. Lee, Y. Lee, and D. Won, "Lightweight user authentication scheme for roaming service in glomonet with privacy preserving," *Plos one*, vol. 16, no. 2, p. e0247441, 2021.

[136] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," *IEEE Communications Letters*, vol. 16, no. 8, pp. 1270–1273, 2012.

[137] D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authentication with conditional privacy for wireless networks," *IEEE Transactions on Computers*, vol. 62, no. 3, pp. 616–622, 2012.

[138] D. He, S. Zeadally, L. Wu, and H. Wang, "Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography," *Computer Networks*, vol. 128, pp. 154–163, 2017.

[139] Y. Park and H.-H. Park, "Analysis of error impact for batch handover authentication protocols in mobile wireless networks," *IEEE Access*, vol. 8, pp. 94112–94125, 2020.

[140] 3GPP tech. rep., TS 33.401 V15.3.0;Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 15), 2018.

[141] 3GPP tech. rep., TS 33.501 V15.4.0;5G; Security architecture and procedures for 5G System (Release 15), 2019.

[142] J. Munilla, M. Burmester, and R. Barco, "An enhanced symmetric-key based 5g-aka protocol," *Computer Networks*, vol. 198, p. 108373, 2021.

[143] M. Ouaissa and M. Ouaissa, "An improved privacy authentication protocol for 5g mobile networks," in *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*, pp. 136–143, IEEE, 2020.

[144] Y. Qiu, M. Ma, and X. Wang, "A proxy signature-based handover authentication scheme for lte wireless networks," *Journal of Network and Computer Applications*, vol. 83, pp. 63–71, 2017.

[145] R. Ma, J. Cao, D. Feng, H. Li, Y. Zhang, and X. Lv, "Ppsha: Privacy preserving secure handover authentication scheme for all application scenarios in lte-a networks," *Ad Hoc Networks*, vol. 87, pp. 49–60, 2019.

[146] S. Gupta, B. L. Parne, and N. S. Chaudhari, "Pseh: A provably secure and efficient handover aka protocol in lte/lte-a network," *Peer-to-Peer Networking and Applications*, vol. 12, no. 4, pp. 989–1011, 2019.

[147] J. Zhou, M. Ma, and S. Sun, "A hybrid authentication protocol for lte/lte-a network," *IEEE Access*, vol. 7, pp. 28319–28333, 2019.

[148] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang, "Sdn-based handover authentication scheme for mobile edge computing in cyber-physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8692–8701, 2019.

[149] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "Cppha: Capability-based privacy-protection handover authentication mechanism for sdn-based 5g hetnets," *IEEE transactions on dependable and secure computing*, vol. 18, no. 3, pp. 1182–1195, 2019.

[150] S. Gupta, B. L. Parne, N. S. Chaudhari, and S. Saxena, "Seai: Secrecy and efficiency aware inter-gnb handover authentication and key agreement protocol in 5g communication network," *Wireless Personal Communications*, vol. 122, no. 4, pp. 2925–2962, 2022.

[151] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5g hetnets," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 858–874, 2019.

[152] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[153] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting ibe technology for privacy in health care," in *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, pp. 432–437, IEEE, 2003.

[154] A. E. Eldewahi, T. M. Sharfi, A. A. Mansor, N. A. Mohamed, and S. M. Alwahbani, "Ssl/tls attacks: Analysis and evaluation," in *2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE)*, pp. 203–208, IEEE, 2015.

[155] P. Sirohi, A. Agarwal, and S. Tyagi, "A comprehensive study on security attacks on ssl/tls protocol," in *2016 2nd international conference on next generation computing technologies (NGCT)*, pp. 893–898, IEEE, 2016.

[156] I. ul Haq, J. Wang, Y. Zhu, and S. Maqbool, "A survey of authenticated key agreement protocols for multi-server architecture," *Journal of Information Security and Applications*, vol. 55, p. 102639, 2020.

[157] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Computers & Security*, vol. 88, p. 101619, 2020.

[158] A. Kumar and H. Om, "An improved and secure multiserver authentication scheme based on biometrics and smartcard," *Digital Communications and Networks*, vol. 4, no. 1, pp. 27–38, 2018.

[159] J. Wang, Y. Zhu, S. Maqbool, *et al.*, "An efficient hash-based authenticated key agreement scheme for multi-server architecture resilient to key compromise impersonation," *Digital Communications and Networks*, vol. 7, no. 1, pp. 140–150, 2021.

[160] S. Zhou, Q. Gan, and X. Wang, "Authentication scheme based on smart card in multi-server environment," *Wireless Networks*, vol. 26, no. 2, pp. 855–863, 2018.

[161] F. Wu, X. Li, L. Xu, A. K. Sangaiah, and J. J. Rodrigues, "Authentication protocol for distributed cloud computing: An explanation of the security situations for internet-of-things-enabled devices," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 38–44, 2018.

[162] L. D. Tsobdjou, S. Pierre, and A. Quintero, "A new mutual authentication and key agreement protocol for mobile client—server environment," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1275–1286, 2021.

[163] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol. 27, pp. 159–194, 2015.

[164] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[165] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[166] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[167] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, pp. 9–14, IEEE, 2007.

[168] Y. Ikezaki, Y. Nozaki, and M. Yoshikawa, "Deep learning attack for physical unclonable function," in *2016 IEEE 5th Global Conference on Consumer Electronics*, pp. 1–2, IEEE, 2016.

[169] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, "Cloning physically unclonable functions," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 1–6, IEEE, 2013.

[170] C. Steinfield, "The development of location based services in mobile commerce," in *E-life after the dot com bust*, pp. 177–197, Springer, 2004.

[171] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless network security*, pp. 103–135, Springer, 2007.

[172] "Span," *http://people.irisa.fr/Thomas.Genet/span/*.

[173] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International conference on computer aided verification*, pp. 281–285, Springer, 2005.

[174] T. Team *et al.*, "Avispa v1. 1 user manual," *Information society technologies programme (June 2006), http://people.irisa.fr/Thomas.Genet/Crypt/AVISPA_manual.pdf*, 2006.

[175] D. Von Oheimb, "The high-level protocol specification language hlpsl developed in the eu project avispa," in *Proceedings of APPSEM 2005 workshop*, pp. 1–17, APPSEM'05, Tallinn, Estonia, 2005.

[176] D. Basin, S. Mödersheim, and L. Vigano, "Ofmc: A symbolic model checker for security protocols," *International Journal of Information Security*, vol. 4, no. 3, pp. 181–208, 2005.

[177] M. Turuani, "The cl-atse protocol analyser," in *International conference on rewriting techniques and applications*, pp. 277–286, Springer, 2006.

[178] "Pycryptodome 3.16," *https://www.pycryptodome.org/en/latest/*.

[179] M. Adalier and A. Teknik, "Efficient and secure elliptic curve cryptography implementation of curve p-256," in *Workshop on elliptic curve cryptography standards*, vol. 66, pp. 2014–2017, 2015.

[180] H. Tsai and A. Harwood, "A scalable anonymous server overlay network," in *20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*, vol. 1, pp. 973–978, IEEE, 2006.

[181] J. A. Elices and F. Pérez-González, "Fingerprinting a flow of messages to an anonymous server," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 97–102, IEEE, 2012.

[182] B. Sterzbach, "Gps-based clock synchronization in a mobile, distributed real-time system," *Real-Time Systems*, vol. 12, no. 1, pp. 63–75, 1997.

[183] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 949–957, IEEE, 2010.

[184] H. W. Lim and G. Yang, "Authenticated key exchange protocols for parallel network file systems," *IEEE transactions on parallel and distributed systems*, vol. 27, no. 1, pp. 92–105, 2015.

[185] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 337–351, Springer, 2002.

[186] S. Chen, F. Qin, B. Hu, X. Li, and Z. Chen, "User-centric ultra-dense networks for 5g: Challenges, methodologies, and directions," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 78–85, 2016.

[187] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Future Generation Computer Systems*, vol. 62, pp. 190–195, 2016.

[188] R.-H. Liou, Y.-B. Lin, and S.-C. Tsai, "An investigation on lte mobility management," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 166–176, 2011.

[189] A. Ulvan, R. Bestak, and M. Ulvan, "The study of handover procedure in lte-based femtocell network," in *WMNC2010*, pp. 1–6, IEEE, 2010.

[190] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[191] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *2010 International Conference on Information Science and Applications*, pp. 1–6, IEEE, 2010.

[192] C.-Y. Chow and M. F. Mokbel, "Privacy in location-based services: a system architecture perspective," *Sigspatial Special*, vol. 1, no. 2, pp. 23–27, 2009.

[193] W. Z. Khan, M. Y. Aalsalem, M. N. B. M. Saad, and Y. Xiang, "Detection and mitigation of node replication attacks in wireless sensor networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 149023, 2013.

[194] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei, and M. Alazab, "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[195] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in wireless sensor network: A survey," in *2012 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–3, IEEE, 2012.

[196] "pypuf," *https://pypuf.readthedocs.io/en/latest/*.

[197] A. Tirumala, "Iperf: The tcp/udp bandwidth measurement tool," *http://dast. nlanr. net/Projects/Iperf/*, 1999.

[198] S. S. Kolahi, S. Narayan, D. D. Nguyen, and Y. Sunarto, "Performance monitoring of various network traffic generators," in *2011 UkSim 13th international conference on computer modelling and simulation*, pp. 501–506, IEEE, 2011.

[199] R. R. Fontes, S. Afzal, S. H. Brito, M. A. Santos, and C. E. Rothenberg, "Mininet-wifi: Emulating software-defined wireless networks," in *2015 11th International Conference on Network and Service Management (CNSM)*, pp. 384–389, IEEE, 2015.

*****