DAFTAR PUSTAKA

[1] S. Athmani, D. E. Boubiche, and A. Bilami, “Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs,” *2013 World Congr. Comput. Inf. Technol. WCCIT 2013*, pp. 0–4, 2013, doi: 10.1109/WCCIT.2013.6618693.

[2] R. Alattas, “Detecting black-hole attacks in WSNs using multiple base stations and check agents,” in *2016 Future Technologies Conference (FTC)*, 2016, no. December, pp. 1020–1024, doi: 10.1109/FTC.2016.7821728.

[3] S. Kumar and D. S. Sangwan, “A Survey of Black Hole Detection Techniques in WSNs,” *IJARCCE*, vol. 4, no. 5, pp. 557–562, May 2015, doi: 10.17148/IJARCCE.2015.45119.

[4] J. Sun and X. Zhang, “Study of ZigBee Wireless Mesh Networks,” in *2009 Ninth International Conference on Hybrid Intelligent Systems*, 2009, pp. 264–267, doi: 10.1109/HIS.2009.164.

[5] M. A. Siddiqi, A. A. Mugheri, and M. Khoso, “Analysis on Security Methods of Wireless Sensor Network,” vol. 2, no. 1, 2018, doi: 10.30537/sjcms.v2i1.69.

[6] F. Khan, “Secure communication and routing architecture in wireless sensor networks,” in *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, 2014, pp. 647–650, doi: 10.1109/GCCE.2014.7031298.

[7] Y. Hu, Y. Wu, and H. Wang, “Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN,” no. November, pp. 237–248, 2014.

[8] S. Vidhya and T. Sasilatha, “Performance analysis of black hole attack

detection scheme using MD5 algorithm in WSN," in *2014 International Conference on Smart Structures and Systems (ICSSS)*, 2014, pp. 51–54, doi: 10.1109/ICSSS.2014.7006194.

[9] A. Kaur, "Detection and isolation of black hole attack in wireless sensor network using hybrid techniques(Received packet and time delay)," *Proc. Int. Conf. Inven. Comput. Technol. ICICT 2016*, vol. 2, pp. 1–5, 2016, doi: 10.1109/INVENTIVE.2016.7824862.

[10] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 551–591, 2013, doi: 10.1109/SURV.2012.062612.00084.

[11] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2205–2224, 2019, doi: 10.1109/JIOT.2018.2883403.

[12] M. A. M. Vieira, C. N. Coelho, D. C. Da Silva, and J. M. Da Mata, "Survey on wireless sensor network devices," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, vol. 1, no. January, pp. 537–544, 2003, doi: 10.1109/ETFA.2003.1247753.

[13] J. Xu, W. Liu, F. Lang, Y. Zhang, and C. Wang, "Distance Measurement Model Based on RSSI in WSN," *Wirel. Sens. Netw.*, vol. 02, no. 08, pp. 606–611, 2010, doi: 10.4236/wsn.2010.28072.

[14] D. Sharma, S. Verma, and K. Sharma, "Network Topologies in Wireless Sensor Networks : A Review," *Int. J. Electron. Commun. Technol.*, vol. 4, pp. 93–97, 2013, doi: 2230-7109.

[15] A. Shrestha and L. Xing, "A performance comparison of different topologies for wireless sensor networks," *2007 IEEE Conf. Technol. Homel. Secur. Enhancing Crit. Infrastruct. Dependability*, pp. 280–285, 2007, doi: 10.1109/THS.2007.370059.

[16] R. W. Anwar *et al.*, “Security Issues and Attacks in Wireless Sensor Network,” vol. 30, no. 10, pp. 1224–1227, 2014, doi: 10.5829/idosi.wasj.2014.30.10.334.

[17] E. Sasikala and N. Rengarajan, “An Intelligent Technique to Detect Jamming Attack in Wireless Sensor Networks (WSNs),” *Int. J. Fuzzy Syst.*, vol. 17, no. 1, pp. 76–83, Mar. 2015, doi: 10.1007/s40815-015-0009-4.

[18] M. A. Jan, P. Nanda, X. He, and R. P. Liu, “A sybil attack detection scheme for a centralized clustering-based hierarchical network,” *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 318–325, 2015, doi: 10.1109/Trustcom.2015.390.

[19] S. Šafarić and K. Malarić, “ZigBee wireless standard,” *Proc. Elmar - Int. Symp. Electron. Mar.*, no. June, pp. 259–262, 2006, doi: 10.1109/ELMAR.2006.329562.

[20] M. Sveda and R. Trchalik, “ZigBee-to-Internet Interconnection Architectures,” *Second Int. Conf. Syst.*, no. ii, pp. 1–6, 2007.

[21] N. Baker, “ZigBee and Bluetooth strengths and weaknesses for industrial applications,” *IEE Comput. Control Eng.*, vol. 16, no. 2, pp. 20–25, 2005, doi: 10.1049/cce:20050204.

[22] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik, and A. ur Rehman, “Detection and prevention of Black Hole Attacks in IOT & WSN,” in *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, 2018, vol. 8, no. 7, pp. 217–226, doi: 10.1109/FMEC.2018.8364068.

[23] J. Schneider and R. Wattenhofer, “Trading bit, message, and time complexity of distributed algorithms,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6950 LNCS, pp. 51–65, 2011, doi: 10.1007/978-3-642-24100-0_4.

[24] R. K. Kodali and N. K. Aravapalli, “Multi-level LEACH protocol model using NS-3,” *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014*, pp.

375–380, 2014, doi: 10.1109/IAdCC.2014.6779352.

[25] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks,” *J. Sensors*, vol. 2016, 2016, doi: 10.1155/2016/4731953.

[26] T. Yue, C. Wang, and Z. X. Zhu, “Hybrid Encryption Algorithm Based on Wireless Sensor Networks,” *Proc. 2019 IEEE Int. Conf. Mechatronics Autom. ICMA 2019*, pp. 690–694, 2019, doi: 10.1109/ICMA.2019.8816451.

[27] V. R. H and R. Gunavathi, “Survey on Discovery Practices of Black Hole Attack in Wireless Sensor Networks,” *Int. J. Inf. Comput. Sci.*, vol. 6, no. 5, pp. 486–492, 2019.

[28] S. Wijetunge, “Performance Analysis of Ieee 802.15.4 Based Wireless Sensor Networks,” vol. 4, no. 4, pp. 1615–1621, 2013.