DAFTAR PUSTAKA

Tiphon, “Telecommunication and Internet Protocol Harmonization Over Network (TIPHON) General Aspect of Quality of Service (QoS),” DTR/TIPHON-05006 (cb0010cs.PDF),1999

Abazari, F., Esposito, F., Takabi, H., Hosseinvand, H., & Pecorella, T. (2019). Teaching software-defined network security through malicious tenant detection. In *Internet Technology Letters* (Vol. 2, Issue 6). John Wiley and Sons Inc. https://doi.org/10.1002/itl2.131

Al-Duwairi, B., Al-Quraan, E., & AbdelQader, Y. (2020). ISDSDN: Mitigating SYN *Flood Attack*s in Software Defined Networks. *Journal of Network and Systems Management*, *28*(4), 1366–1390. https://doi.org/10.1007/s10922-020-09540-1

Alsmadi, I. M., Alazzam, I., & Akour, M. (2017). A systematic literature review on software-defined networking. In *Studies in Computational Intelligence* (Vol. 691, pp. 333–369). Springer Verlag. https://doi.org/10.1007/978-3-319-44257-0_14

Gao, Y., & Xu, M. (2023). *Defense Against Software-Defined Network Topology Poisoning Attacks* (Vol. 28, Issue 1).

Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and OpenFlow: From concept to *implement*ation. In *IEEE Communications Surveys and Tutorials* (Vol. 16, Issue 4, pp. 2181–2206). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2014.2326417

Jāmiʿat Qaṭar, Institute of Electrical and Electronics Engineers. Qatar Section., & Institute of Electrical and Electronics Engineers. (n.d.). *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) : February 2-5, Doha, Qatar*.

Joglekar, C. A. (2017). *Route Manipulation using SDN and Quagga*.

Lin, B., Zhu, X., & Ding, Z. (2017). *Research on the Vulnerability of Software Defined Network*.

Pickett, G., & Com, G. P. (n.d.). *Abusing Software Defined Networks*.

Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. (2018). *Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions*. http://arxiv.org/abs/1804.00262

Sherwood, R., Foster, N., Association for Computing Machinery. Special Interest Group on Data Communications, Association for Computing Machinery, ACM Digital Library., & ACM SIGCOMM Conference (2013 : Hong Kong, C. (n.d.). *HotSDN'13 : proceedings of the 2013 ACM SIGCOMM Workshop on Hot topics in Software Defined Networking : August 16, 2013, Hong Kong, China*.

Shrivastava, P., Agarwal, A., & Kataoka, K. (2018). Poster: Detection of *topology poisoning* by silent *Relay Attacker* in SDN. *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, 792–794. https://doi.org/10.1145/3241539.3267763

Sistem, J., & Fakultas, K. (n.d.). *Ahmad Heryanto, Afrilia*.

Wang, J., Tan, Y., & Liu, J. (2020). *Topology poisoning attack*s and countermeasures in SDN-enabled vehicular networks. *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, *2020-January*. https://doi.org/10.1109/GLOBECOM42002.2020.9348183

Wang, J., Wen, R., Li, J., Yan, F., Zhao, B., & Yu, F. (2019). Detecting and Mitigating Target *Link-Flood*ing *Attack*s Using SDN. *IEEE Translation on Dependable and Secure Computing*, *16*(6), 944–956. https://doi.org/10.1109/TDSC.2018.2822275

Zhang, C., Hu, G., Chen, G., Sangaiah, A. K., Zhang, P., Yan, X., & Jiang, W. (2017). Towards a SDN-Based Integrated Architecture for Mitigating *IP Spoofing Attack*. *IEEE Access*, *6*, 22764–22777. https://doi.org/10.1109/ACCESS.2017.2785236