REFERENCES

Ahmed, M. E., & Kim, H (2016). DDoS Attack Mitigation in Internet of Things Using Software Defined Networking.

Alaidaros, H., Mahmuddin, M., & Al-Mazari, A. (2011). An overview of flow-based and packet-based intrusion detection performance in high speed networks.

Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2015). A survey of securing networks using software defined networking. IEEE transactions on reliability, 64(3), 1086-1097.

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: Methods, practices, and solutions. Arabian Journal for Science and Engineering, 42(2), 425-441.

Behal, S., & Kumar, K. (2016). Trends in validation of ddos research. Procedia Computer Science, 85, 7-15.

Bhattacharyya, D. K., & Kalita, J. K. (2016). DDoS attacks: evolution, detection, prevention, reaction, and tolerance. Chapman and Hall/CRC.

Bhushan, K., & Gupta, B. B. (2018, February). Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing Environment. In 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 872-877). IEEE.

Braga, R., Mota, E., & Passito, A. (2010, October). Lightweight DDoS flooding attack detection using NOX/OpenFlow. In Local Computer Networks (LCN), 2010 IEEE 35th Conference on (pp. 408-415). IEEE.

Brian, L. MiniEdit. (Online posting). <http://www.brianlinkletter.com/how-to-use-miniedit-mininets-graphical-user interface/>. Accessed: 27 April 2016.

Cvitić, I., Peraković, D., Periša, M., & Musa, M. (2017, November). Network parameters applicable in detection of infrastructure level DDoS attacks. In 2017 25th Telecommunication Forum (TELFOR) (pp. 1-4). IEEE.

Chin, T., Mountrouidou, X., Li, X., & Xiong, K. (2015, June). Selective packet inspection to detect DoS flooding using software defined networking (SDN).

In Distributed Computing Systems Workshops (ICDCSW), 2015 IEEE 35th International Conference on (pp. 95-99). IEEE.

Chung, C. J., Khatkar, P., Xing, T., Lee, J., & Huang, D. (2013). NICE: Network intrusion detection and countermeasure selection in virtual network systems. IEEE transactions on dependable and secure computing, 10(4), 198-211.

Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., & Zheng, X. (2016). SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications, 68, 65-79.

Davis, J. P., Eisenhardt, K. M., & Bingham, C. B. (2007). Developing theory through simulation methods. Academy of Management Review, 32(2), 480-499.

Dharma, N. G., Muthohar, M. F., Prayuda, J. A., Priagung, K., & Choi, D. (2015, August). Time-based DDoS detection and mitigation for SDN controller. In 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 550-553). IEEE.

Dillon, C., & Berkelaar, M. (2014). OpenFlow (D) DoS Mitigation. Technical report (February 2014), http://www. delaat. net/rp/2013-2014/p42/report. pdf.

Dong, P., Du, X., Zhang, H., & Xu, T. (2016, May). A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows. In 2016 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

Doria, A., Salim, J. H., Haas, R., Khosravi, H., Wang, W., Dong, L., & Halpern, J. (2010). Forwarding and control element separation (ForCES) protocol specification (No. RFC 5810).

Dotcenko, S., Vladyko, A., & Letenko, I. (2014, February). A fuzzy logic-based information security management for software-defined networks. In Advanced Communication Technology (ICACT), 2014 16th International Conference on (pp. 167-171). IEEE.

Feng, Y., Guo, R., Wang, D., & Zhang, B. (2009, August). Research on the active DDoS filtering algorithm based on IP flow. In Natural Computation, 2009. ICNC'09. Fifth International Conference on (Vol. 4, pp. 628-632). IEEE.

Fernandez, M. (2013, January). Evaluating OpenFlow controller paradigms. In ICN 2013, The Twelfth International Conference on Networks (pp. 151-157).

Fundation, O. N. (2012). Software-defined networking: The new norm for networks. ONF White Paper Available at: https://www.opennetworking.org/images/stories/downloads/sdnresources/white-papers/wp-sdn-newnorm.pdf. Accessed: 22/11/2015.

Fu, M. C., Glover, F. W., & April, J. (2005, December). Simulation optimization: a review, new developments, and applications. In Proceedings of the Winter Simulation Conference, 2005. (pp. 13-pp). IEEE.

Gao, M., Zhang, K., & Lu, J. (2006, April). Efficient packet matching for gigabit network intrusion detection using TCAMs. In Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on (Vol. 1, pp. 6-pp). IEEE.

Gao, S., & Chen, W. (2016). A partition-based random search for stochastic constrained optimization via simulation. IEEE Transactions on Automatic Control, 62(2), 740-752.

Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., & Maglaris, V. (2014). Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Computer Networks, 62, 122-136.

Gu, Y., McCallum, A., & Towsley, D. (2005, October). Detecting anomalies in network traffic using maximum entropy estimation. In Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement (pp. 32-32). USENIX Association.

Guha, A., Reitblatt, M., & Foster, N. (2013, June). Machine-verified network controllers. In ACM SIGPLAN Notices (Vol. 48, No. 6, pp. 483-494). ACM.

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2242-2270.

Hu, F. (2014). Network Innovation through OpenFlow and SDN: Principles and Design. CRC Press.

Ince, N., & Bragg, A. (Eds.). (2007). Recent advances in modeling and simulation tools for communication networks and services. Springer Science & Business Media.

Ivanov, D. (2017). Simulation-based ripple effect modelling in the supply chain. International Journal of Production Research, 55(7), 2083-2101.

Jain, R. (2015). Art of Computer Systems Performance Analysis: Techniques for Experimental Design Measurements Simulation and Modeling (2nd ed.). NewYork: Wiley.

Jain, S., Kumar, A., Mandal, S., Ong, J., Poutievski, L., Singh, A., & Zolla, J. (2013, August). B4: Experience with a globally-deployed software defined WAN. In ACM SIGCOMM Computer Communication Review (Vol. 43, No. 4, pp. 3-14). ACM.

Javed, M., Ashfaq, A. B., Shafiq, M. Z., & Khayam, S. A. (2009, September). On the Inefficient Use of Entropy for Anomaly Detection. In RAID (pp. 369-370).

Katta, N., Alipourfard, O., Rexford, J., & Walker, D. (2016, March). Cacheflow: Dependency-aware rule-caching for software-defined networks. In Proceedings of the Symposium on SDN Research(p. 6). ACM.

Keshav, S. (1991). Congestion Control in Computer Networks PhD Thesis. UC Berkeley TR-654.

Kia, M. (2015). Early Detection and Mitigation of DDoS Attacks In Software Defined Networks(Doctoral dissertation, Ryerson University).

Kim, J., Firoozjaei, M. D., Jeong, J. P., Kim, H., & Park, J. S. (2015, October). SDN-based security services using interface to network security functions. In Information and Communication Technology Convergence (ICTC), 2015 International Conference on (pp. 526-529). IEEE.

Kim, M. S., Kong, H. J., Hong, S. C., Chung, S. H., & Hong, J. W. (2004, April). A flow-based method for abnormal network traffic detection. In Network operations and management symposium, 2004. NOMS 2004. IEEE/IFIP (Vol. 1, pp. 599-612). IEEE.

Lai, H., Cai, S., Huang, H., Xie, J., & Li, H. (2004, June). A parallel intrusion detection system for high-speed networks. In International Conference on Applied Cryptography and Network Security(pp. 439-451). Springer, Berlin, Heidelberg.

Lakhina, A., Crovella, M., & Diot, C. (2005, August). Mining using traffic feature distributions. In ACM SIGCOMM Computer Communication Review (Vol. 35, No. 4, pp. 217-228). ACM.

Law, A. & Kelton, W. (1991). *Simulation modeling and analysis* (2nd ed.). McGraw-Hill.

Law, A. (2007). McGraw-Hill series in industrial engineering and management science. Simulation modeling and analysis, 19, 768-768.
Lee, D. (2015). Improving detection capability of flow-based IDS in SDN.

Lim, S., Ha, J., Kim, H., Kim, Y., & Yang, S. (2014, July). A SDN-oriented DDoS blocking scheme for botnet-based attacks. In Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on (pp. 63-68). IEEE.

Mahoney, M. V. (2003, March). Network traffic anomaly detection based on packet bytes. In Proceedings of the 2003 ACM symposium on Applied computing (pp. 346-350). ACM.

Malik, M. S., Montanari, M., Huh, J. H., Bobba, R. B., & Campbell, R. H. (2013, June). Towards SDN enabled network control delegation in clouds. In Dependable Systems and Networks (DSN), 2013 43rd Annual IEEE/IFIP International Conference on (pp. 1-6). IEEE.L.

McCauley, M. (2014). NOXRepo. Online: http://www. noxrepo. org.

Meena, D. L., & Jadon, R. S. (2014). Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches. *International Journal*, *2*(4).

Mehdi, S. A., Khalid, J., & Khayam, S. A. (2011, September). Revisiting traffic anomaly detection using software defined networking. In International workshop on recent advances in intrusion detection (pp. 161-180). Springer, Berlin, Heidelberg.

Mininet. Vers. 2.2.1. <http://mininet.org/download/> Accessed: 25 February 2016.

Mousavi, S. M. (2014). Early detection of DDoS attacks in software defined networks controller(Doctoral dissertation, Carleton University).

Mukherjee, S. (2014). Analytical modeling of heterogeneous cellular networks. Cambridge University Press.

Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T., & Vasupongayya, S. (2019). Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN). Journal of Computer Networks and Communications, 2019.

Nishtha & M. Sood, "Software defined network - architectures," PDGC- 2014, 2014.

Niyaz, Q., Sun, W., & Javaid, A. Y. (2017). A deep learning based DDoS detection system in software-defined networking (SDN). arXiv preprint arXiv:1611.07400.

Noble, G., & Sujitha, M. (2015). Flow Based Solutions for DoS and DDoS Attack Detection. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 3, March 2015.

Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634.

Paroutis, S., Bennett, M., & Heracleous, L. (2014). A strategic view on smart city technology: The case of IBM Smarter Cities during a recession. Technological Forecasting and Social Change, 89, 262-272.

McCauley, M. POX Controller (Online posting). <https://openflow.stanford.edu/display/ONL/POX+Wiki> Accessed: 13 March 2016.

Prete, L. R., Schweitzer, C. M., Shinoda, A. A., & de Oliveira, R. L. S. (2014, June). Simulation in an SDN network scenario using the POX Controller. In Communications and Computing (COLCOM), 2014 IEEE Colombian Conference on (pp. 1-6). IEEE.

Saboor, A., & Aslam, B. (2015, January). Analyses of flow based techniques to detect distributed denial of service attacks. In Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on (pp. 354-362). IEEE.

Sahoo, K. S., Puthal, D., Tiwary, M., Rodrigues, J. J., Sahoo, B., & Dash, R. (2018). An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics, Future Generation Computer Systems, https://doi.org/10.1016/j.

Schmidt, D., Suriadi, S., Tickle, A., Clark, A., Mohay, G., Ahmed, E., & Mackie, J. (2010). A distributed denial of service testbed. In What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience (pp. 338-349). Springer, Berlin, Heidelberg.

Schechter, S. E., Jung, J., & Berger, A. W. (2004, September). Fast detection of scanning worm infections. In International Workshop on Recent Advances in Intrusion Detection (pp. 59-81). Springer, Berlin, Heidelberg.

Securelist. 2019. "DDOS attacks in Q1 2019". (Online posting). < https://securelist.com/ddos-report-q1-2019/90792/>. Accessed: 25 May 2019.

Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013, November). SDN security: A survey. In Future Networks and Services (SDN4FNS), 2013 IEEE SDN For (pp. 1-7). IEEE.

Shin, S., & Gu, G. (2013, August). Attacking software-defined networks: A first feasibility study. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 165-166). ACM.

Specification, O. S. (2009). Version 1.0. 0 (Wire Protocol 0x01). Open Networking Foundation.

Sperotto, A., Schaffrath, G., Sadre, R., Morariu, C., Pras, A., & Stiller, B. (2010). An overview of ip flow-based intrusion detection. IEEE Communications Surveys and Tutorials, 12(3), 343-356.

Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016, October).
Deep learning approach for network intrusion detection in software defined networking. In Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on (pp. 258-263). IEEE.

Version, O. S. S. 1.5. 1 (Protocol version 0x06), December, 2014.

Vykopal, J. (2013). Flow-based brute-force attack detection in large and high-speed networks (Doctoral dissertation, Masarykova univerzita, Fakulta informatiky).

Oracle Corporation. *VirtualBox.* Vers. 5.2. https://www.virtualbox.org/wiki/Downloads>. Accessed: 3 February 2016.

Wang, A., Guo, Y., Hao, F., Lakshman, T. V., & Chen, S. (2014, December). Scotch: Elastically scaling up sdn control-plane using vswitch based overlay.

In Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies (pp. 403-414). ACM.

Wang, R., Jia, Z., & Ju, L. (2015, August). An entropy-based distributed DDoS detection mechanism in software-defined networking. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 310-317). IEEE.

Williamson, M. M. (2002). Throttling viruses: Restricting propagation to defeat malicious mobile code. In Computer Security Applications Conference, 2002. Proceedings. 18th Annual (pp. 61-68). IEEE.

Xiang, Y., Li, K., & Zhou, W. (2011). Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE transactions on information forensics and security, 6(2), 426-437.

Xing, T., Huang, D., Xu, L., Chung, C. J., & Khatkar, P. (2013, March). Snortflow: A openflow-based intrusion prevention system in cloud environment. In Research and Educational Experiment Workshop (GREE), 2013 Second GENI (pp. 89-92). IEEE.

XU, X., YU, H., & YANG, K. (2017). DDoS Attack in Software Defined Networks: A Survey. ZTE COMMUNICATIONS, 15(3).

Yadav, V. K., Trivedi, M. C., & Mehtre, B. M. (2016). DDA: an approach to handle DDoS (Ping flood) attack. In Proceedings of International Conference on ICT for Sustainable Development(pp. 11-23). Springer, Singapore.

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials, 18(1), 602-622.

Yavanoglu, O., & Aydos, M. (2017, December). A review on cyber security datasets for machine learning algorithms. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 2186-2193). IEEE.

YuHunag, C., MinChi, T., YaoTing, C., YuChieh, C., & YanRen, C. (2010, November). A novel design for future on-demand service and security. In Communication Technology (ICCT), 2010 12th IEEE International Conference on (pp. 385-388). IEEE.

Yu, S., Zhou, W., Doss, R., & Jia, W. (2012). Traceback of DDoS attacks using entropy variations. IEEE transactions on parallel and distributed systems , vol. 23, no. 3, pp. 412–425, 2012.

Zhou, L., Liao, M., Yuan, C., & Zhang, H. (2017). Low-rate DDoS attack detection using expectation of packet size. Security and Communication Networks, 2017.