Bibliography

[1] Kang, M.S., Lee, S.B. and Gligor, V.D. The crossfire attack. In *Security and Privacy (SP)*, pages 127-141, IEEE Symposium, 2013. IEEE..

[2] Mirkovic, J. and Reiher, P., A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39-53, 2004.

[3] Hoque, N., Bhuyan, M.H., Baishya, R.C., Bhattacharyya, D.K. and Kalita, J.K., Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40(2):307-324, 2014.

[4] CNN. Xie, Y., and Yu, S. Z. Monitoring the application-layer DDoS attacks for popular websites. *IEEE/ACM Transactions on Networking*, 17(1):15-25, 2009.

[5] H., Zhang, D., and Shin, K. G. Detecting SYN flooding attacks. In *INFOCOM 2002, Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies,*pages 1530-1539, Proceedings, 2002. IEEE.

[6] Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., and Gritzalis, S. DNS amplification attack revisited. *Computers and Security*, 39(2):475-485, 2013.

[7] Rossow, C. Amplification hell: Revisiting network protocols for DDoS abuse, In *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[8] Kuzmanovic, A., and Knightly, E. W. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 75-86, 2003. ACM.

[9] Studer, A., and Perrig, A. The coremelt attack. In *Computer SecurityE-SORICS*, pages 37-52, 2009. Springer Berlin Heidelberg.

[10] Yatagai, T., Isohara, T., and Sasase, I. Detection of HTTP-GET flood attack based on analysis of page access behavior. In *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pages 232-235, 2007. IEEE.

[11] Loek Essers,IDG News Service, *DDoS attack takes Dutch government sites offline for 10 hours*, Retrieved on 10 Dec. 2017 from `http://www.pcworld.com/article/2883092/ddosattack-takes-dutch-government-sites-offline-for-10-hours.html,20June,2015.`

[12] Connor Adams Sheets, *NSA Website Down Following Apparent DDoS Attack Possibly By Anonymous Or A Foreign Government.* Retrieved on 10 Dec. 2017 from **http://www.ibtimes.com/nsa-website-down-following-apparent-ddos-attack-possibly-anonymous-or-foreign-government-1442452, 20 June,2015.**

[13] Wikipedia. *Anonymous (group).* Retrieved on 10 Dec. 2017 from **https://en.wikipedia.org/wiki/Anonymous_(group)**

[14] Dan Goodin. *Massive denial-of-service attack on GitHub tied to Chinese government.* Retrieved on 10 Dec. 2017 from **http://arstechnica.com/security/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government**

[15] Yu, S., and Zhou, W. Entropy-based collaborative detection of DDOS attacks on community networks. In *Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 566-571, 2008. IEEE.

[16] Zargar, S. T., Joshi, J., and Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *Communications Surveys and Tutorials, IEEE*, 15(4):2046-2069, 2013.

[17] Sam Thielman and Chris Johnston. *Major cyber attack disrupts internet service across Europe and US.* Retrieved on 10 Dec. 2017 from **https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service**

[18] B. E. Brodsky and B. S. Darkhovsky. *Nonparametric Methods in Change-point Problems.* Kluwer Academic Publishers, 1993.

[19] Yau, D. K., Lui, J., Liang, F., and Yam, Y. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. *IEEE/ACM Transactions on Networking (TON),* 13(1):29-42, 2005.

[20] Chou, J. C. Y., Lin, B., Sen, S., and Spatscheck, O. Proactive surge protection: a defense mechanism for bandwidth-based attacks. *IEEE/ACM Transactions on Networking (TON)*,17(6): 1711-1723, 2009.

[21] Xu, J., and Lee, W. Sustaining availability of web services under distributed denial of service attacks. *IEEE Transactions on Computers,*52(2):195-208, 2003.

[22] Packet Storm, *DDoS Attack Tools, 2015.* Retrieved on 10 Dec. 2017 from `http://packetstormsecurity.org`.

[23] Lee, W., and Xiang, D. Information-theoretic measures for anomaly detection. In *Proceedings of 2001 IEEE Symposium on Security and Privacy*, pages 130-143, 2001. IEEE.

[24] Lu, K., Wu, D., Fan, J., Todorovic, S., and Nucci, A. Robust and efficient detection of DDoS attacks for large-scale Internet. *Computer Networks*, 51(18):5036-5056, 2007.

[25] Jin, S., and Yeung, D. S. A covariance analysis model for DDoS attack detection, In *International Conference on Communications*, pages 1882-1886, 2004. IEEE.

[26] Yaar, A., Perrig, A., and Song, D. Pi: A path identification mechanism to defend against DDoS attacks. In *Proceedings 2003 Symposium on Security and Privacy*, pages 93-107, 2003. IEEE.

[27] Yaar, A., Perrig, A., and Song, D. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. *IEEE Journal on Selected Areas in Communications,*24(10):1853-1863, 2006.

[28] Goodrich, M. T. Probabilistic packet marking for large-scale IP traceback. *IEEE/ACM Transactions on Networking,*16(1):15-24, 2008.

[29] Belenky, A., and Ansari, N. IP traceback with deterministic packet marking. *IEEE communications letters,*7(4):162-164, 2003.

[30] Peng, T., Leckie, C., and Ramamohanarao, K. Protection from distributed denial of service attacks using history-based IP filtering. In *IEEE International Conference on Communications ICC'03*, pages 482-486, 2003. IEEE.

[31] Feinstein, L., Schnackenberg, D., Balupari, R., and Kindred, D. Statistical approaches to DDoS attack detection and response. In *DARPA Information Survivability Conference and Exposition*, pages 303-314, 2003. IEEE.

[32] Sourceforge. *DDoS Attack Tools,2012.* Retrieved on 10 Dec. 2017 from `http://sourceforge.net/projects`.

[33] Xiang, Y., Li, K., and Zhou, W. Low-rate DDoS attacks detection and traceback by using new information metrics. *IEEE Transactions on Information Forensics and Security,*6(2):426-437, 2011.

[34] Chen, Y., Hwang, K., and Ku, W. S. Collaborative detection of DDoS attacks over multiple network domains. *IEEE Transactions on Parallel and Distributed Systems*, 18(12):1649-1662, 2007.

[35] Xiang, Y., and Zhou, W. Mark-aided distributed filtering by using neural network for ddos defense. In *GLOBECOM'05: IEEE Global Telecommunications Conference*, St. Louis, Missouri, USA, discovery past and future, pages 1701-1705, 2005. IEEE Globecom.

[36] Bertino, E. and Islam, N. Botnets and internet of things security. *Computer*, 50(2):76-79, 2017.

[37] Yu, J., Li, Z., Chen, H., and Chen, X. A detection and offense mechanism to defend against application layer DDoS attacks. In *Third International Conference on Networking and Services*, pages 54-54, 2007. IEEE.

[38] Xie, Y., and Yu, S. Z. A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors. *IEEE/ACM Transactions on Networking*, 17(1):54-65, 2009.

[39] Bhuyan, M. H., Bhattacharyya, D. K., and Kalita, J. K. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters*, 51(2):1-7, 2015.

[40] Ain, A., Bhuyan, M.H., Bhattacharyya, D.K. and Kalita, J.K., Rank Correlation for Low-Rate DDoS Attack Detection: An Empirical Evaluation. *IJ Network Security*, 18(3):474–480, 2016.

[41] Mahoney, M. V., and Chan, P. K. Learning nonstationary models of normal network traffic for detecting novel attacks. In *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 376-385, 2002. ACM.

[42] Vijayasarathy, R., Raghavan, S. V., Ravindran, B. A system approach to network modeling for DDoS detection using a Naive Bayesian classifier. In *Third International Conference on In Communication Systems and Networks (COMSNETS)*, pages 1-10, 2011. IEEE.

[43] Kumar, P. A. R., and Selvakumar, S. Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications* , 34(11):1328-1341, 2011.

[44] Sheikhan, M., and Jadidi, Z. Flow-based anomaly detection in high-speed links using modified GSA-optimized neural network. *Neural Computing and Applications*, 24(3-4):599–611, 2014.

[45] Lee, K., Kim, J., Kwon, K. H., Han, Y., and Kim, S. DDoS attack detection method using cluster analysis. *Expert Systems with Applications*, 34(3):1659-1665, 2008.

[46] Wang, H., Jin, C., and Shin, K. G. Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM Transactions on Networking (ToN)*, 15(1):40-53, 2007.

[47] Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., Service resizing for quick DDoS mitigation in cloud computing environment. *Annals of Telecommunications*, 72(6):237-252, 2017.

[48] Spognardi, A., De Donno, M., Dragoni, N. and Giaretta, A. Analysis of DDoS-Capable IoT Malwares. *Annals of Computer Science and Information Systems*, 11(2):807-816, 2017.

[49] Osanaiye, O., Choo, K.K.R. and Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67(2):147-165, 2016.

[50] Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7):80-84, 2017.

[51] Ioannidis, J. and Bellovin, S.M., Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *NDSS*, 2002.

[52] Yu, S., Zhou, W., Doss, R. and Jia, W. Traceback of DDoS attacks using entropy variations. *IEEE Transactions on Parallel and Distributed Systems*, 22(3):412-425, 2011.

[53] Gulisano, V., Callau-Zori, M., Fu, Z., Jimnez-Peris, R., Papatriantafilou, M. and Patio-Martnez, M. STONE: A streaming DDoS defense framework. *Expert Systems with Applications*, 42(24):9620-9633, 2015.

[54] Hoque, N., Bhattacharyya, D.K. and Kalita, J.K. FFSc: a novel measure for lowrate and highrate DDoS attack detection using multivariate data analysis. *Security and Communication Networks*, 9(13):2032-2041, 2016.

[55] Saied, A., Overill, R.E. and Radzik, T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*, 172(2):385-393, 2016.

[56] Rogaway, P. and Shrimpton, T. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption*, pages 371-388, Springer, Berlin, Heidelberg, 2004.

[57] Maurer, W.D. and Lewis, T.G. Hash table methods. *ACM Computing Surveys (CSUR)*, 7(1):5-19, 1975.

[58] Broder, A. and Mitzenmacher, M. Network applications of bloom filters: A survey. *Internet mathematics*, 1(4):485-509, 2004.

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

[60] Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S. and Stiller, B. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*, pages 16-29, Springer, Cham, 2017 .

[61] *Waikato Applied Network Dynamic Research Group*. Retrieved on 10 Dec. 2017 from (`http://wand.net.nz/wits/auck/8/`)

[62] *Waikato Applied Network Dynamic Research Group.* Retrieved on 10 Dec. 2017 from (`http://wand.net.nz/wits/waikato/8/`)

[63] *Waikato Applied Network Dynamic Research Group.* Retrieved on 10 Dec. 2017 from (`http://research.wand.net.nz/software/libtrace.php`)

[64] *CAIDA Macroscopie Internet Topology Data Kit (ITDK) #0304* . Retrieved on 10 Dec. 2017 from (`www.caida.org/datasets/topology/skitter/itdk/ITDK0304/LNK0304`)

[65] *The CAIDA UCSD "DDoS Attack 2007" Dataset.* Retrieved on 10 Dec. 2017 from (`www.caida.org/data/passive/ddos-20070804_dataset.xml`)

[66] *DARPA Intrusion Detection Data Sets.* Retrieved on 10 Dec. 2017 from (`www.ll.mit.edu/ideval/data/`)

[67] Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., DDoS attacks in cloud computing: issues, taxonomy, and future directions. *Computer Communications*, 2017.

[68] Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J. and Zheng, X., SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. *Journal of Network and Computer Applications*, 68(14):65-79, 2016.

[69] Mahajan, R., Bellovin, S.M., Floyd, S., Ioannidis, J., Paxson, V. and Shenker, S. Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review*, 32(3):62-73, 2002.

[70] Gupta, B.B. and Badve, O.P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. *Neural Computing and Applications*, 28(12):3655-3682, 2017.

[71] Blazek, R.B., Kim, H., Rozovskii, B. and Tartakovsky, A. A novel approach to detection of denialofservice attacks via adaptive sequential and batchsequential changepoint detection methods. In *Workshop on Information Assurance and Security*, pages 922-930, 2002.

[72] Peng, T., Leckie, C. and Ramamohanarao, K. Proactively detecting distributed denial of service attacks using source IP address monitoring. In *International Conference on Research in Networking*, pages 771-782, Springer, Berlin, Heidelberg, 2004.

[73] Wong, F. and Tan, C.X. A survey of trends in massive DDoS attacks and cloud-based mitigations. *International Journal of Network Security and Its Applications*, 6(3):57-57, 2014.

[74] Savage, S., Wetherall, D., Karlin, A. and Anderson, T. Practical network support for IP traceback. In *ACM SIGCOMM Computer Communication Review*, 30(4):295-306, 2000.

[75] Song, D.X. and Perrig, A. Advanced and authenticated marking schemes for IP traceback. In *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*. Proceedings. IEEE, pages 878-886. IEEE.

[76] Dean, D., Franklin, M. and Stubblefield, A. An algebraic approach to IP traceback. *ACM Transactions on Information and System Security (TISSEC)*, 5(2):119-137, 2002.

[77] Scott-Hayward, S., O'Callaghan, G. and Sezer, S. SDN security: A survey. In *Future Networks and Services (SDN4FNS)*, pages 1-7, 2013. IEEE.

[78] Negi, P., Mishra, A., and Gupta, B. B. Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment. *arXiv preprint arXiv*, 1304.7073.

[79] Jeyanthi, N., and Iyengar, N. C. S. N. An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks. *IJ Network Security*, 14(5):257-269, 2012.

[80] Chen, Y., Das, S., Dhar, P., El-Saddik, A., and Nayak, A. Detecting and Preventing IP-spoofed Distributed DoS Attacks. *IJ Network Security*, 7(1):69-80, 2008.

[81] Chen, Yu, Kai Hwang, and Wei-Shinn Ku. Collaborative detection of DDoS attacks over multiple network domains. *Parallel and Distributed Systems, IEEE Transactions on*, 18(12):1649-1662, 2007.

[82] Yan, Q., Yu, F.R., Gong, Q. and Li, J. 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 and Tutorials*, 18(1):602-622, 2016.

[83] Elejla, O.E., Anbar, M. and Belaton, B. ICMPv6-based DoS and DDoS attacks and defense mechanisms.]itIETE Technical Review, 34(4):390-407, 2017.

[84] *The CAIDA Anonymized Internet Traces 2014 Dataset*, Retrieved on 10 Dec. 2017 from `http://www.caida.org/data/passive/passive_2014_dataset.xml`

[85] Wang, B., Zheng, Y., Lou, W. and Hou, Y.T. DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks*, 81(2):308-319, 2015.

[86] Peng, T., Leckie, C. and Ramamohanarao, K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1):3, 2007.

[87] Bhavani, Y., Janaki, V. and Sridevi, R. IP traceback through modified probabilistic packet marking algorithm using Chinese remainder theorem. *Ain Shams Engineering Journal*, 6(2):715-722, 2015.

[88] Jin, C., Wang, H. and Shin, K.G. Hop-count filtering: an effective defense against spoofed DDoS traffic. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 30-41, 2003. ACM.

[89] Behal, S. and Kumar, K. Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review. *International Journal of Network Security*, 19(3):383-393, 2017.

[90] *Wireshark Users Guide*. Retrieved on 10 Dec. 2017 from `https://www.wireshark.org/docs/wsug_html_chunked/`.

[91] Belenky, A. and Ansari, N. On deterministic packet marking. *Computer Networks*, 51(10):2677-2700, 2007.

[92] Gong, C., Le, T., Korkmaz, T. and Sarac, K. Single packet IP traceback in AS-level partial deployment scenario. In *in Proc. of IEEE GLOBECOM*, 2005.

[93] Gong, C. and Sarac, K. IP traceback based on packet marking and logging. In *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, pages 1043-1047, 2005. IEEE.

[94] Li, J., Sung, M., Xu, J. and Li, L. Large-scale IP traceback in high-speed Internet: Practical techniques and theoretical foundation. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 115-129, 2004. IEEE.

[95] KrishnaKumar, B., Kumar, P.K. and Sukanesh, R. Hop count based packet processing approach to counter DDoS attacks. In *Recent Trends in Information, Telecommunication and Computing (ITC), 2010 International Conference on*, pages 271-273, 2010. IEEE.

[96] Rivest, R. The MD5 message-digest algorithm. 1992.

[97] Sattari, P., Gjoka, M. and Markopoulou, A. A network coding approach to IP traceback. In *Network Coding (NetCod), 2010 IEEE International Symposium on*pages 1-6, 2010. IEEE.

[98] Carl, G., Kesidis, G., Brooks, R.R. and Rai, S. Denial-of-service attack-detection techniques. *IEEE Internet computing*, 10(1):82-89, 2006.

[99] Shevtekar, A., Anantharam, K. and Ansari, N., Low rate TCP denial-of-service attack detection at edge routers. *IEEE Communications Letters*, 9(4):363-365, 2005.

[100] Yan, D., Wang, Y., Su, S., and Yang, F. A precise and practical IP traceback technique based on packet marking and logging. *Journal of Information Science and Engineering*, 28(3):453-470, 2012.

[101] Belenky, A. and Ansari, N. Tracing multiple attackers with deterministic packet marking (DPM). In *Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on*1:49-52, 2003.

[102] Burch, H., and Cheswick, B. Tracing Anonymous Packets to Their Approximate Source. In *LISA*, pages 319-327, 2000.

[103] Bellovin, S. M., Leech, M., and Taylor, T. ICMP traceback messages, 2003.

[104] Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A. and Powell, W. Catch me if you can: A cloud-enabled ddos defense. In *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*, pages 264-275, 2014. IEEE.

[105] Yu, S., Thapngam, T., Liu, J., Wei, S. and Zhou, W. Discriminating DDoS flows from flash crowds using information distance. In *Network and System Security, 2009. NSS'09. Third International Conference on*, pages 351-356, 2009. IEEE.

[106] Segura, V. and Lahuerta, J. Modeling the economic incentives of ddos attacks: Femtocell case study. In *Economics of information security and privacy*, pages 107-119, 2010.

[107] Lee, F.Y. and Shieh, S. Defending against spoofed DDoS attacks with path fingerprint. *Computers and Security*, 24(7):571-586, 2005.

[108] Chen, Y., Hwang, K. and Kwok, Y.K. Filtering of shrew DDoS attacks in frequency domain. In *Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on*, pages 8-12, 2005. IEEE.

[109] Al-Duwairi, B. and Govindarasu, M. Novel hybrid schemes employing packet marking and logging for IP traceback. *IEEE Transactions on Parallel and Distributed Systems*, 17(5):403-418, 2006.

[110] Malliga, S., Tamilarasi, A., and Janani, M. Filtering spoofed traffic at source end for defending against DoS/DDoS attacks. In *Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on*, pages 1-5, 2008. IEEE.

[111] Mirkovic, J., Prier, G., and Reiher, P. Attacking DDoS at the source. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, pages 312-321, 2002. IEEE.

[112] Beverly, R. and Bauer, S. The Spoofer project: Inferring the extent of source address filtering on the Internet. In *Usenix Sruti*, pages 53-59, 2005.

[113] Xiang, Y., Zhou, W. and Guo, M. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks. *IEEE Transactions on Parallel and Distributed Systems*, 20(4):567-580, 2009.

[114] Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Schwartz, B., Kent, S.T. and Strayer, W.T. Single-packet IP traceback. *IEEE/ACM Transactions on Networking (ToN)*, 10(6):721-734, 2002.

[115] Zhang, L. and Guan, Y. TOPO: A topology-aware single packet attack traceback scheme. In *Securecomm and Workshops*, pages 1-10, 2006. IEEE.

[116] Yang, M.H. and Yang, M.C. RIHT: A novel hybrid IP traceback scheme. *IEEE Transactions on Information Forensics and Security*, 7(2):789-797, 2012.

[117] Gao, Z., and Ansari, N. (2005). Tracing cyber attacks from the practical perspective. *Communications Magazine, IEEE*, 43(5):123-131, 2005.

[118] Rahmani, H., Sahli, N. and Kamoun, F. DDoS flooding attack detection scheme based on F-divergence. *Computer Communications*, 35(11):1380-1391, 2012.

[119] Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Kent, S. T., & Strayer, W. T. Hash-based IP traceback. In *ACM SIGCOMM Computer Communication Review*, 31(4):3-14, 2001.

[120] Vincent, S., and Raja, J. I. J. A survey of IP traceback mechanisms to overcome denial-of-service attacks. In *Proceedings of the 12th international conference on Networking, VLSI and signal processing*, pages 93-98, 2010. World Scientific and Engineering Academy and Society (WSEAS).

[121] Bhattacharyya, D. K. and Kalita, J. K. DDoS Attacks: Evolution, Detection, Prevention, Reaction and Tolerance. *CRC Press, Taylor and Francis Group,* May, 2016.

[122] Malliga, S., and Tamilarasi, A. A proposal for new marking scheme with its performance evaluation for IP traceback. *WSEAS Transactions on Computer Research*, 3(4):259-272, 2008.

[123] Malliga, S., and Tamilarasi, A. A hybrid scheme using packet marking and logging for IP traceback. *International Journal of Internet Protocol Technology*, 5(1-2):81-91, 2010.

[124] Tian, H., Bi, J., Jiang, X. and Zhang, W. A probabilistic marking scheme for fast traceback. In *Evolving Internet (INTERNET), 2010 Second International Conference on*, pages 137-141, 2010. IEEE.

[125] Cheng, L., Divakaran, D.M., Ang, A.W.K., Lim, W.Y. and Thing, V.L. FACT: A Framework for Authentication in Cloud-Based IP Traceback. *IEEE Transactions on Information Forensics and Security*, 12(3):604-616, 2017.

[126] Chen, Y. and Hwang, K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. *Journal of Parallel and Distributed Computing*, 66(9):1137-1151, 2006.

[127] Gong, C. and Sarac, K. A more practical approach for single-packet IP traceback using packet logging and marking. *IEEE Transactions on Parallel and Distributed Systems*, 19(10):1310-1324, 2008.

[128] Kumar, V.A., Jayalekshmy, P.S., Patra, G.K. and Thangavelu, R.P. On remote exploitation of TCP sender for low-rate flooding denial-of-service attack. *IEEE Communications Letters*, 13(1):46-48, 2009.

[129] Braga, R., Mota, E. and Passito, A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. In *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, pages 408-415, 2010. IEEE.

[130] Sun, H., Zhaung, Y. and Chao, H.J. A principal components analysis-based robust DDoS defense system. In *Communications, 2008. ICC'08. IEEE International Conference on*, pages 1663-1669, 2008. IEEE.

[131] Kim, Y., Lau, W.C., Chuah, M.C. and Chao, H.J. PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. *IEEE transactions on dependable and secure computing*, 3(2):141-155, 2006.

[132] Ayres, P.E., Sun, H., Chao, H.J. and Lau, W.C. ALPi: A DDoS defense system for high-speed networks. *IEEE Journal on Selected Areas in Communications*, 24(10):1864-1876, 2006.

[133] Chen, Q., Lin, W., Dou, W. and Yu, S. CBF: a packet filtering method for DDoS attack defense in cloud environment. In *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, pages 427-434, 2011. IEEE.

[134] Kalkan, K., Gr, G. and Alagz, F.Filtering-based defense mechanisms against DDoS attacks: A survey. *IEEE Systems Journal*, 2016.

[135] Kalkan, K., Gur, G. and Alagoz, F.Defense Mechanisms against DDoS Attacks in SDN Environment. *IEEE Communications Magazine*, 55(9):175-179, 2017.

[136] Yang, X., Han, B., Sun, Z. and Huang, J. SDN-based DDoS Attack Detection with Cross-Plane Collaboration and Lightweight Flow Monitoring. *GLOBECOM*, 2017.

[137] Yu, S., Tian, Y., Guo, S. and Wu, D.O.Can we beat DDoS attacks in clouds?. *IEEE Transactions on Parallel and Distributed Systems*, 25(9):2245-2254, 2014.

[138] Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Schwartz, B., and Strayer, W. T. Single-packet IP traceback. *IEEE/ACM Transactions on Networking (ToN)*, 10(6):721-734, 2002.

[139] Bloom, B.H. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422-426, 1970.

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

[141] Liu, B., Bi, J. and Vasilakos, A.V. Toward incentivizing anti-spoofing deployment. *IEEE Transactions on Information Forensics and Security*, 9(3):436-450, 2014.

[142] Amin, S.O. and Hong, C.S., 2006, February. On ipv6 traceback. In *Advanced Communication Technology*, pages 5-10, 2006,IEEE.

[143] Cheng, L., Divakaran, D.M., Lim, W.Y. and Thing, V.L., Opportunistic piggyback marking for IP traceback. *IEEE Transactions on Information Forensics and Security*, 11(2):273-288, 2016.

[144] An, H., Lee, H. and Perrig, A. Coordination of anti-spoofing mechanisms in partial deployments, *Journal of Communications and Networks*, 18(6):948-961, 2016.

[145] Geva, M., Herzberg, A. and Gev, Y. Bandwidth distributed denial of service: Attacks and defenses. *IEEE Security & Privacy*, 12(1):54-61, 2014.

[146] *DDoS attack halts heating in Finland amidst winter.* Retrieved on 10 Dec. 2017 from (`http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter`)

[147] *Danish Railway Company DSB Suffers DDoS Attack.* Retrieved on 10 July. 2018 from (`https://www.infosecurity-magazine.com/news/danish-railway-ddos-attack/`)

[148] *DDoS Attacks on Swedens Transit System Signal a Significant Threat.* Retrieved on 10 Dec. 2017 from (`https://www.corero.com/blog/847-ddos-attacks-on-swedens-transit-system-signal-a-significant-threat.html`)

[149] *WannaCry Ransomware Attack Wreaks Havoc Across Globe.* Retrieved on 10 Dec. 2017 from (`https://www.corero.com/blog/818-wannacry-ransomware-attack-wreaks-havoc-across-globe.html`)

[150] Maglaras, L.A., Kim, K.H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., Maglaras, A. and Cruz, T.J., *Cyber security of critical infrastructures, ICT Express, 2018.*

[151] Goh, J., Adepu, S., Tan, M. and Lee, Z.S., January. Anomaly detection in cyber physical systems using recurrent neural networks. In High Assurance Systems Engineering (HASE), 2017 IEEE 18th International Symposium on, pages 140-145, 2017, IEEE.

[152] Goh, J., Adepu, S., Junejo, K.N. and Mathur, A.,. A dataset to support research in the design of secure water treatment systems. In *International Conference on Critical Information Infrastructures Security*, pages 88-99, 2016, Springer, Cham.

[153] Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C.M. and Sun, J.,. Anomaly detection for a water treatment system using unsupervised machine learning. In *Data Mining Workshops (ICDMW), 2017 IEEE International Conference on*, pages 1058-1065, 2017, November, IEEE.

[154] Lin, Q., Adepu, S., Verwer, S. and Mathur, A., 2018, May. TABOR: A Graphical Model-based Approach for Anomaly Detection in Industrial Control Systems. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 525-536, 2018, ACM.

[155] Laso, P.M., Brosset, D. and Puentes, J., Dataset of anomalies and malicious acts in a cyber-physical subsystem. *Data in brief*, 14(1):186-191, 2017.

[156] Choi, S., Lee, W., Shin, H.K., Yun, J.H. and Kim, S.K., POSTER: CPS Security Testbed Development Using Controller-in-the-Middle. In *Proceedings*

of the 2018 on Asia Conference on Computer and Communications Security, pages 829-831, 2018, May, ACM.

[157] *Mirai Botnet DDoS Attack Type*. Retrieved on 10 Dec. 2017 from (`https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html`)

[158] *JenX Botnet: A New IoT Botnet Threatening All*. Retrieved on 10 Feb. 2018 from (`https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx/`)

[159] *Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869*. Retrieved on 10 Dec. 2017 from (`http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-`

[160] *BrickerBot PDoS Attack: Back With A Vengeance*. Retrieved on 10 Dec. 2017 from (`https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/`)

[161] *Hajime Sophisticated, Flexible, Thoughtfully Designed and Future-Proof*. Retrieved on 10 Dec. 2017 from (`https://blog.radware.com/security/2017/04/hajime-futureproof-botnet/`)

[162] *OMG: Mirai-based Bot Turns IoT Devices into Proxy Servers*. Retrieved on 20 March. 2018 from (`https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html`)

[163] *Wicked Comes For IoT Devices*. Retrieved on 5 June. 2018 from (`https://civsourceonline.com/2018/05/21/wicked-bot-comes-for-iot-devices/`)

[164] *IoTroop/Reaper: A Massive Botnet Cyberstorm Is Coming To Take Down The Internet*. Retrieved on 10 Dec. 2017 from (`https://fossbytes.com/iotroop-reaper-botnet-attack/`)

[165] *KrebsOnSecurity Hit With Record DDoS*. Retrieved on 10 Dec. 2017 from (`https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/`)

[166] *Record-breaking DDoS reportedly delivered by >145k hacked cameras.* Retrieved on 10 Dec. 2017 from (`https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/`)