[50] Perényi M, Dang T D, Gefferth A, *et al*. Identification and analysis of peer-to-peer traffic. Journal of Communications, 2006,1(7): 36–46. [doi: 10.1109/ICIW.2010.36]

[51] John W, Tafvelin S. Heuristics to classify Internet backbone traffic based on connection patterns. In: Proc. of the Int'l Conf. on Information Networking, ICOIN 2008. IEEE, 2008. 1–5. [doi: 10.1109/ICOIN.2008.4472818]

[52] Barker J, Hannay P, Szewczyk P. Using traffic analysis to identify the second generation onion router. In: Proc. of the 9th IFIP Int'l Conf. on Embedded and Ubiquitous Computing (EUC). IEEE, 2011. 72–78. [doi: 10.1109/EUC.2011.76]

[53] Dixon L, Ristenpart T, Shrimpton T. Network traffic obfuscation and automated Internet censorship. IEEE Security & Privacy, 2016,14(6):43–53. [doi: 10.1109/MSP.2016.121]

[54] Song M, Xiong G, Li Z, *et al*. A de-anonymize attack method based on traffic analysis. In: Proc. of the Int'l ICST Conf. on Communications and NETWORKING in China. IEEE, 2014. 455–460. [doi: 10.1109/ChinaCom.2013.6694639]

[55] Almubayed A, Hadi A, Atoum J. A model for detecting Tor encrypted traffic using supervised. Machine Learning, 2015,7(7): 10–23.

[56] Shahbar K, Zincir-Heywood AN. Benchmarking two techniques for Tor classification: Flow level and circuit level classification. In: Proc. of the Computational Intelligence in Cyber Security. IEEE, 2015. 1–8. [doi: 10.1109/CICYBS.2014.7013368]

[57] Lashkari AH, Gil GD, Mamun MSI, *et al*. Characterization of Tor traffic using time based features. In: Proc. of the Int'l Conf. on Information Systems Security and Privacy. 2017. 253–262.

[58] Deng Z, Qian G, Chen Z, *et al*. Identifying Tor anonymous traffic based on gravitational clustering analysis. In: Proc. of the Int'l Conf. on Intelligent Human-Machine Systems and Cybernetics. IEEE, 2017. [doi: 10.1109/IHMSC.2017.133]

[59] Hodo E, Bellekens X, Iorkyase E, *et al*. Machine learning approach for detection of nonTor traffic. Journal of Cyber Security and Mobility, 2017,6(2):171–194.

[60] Lotfollahi M, Shirali R, Siavoshani MJ, *et al*. Deep packet: A novel approach for encrypted traffic classification using deep learning. 2017. http://xueshu.baidu.com/s?wd=paperuri%3A%282bdf662742490a13dadbc5c37fbd0aff%29&filter=sc_long_sign&tn=SE_xueshusource_2kduw22v&sc_vurl=http%3A%2F%2Farxiv.org%2Fpdf%2F1709.02656&ie=utf-8&sc_us=7953292138050080248

[61] Tor-nonTor dataset. http://www.unb.ca/cic/datasets/tor.html

[62] Zhao GF, Chao-Ming JI, Chuan XU. Survey of techniques for Internet traffic identification. Journal of Chinese Computer Systems, 2010,31(8):1514–1520 (in Chinese with English abstract).

[63] Wang J, He H, Luo X, *et al*. Network traffic classification based on ensemble learning and co-training. Science in China, 2009, 52(2):338–346.

[64] Lü B, Liao Y, Xie HY. Survey on attack technologies to Tor anonymous network. Journal of CAEIT, 2017,12(1):14–19 (in Chinese with English abstract).

[65] Berthold O, Federrath H, Köhntopp M. Project anonymity and unobservability in the Internet. In: Proc. of the 10th Conf. on Computers, Freedom and Privacy: Challenging the Assumptions. ACM, 2000. 57–65.

[66] Agrawal D, Kesdogan D. Measuring anonymity: The disclosure attack. IEEE Security & Privacy, 2003,99(6):27–34. [doi: 10.1109/MSECP.2003.1253565]

[67] Danezis G. Statistical disclosure attacks. In: Security and Privacy in the Age of Uncertainty. Boston: Springer-Verlag, 2003. 421–426.

[68] Qin Y, Huang D, Li B. STARS: A statistical traffic pattern discovery system for MANETs. IEEE Trans. on Dependable and Secure Computing, 2014,11(2):181–192. [doi: 10.1109/TDSC.2013.33]

[69] Mallesh N, Wright M. An analysis of the statistical disclosure attack and receiver-bound cover. Computers & Security, 2011,30(8): 597–612. [doi: 10.1016/j.cose.2011.08.011]

[70] Bagai R, Lu H, Tang B. On the sender cover traffic countermeasure against an improved statistical disclosure attack. In: Proc. of the IEEE/IFIP Int'l Conf. on Embedded and Ubiquitous Computing. IEEE, 2011. 555–560. [doi: 10.1109/EUC.2010.90]

[71] Herrmann D, Wendolsky R, Federrath H. Website fingerprinting: Attacking popular privacy enhancing technologies with the multinomial Naïve-Bayes classifier. In: Proc. of the CCS 2009, Cloud Computing Security Workshop. 2009. 31–42. [doi: 10.1145/1655008.1655013]

[72] Murdoch SJ, Danezis G. Low-Cost traffic analysis of Tor. In: Proc. of the IEEE Symp. on Security & Privacy. IEEE, 2005. 183–195. [doi: 10.1109/SP.2005.12]

[73] Fusenig V, Staab E, Sorger U, *et al*. Slotted packet counting attacks on anonymity protocols. In: Proc. of the Australasian Conf. on Information Security. Australian Computer Society, Inc., 2009. 53–60.

[74] Murdoch SJ. Hot or not: Revealing hidden services by their clock skew. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. ACM, 2006. 27–36.

[75] Weinberg Z, Wang J, Yegneswaran V, *et al*. StegoTorus: A camouflage proxy for the Tor anonymity system. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. ACM, 2012. 109–120.

[76] Biryukov A, Pustogarov I, Weinmann RP. Trawling for tor hidden services: Detection, measurement, deanonymization. In: Proc. of the 2013 IEEE Symp. on Security and Privacy (SP). IEEE, 2013. 80–94 .[doi: 10.1109/SP.2013.15]

[77] Liberatore M, Levine BN. Inferring the source of encrypted HTTP connections. In: Proc. of the ACM Conf. on Computer and Communications Security. ACM, 2006. 255–263.

[78] Wang T, Cai X, Nithyanand R, *et al*. Effective attacks and provable defenses for Website fingerprinting. In: Proc. of the USENIX Security Symp. 2014. 143–157.

[79] Kwon A, AlSabah M, Lazar D, *et al*. Circuit fingerprinting attacks: Passive deanonymization of tor hidden services. In: Proc. of the USENIX Security. 2015. 20.

[80] Hayes J, Danezis G. *k*-Fingerprinting: A robust scalable Website fingerprinting technique. In: Proc. of the USENIX Security Symp. 2016. 1187–1203.

[81] Zhuo Z, Zhang Y, Zhang Z, *et al*. Website fingerprinting attack on anonymity networks based on profile hidden Markov model. IEEE Trans. on Information Forensics and Security, 2017. [doi: 10.1109/TIFS.2017.2762825]

[82] Juarez M, Afroz S, Acar G, *et al*. A critical evaluation of Website fingerprinting attacks. In: Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2014. 263–274. [doi: 10.1145/2660267.2660368]

[83] Guo XJ, Cheng G, Zhu CG, *et al*. Progress in research on active network flow watermark. Journal on Communications, 2014,35(7): 178–192 (in Chinese with English abstract). [doi: 1000-436X(2014)07-0178-15]

[84] Pyun YJ, Park YH, Wang X, *et al*. Tracing traffic through intermediate hosts that repacketize flows. In: Proc. of the INFOCOM the 26th IEEE Int'l Conf. on Computer Communications. IEEE, 2007. 634–642. [doi: 10.1109/INFCOM.2007.80]

[85] Houmansadr A, Borisov N. SWIRL: A scalable watermark to detect correlated network flows. In: Proc.of the Network and Distributed System Security Symp., NDSS 2011. San Diego: DBLP, 2011.

[86] Kiyavash N, Houmansadr A, Borisov N. Multi-Flow attacks against network flow watermarking schemes. In: Proc. of the Conf. on Security Symp. USENIX Association, 2008. 307–320.

[87] Luo J, Wang X, Yang M. An interval centroid based spread spectrum watermarking scheme for multi-flow traceback. Journal of Network and Computer Applications, 2012,35(1):60–71. [doi: 10.1016/j.jnca.2011.03.003]

[88] Wang X, Luo J, Yang M. A double interval centroid-based watermark for network flow traceback. In: Proc. of the Int'l Conf. on Computer Supported Cooperative Work in Design. IEEE, 2010. 146–151. [doi: 10.1109/CSCWD.2010.5471985]

[89] Wang X, Luo J, Yang M, *et al*. A novel flow multiplication attack against Tor. In: Proc. of the Int'l Conf. on Computer Supported Cooperative Work in Design. IEEE Computer Society, 2009. 686–691. [doi: 10.1109/CSCWD.2009.4968138]

[90] Abbott TG, Lai KJ, Lieberman MR, *et al*. Browser-Based attacks on Tor. In: Proc. of the Int'l Symp. on Privacy Enhancing Technologies, PET 2007. Ottawa: DBLP, 2007. 184–199.

[91] Dainotti A, Pescape A, Ventre G. A packet-level traffic model of starcraft. In: Proc. of the Int'l Workshop on Hot Topics in Peer-to-Peer Systems, Hot-P2P. IEEE, 2005. 33–42. [doi: 10.1109/PTPSYS.2005.4]

[92] Murdoch SJ, Danezis G. Low-Cost traffic analysis of Tor. In: Proc. of the 2005 IEEE Symp. on Security and Privacy. IEEE, 2005. 183–195. [doi: 10.1109/SP.2005.12]

[93] Mclachlan J, Hopper N. On the risks of serving whenever you surf: Vulnerabilities in Tor's blocking resistance design. In: Proc. of the ACM Workshop on Privacy in the Electronic Society. ACM, 2009. 31–40. [doi: 10.1145/1655188.1655193]

[94] Winter P, Lindskog S. How China is blocking Tor. In: Proc. of the USENIX Workshop on Free and Open Communications on the Internet (FOCI). 2012.

[95] Ensafi R, Winter P, Mueen A, *et al*. Analyzing the Great Firewall of China over space and time. Proc. on Privacy Enhancing Technologies, 2015,2015(1):61–76. [doi: 10.1515/popets-2015-0005]

[96] Tan J, Chen XS, Min DU, *et al*. Internet traffic identification algorithm based on adaptive BP neural network. In: Proc. of the Workshop on Intelligent Information Technology Applications. IEEE, 2012. 151–154. [doi: 10.3969/j.issn.1001-0548.2012.04.020]

[97] Ling Z, Luo J, Wu K, *et al*. TorWard: Discovery, blocking, and traceback of malicious traffic over Tor. IEEE Trans. on Information Forensics & Security, 2015,10(12):2515–2530. [doi: 10.1109/TIFS.2015.2465934]

附中文参考文献:

[14] 黄艳梅,林艳华.跨国网络犯罪愈演愈烈中国东盟谋求携手打击.2015. http://www.12377.cn/txt/2015-09/15/content_8235494.htm

[17] 工业和信息化部.工业和信息化部关于清理规范互联网网络接入服务市场的通知.http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html

[18] 何高峰,杨明,罗军舟,张璐.Tor 匿名通信流量在线识别方法.软件学报,2013(3):540–556. http://www.jos.org.cn/1000-9825/4253.htm [doi: 10.3724/SP.J.1001.2013.04253]

[32] 李响.基于 Meek 的 Tor 匿名通信识别方法的研究和实现[硕士学位论文].北京:北京交通大学,2016.

[33] 谭庆丰,时金桥,方滨兴,等.匿名通信系统不可观测性度量方法.计算机研究与发展,2015,52(10):2373–2381. [doi: 10.3969/j.issn.1001-0548.2012.04.020]

[39] 何永忠,陈美玲.基于协议的拟态研究综述.北京交通大学学报,2016,40(5):1–8. [doi:10.11860/j.issn.1673-0291.2016.05.001]

[42] 吴倩.基于 DPI 与 DFI 的流量识别与控制系统的设计与实现[博士学位论文].成都:电子科技大学,2013.

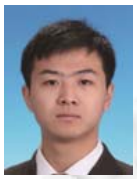
[44] 鲁刚,张宏莉,叶麟.P2P 流量识别.软件学报,2011,22(6):1281−1298. http://www.jos.org.cn/1000-9825/3995.htm [doi: 10.3724/SP.J.1001.2011.03995]

[48] 吴震,刘兴彬,童晓民.基于信息熵的流量识别方法.计算机工程,2009,35(20):115−116.

[62] 赵国锋,吉朝明,徐川.Internet 流量识别技术研究.小型微型计算机系统,2010,31(8):1514–1520. [doi:1000-1220(2010)08-1514-07]

[64] 吕博,廖勇,谢海永.Tor 匿名网络攻击技术综述.中国电子科学研究院学报,2017,12(1):14–19. [doi:10.3969/j.issn.1673-5692.2017.01.003]

[83] 郭晓军,程光,朱琛刚,等.主动网络流水印技术研究进展.通信学报,2014,35(7):178–192. [doi:10.3969/j.issn.1000-436x.2014.07.022]



姚忠将(1988－),男,山东聊城人,博士生,主要研究领域为流量识别与追踪,区块链,隐私保护,机器学习.

葛敬国(1973－),男,博士,研究员,博士生导师,主要研究领域为软件定义网络,网络虚拟化,云计算.

张潇丹(1983－),女,博士,副研究员,主要研究领域为未来网络实验环境,网络虚拟化及软件定义网络,新型网络技术测量分析与评估.

郑宏波(1977－),男,工程师,主要研究领域为软件定义网络,网络虚拟化,云计算.

邹壮(1993－),男,硕士生,主要研究领域为软件定义网络,网络虚拟化,云计算.

孙焜焜(1995－),男,硕士生,主要研究领域为软件定义网络.

许子豪(1995－),男,硕士生,主要研究领域为软件定义网络,网络功能虚拟化.