证实爱丽丝与鲍勃之间存在通信关系,在爱丽丝出口处设置调制器将水印信息嵌入流量,然后在鲍勃接收前设置检测器检测水印信息,如果水印信息匹配,则证明爱丽丝与鲍勃之间具有通信关系.ANFW 根据水印嵌入方式,将流水印分为基于流速的流水印和基于时间特征的流水印.

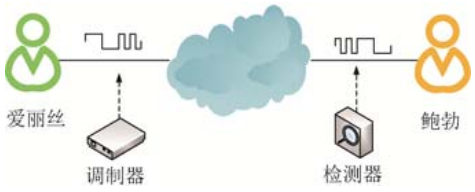


Fig.4 Architecture of flow watermark technology

图 4 流水印使用方法

(1) 基于流速

基于流速的流水印技术主要依靠调制流量发送速率.扩频是调制流量发送速率的典型方法.在物理层对发送信号按照某种扩频函数(如利用伪噪声 pseudo-noise,简称 PN)扩展频带宽度.扩频函数就是水印嵌入方法,嵌入的信息被称为水印信号.直序扩频(DSSS)[35]是扩频水印的典型代表.追踪者对原始信号 D_s 加入水印(PN_s 码)信号后得到信号 S_s,经路由转发(假设未受干扰)后,追踪者提取信号 S_r,如果 S_S=S_r,则利用 PN_r 逆运算可恢复原始信号 D_r.

$$D_r=\frac{\sum S_r\cdot PN_r}{N}=D_s\frac{\sum PN_s\cdot PN_r}{N}.$$

扩频流水印提供一个隐蔽、实时的流量追踪技术.目前尚未有允许用户消除扩频流水印的解决方案.

(2) 基于时间

基于时间的流水印技术分为两种:(1) 基于报文间隔;(2) 基于时隙分割.基于报文间隔的流水印技术通过调整间隔嵌入水印.Wang 在 2003 年提出的 IBW 方法通过随机选取流内两个包分组,调整分组到达或离开的时间间隔以实现水印注入[84].为了解决 MFA 攻击威胁,Houmansadr 提出 SWIRL[85].SWIRL 算法虽然具有良好的多流攻击、拥塞攻击抵御能力,但易受抖动和垃圾包注入的干扰,鲁棒性较差.基于时隙分割的流水印技术按照时隙分组嵌入水印.基于时隙分割流水印技术的典型实例是基于时隙质心的流水印技术[36].将 2n 个时隙按照水印信号的 bit 数分为 2 个组,每个组包含 L 个小组,每个小组对应 n/L 个时隙.如下计算各小组时隙质心:

$$Cent(I_i)=\frac{1}{n_i}\sum_{j=0}^{n_i-1}\Delta t_{ij}.$$

计算两个群中对应同一水印 bit 的时隙差.水印调制模块根据差值决定每个组的延时增量.

基于时隙质心的流水印技术虽然具有较好的隐蔽性和抗干扰能力,但 Kiyavash 针对 IBW、ICBW 提出多流攻击(MFA)[86].Luo 等人将 ICBW 与 DSSS 相结合,提出基于直序扩频的时隙质心流水印方法(interval centroid based spread spectrum watermarking,简称 ICBSSW)[87],在应对 MSAC 攻击和 MFA 方面具有较好的效果.同时,具有追踪多条流的能力,但算法复杂度高,开销大,实用性低.Wang 提出的 DICBW[88]在抵御 MFA、网络干扰、流分割与合并等方面有较好表现.

3.2.2 渗 透

(1) 中间人

混淆技术难以抵御中间人攻击.审查者提出基于 HTTP 的中间人攻击,利用受控节点嵌入指定数量图片标签的页面,发现客户端与 Web 服务器通信[89].嵌入图片增加了通信开销,隐蔽性差.研究者利用受控出口节点在 HTTP 中嵌入 JavaScript 或 HTML 代码,进行中间人攻击[90].基于 botnet 的技术,利用 bot master 控制大量沦陷的网络节点监控网络活动[91].卡内基梅隆大学研究员 Michael 和 Alexander 提出了打入受控卧底节点破解 Tor 网络的方法,这与 FBI 侦破丝绸之路的方法不谋而合.为了提高追踪效率,Murdoch 和 Danezis 提出 Circuit Clogging 方案,用探针探测 Tor Relay 节点流量并假冒服务器做出回应[92].

(2) 节点发现

VPN 只有一个代理节点.利用混淆流量识别技术即可发现 VPN 代理节点.但 Tor 中继节点信息或网桥信息是非公开且变化的,混淆技术的引入增强了 Tor 中继节点和网桥的隐蔽性,基于 Tor 的混淆流量追踪具有很大的挑战性.Mclachlan 等人提出基于大量邮件和 HTTP 服务器中包含的隐藏网桥信息进行枚举攻击[93].Winter 和 Ensafi 等人推断 GFW(The Great FireWall of China)通过流量识别技术和节点发现攻击技术确认发往 Tor 网桥的混淆流量,并调度扫描节点伪造连接请求以尝试连接 Tor 网桥[94,95].

(3) 重放

重放攻击重复发送通信中被截取的报文,干扰信息的正常接收.假设攻击者控制某节点复制混淆流量,沿相同方向再次发送相同报文就会扰乱 Tor 节点计数器计数,造成解密失败[47].通过受控恶意入口节点复制、篡改发送的报文导致出口节点无法识别[96].Zhen 提出基于 Tor 的发现、阻断和追踪恶意流量的系统 TorWard[97].TorWard 在 Tor 出口节点部署入侵检测系统(IDS),用于 Tor 恶意流量的检测、阻断和追踪.TorWard 中出口节点作为代理提取转出流量信息,交给自动管理工具后重新将流量注入 Tor 网络中发往服务端.

流量追踪技术对比分析

本节汇总流量追踪技术,细节可见表 4.从汇总表可以看出,被动关联技术包括揭露分析、流量形状和流量指纹技术.但是 3 种方法均需在网络中部署探针被动采集大量流量,并做大量分析计算工作,实时性差.Song 等人使用 *K*-means 聚类算法实现 Tor 入口流量和 Tor 出口流量的关联,为被动关联技术提高追踪效率提供借鉴[54].主动关联技术以流水印技术和渗透技术为主.两种主动关联技术都可以简单、有效地达到追踪目的,但是流水印技术容易受到报文重放、篡改、乱序等情况的干扰,渗透技术部署难度大、成本高.

被动关联技术以流量识别技术为基础,对流量特征依赖性较强,故对随机化流量、拟态流量追踪能力较差.主动关联技术中的流水印技术操作简单,精度高,可以追踪任何混淆流量,因此将会是未来发展的趋势.渗透技术因可有效探知任何混淆流量,可同时追踪多种流量,自产生至今一直沿用.但其部署难度大、成本高是影响其广泛使用的重要因素.如何克服这些弊端将是研究渗透技术的未来研究重点.

Table 4 Flow tracking technology summary

表 4 流量追踪技术汇总表

分类	追踪技术		追踪障碍	混淆工具	精确率
被动关联技术	揭露分析技术		交集范围限制	任何混淆技术	与流量采集规模有关
	流量形状攻击		重放、广播等	任何混淆技术	与流量采集规模有关
	流量指纹技术		混淆能力	任何混淆技术	与流量采集规模有关
主动关联技术	流水印技术	基于流速	多流攻击	任何混淆技术	–
		基于时间	丢包、重组、乱序、多流攻击	任何混淆技术	与时隙内报文个数相关
	渗透技术	节点发现	节点信息隐藏	Tor	追踪到第 1 跳节点前
		中间人	成本、部署	任何混淆技术	与受控节点数量有关
		重放攻击	时间检测	任何混淆技术	–

4 总 结

本文从当前审查规避系统的背景入手,描述了流量混淆技术的重要性,分析了当前比较重要的 3 类流量混淆技术,总结了混淆技术框架并分析其隐蔽性.从混淆技术出发,进一步探讨了针对混淆流量的识别技术,并将其按照混淆技术类型分为基于深度包检测的流量识别技术和基于机器学习的流量识别技术.随着网络的发展和人工智能的广泛应用,实时性和智能化将会成为流量识别的趋势.为了进一步威慑非法网络行为,审查者开始研究流量追踪技术.流量追踪技术包含被动关联和主动关联技术两种.被动关联存在开销大、周期长等弊端,机器学习技术在流量分析上具有高效、准确等特点,将是未来研究的方向.主动关联技术减少了数据处理规模和计算开销,但流水印技术抗干扰能力差,难以抵抗多流攻击等,而渗透技术部署难度大、成本高.流水印技术的当务之急是提高抗干扰能力和抵抗攻击能力,而轻量型低成本是渗透技术未来的研究方向.

References:

[1] Chaum DL. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981,24(2): 84–90. [doi: 10.1145/358549.358563]

[2] Boyan J. The Anonymizer: Protecting user privacy on the Web. Computer-Mediated Communication (CMC) Magazine, 1997.

[3] Reiter MK, Rubin A D. Crowds: Anonymity for Web transactions. ACM Trans. on Information and System Security (TISSEC), 1998,1(1):66–92. [doi: 10.1145/290163.290168]

[4] Hao F, Zielinski P. A 2-round anonymous veto protocol. In: Proc. of the Security Protocols Workshop. 2006,5087:202–211. [doi: 10.1007/978-3-642-04904-028]

[5] Sherwood R, Bhattacharjee B, Srinivasan A. P5: A protocol for scalable anonymous communication. Journal of Computer Security, 2005,13(6):839–876. [doi: 10.1109/SECPRI.2002.1004362]

[6] Zantout B, Haraty R. I2P data communication system. In: Proc. of the ICN. 2011. 401–409.

[7] lantern. https://github.com/getlantern/lantern

[8] Kean S. Internet research, uncensored. Chronicle of Higher Education, 2007,53(29).

[9] SnapVPN. https://snap-vpn.cn.uptodown.com/android

[10] jisuVPN. http://jisuvpn.msnyou.com/

[11] Pokemonvpn. https://play.google.com/store/apps/details?id= com.xxykj.pokemonvpn

[12] VPN Usage Around the World-Q2. 2017. Globalwebindex. https://cdn2.hubspot.net/hubfs/304927/Downloads/VPN-Usage-Around-the-World-Infographic.pdf

[13] China Officially Outlaws Unauthorised VPNs. 2017. https://advox.globalvoices.org/2017/01/23/china-officially-outlaws-unauthorised-vpns/

[14] Huang Y, Lin Y. Transnational cybercrime is getting worse and stronger, China and ASEAN seek to join hands. 2015 (in Chinese). http://www.12377.cn/txt/2015-09/15/content_8235494.htm

[15] Aliens C. Terrorist used Tor to connect with ISIS, source said. 2017. https://www.deepdotweb.com/2017/06/26/terrorist-used-tor-connect-isis-source-said/

[16] Censorship of Twitter. https://en.wikipedia.org/wiki/Censorship_of_Twitter

[17] Ministry of Industry and Information Technology of the People's Republic of China (in Chinese). http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html

[18] He GF, Yang M, Luo JZ, Zhang L. Online identification of tor anonymous communication traffic. Ruan Jian Xue Bao/Journal of Software, 2014,24(3):540–546 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4253.htm [doi: 10.3724/SP.J.1001.2013.04253]

[19] Wiley B. Dust: A blocking-resistant internet transport protocol. Technical Report, 2011. http://blanu.net/Dust.pdf

[20] Kadianakis G, Mathewson G. Obfs2 (the twobfuscator). 2011. https://gitweb.torproject.org/pluggabletransports/obfsproxy.git/tree/doc/obfs2/obfs2-protocolspec.txt

[21] Kadianakis G, Mathewson G. obfs3 (the threebfuscator). 2013. https://gitweb.torproject.org/pluggabletransports/obfs proxy.git/tree/doc/obfs3/obfs3-protocolspec.txt

[22] Angel Y ,Winter P. obfs4 (the obfourscator). 2014. https://gitweb.torproject.org/pluggable-transports/obfs4.git/tree/doc/obfs4-spec.txt

[23] Winter P, Pulls T, Fuss J. ScrambleSuit: A polymorphic network protocol to circumvent censorship. In: Proc. of the 12th ACM Workshop on Privacy in the Electronic Society. ACM, 2013. 213–224.

[24] Dyer KP, Coull SE, Ristenpart T, *et al*. Protocol misidentification made easy with format-transforming encryption. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. ACM, 2013. 61–72.

[25] Wang Q, Gong X, Nguyen GTK, *et al*. Censorspoofer: Asymmetric communication using IP spoofing for censorship-resistant Web browsing. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. ACM, 2012. 121–132.

[26] Mohajeri Moghaddam H, Li B, Derakhshani M, *et al*. Skypemorph: Protocol obfuscation for tor bridges. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. ACM, 2012. 97–108.

[27] Moghaddam MH. SkypeMorph: Protocol obfuscation for censorship resistance [MS. Thesis]. University of Waterloo, 2013.

[28] Brubaker C, Houmansadr A, Shmatikov V. Cloudtransport: Using cloud storage for censorship-resistant networking. In: Proc. of the Int'l Symp. on Privacy Enhancing Technologies Symp. Cham: Springer-Verlag, 2014. 1–20. [doi: 10.1007/978-3-319-08506-7_1]

[29] Fifield D, Lan C, Hynes R, *et al*. Blocking-Resistant communication through domain fronting. Proc. on Privacy Enhancing Technologies, 2015,2015(2):46–64.

[30] Karlin J, Ellard D, Jackson AW, *et al*. Decoy routing: Toward unblockable internet communication. In: Proc. of the USENIX Workshop on Free and Open Communications on the Internet. 2011. https://www.usenix.org/legacy/event/foci11/tech/final_files/Karlin.pdf

[31] Wang L, Dyer KP, Akella A, *et al*. Seeing through network-protocol obfuscation. In: Proc. of the ACM SIGSAC Conf. ACM, 2015. 57–69. [doi: 10.1145/2810103.2813715]

[32] Li X. Research and implementation of identification for Tor anonymous communication based on meek [MS. Thesis]. Beijing: Beijing Jiaotong University, 2016 (in Chinese with English abstract).

[33] Tan Q, Shi J, Fang B, *et al*. Towards measuring unobservability in anonymous communication systems. Journal of Computer Research and Development, 2015,52 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2015.20150562]

[34] Zhioua S. Tor traffic analysis using hidden Markov models. Security & Communication Networks, 2013,6(9):1075–1086. [doi: 10.1002/sec.669]

[35] Yu W, Fu X, Graham S, *et al*. DSSS-Based flow marking technique for invisible traceback. In: Proc. of the IEEE Symp. on Security and Privacy. 2007. 18–32. [doi: 10.1109/SP.2007.14]

[36] Wang X, Chen S, Jajodia S. Network flow watermarking attack on low-latency anonymous communication systems. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2007. 116–130. [doi: 10.1109/SP.2007.30]

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

[38] Jia W, Tso FP, Ling Z, *et al*. Blind detection of spread spectrum flow watermarks. Security and Communication Networks, 2013,6(3):257–274.

[39] He YZ, Chen M. Protocol mimicry technique and its development. Journal of Beijing Jiaotong University, 2016 (in Chinese with English abstract). [doi: 10.11860/j.issn.1673-0291.2016.05.001]

[40] Wustrow E, Wolchok S, Goldberg I, *et al*. Telex: Anticensorship in the network infrastructure. 2011. https://www.usenix.org/legacy/event/sec11/tech/full_papers/Wustrow.pdf [doi: 10.1.1.211.418]

[41] Karlin J, Ellard D, Jackson AW, *et al*. Decoy routing: Toward unblockable Internet communication. In: Proc. of the USENIX Workshop on Free and Open Communications on the Internet. 2011. https://www.usenix.org/legacy/event/foci11/tech/final_files/Karlin.pdf

[42] Wu Q. Design and implementation DPI and DFI-based system of flow identification and control [Ph.D. Thesis]. Chengdu: University of Electronic Science and Technology of China, 2013 (in Chinese with English abstract).

[43] Nychis G, Sekar V, Andersen DG, *et al*. An empirical evaluation of entropy-based traffic anomaly detection. In: Proc. of the Internet Measurement Conf. 2008. 151–156. [doi: 10.1145/1452520.1452539]

[44] Lu G, Zhang HL, Ye L. P2P traffic identification. Ruan Jian Xue Bao/Journal of Software, 2011,22(6):1281−1298 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3995.htm [doi: 10.3724/SP.J.1001.2011.03995]

[45] Wright CV, Ballard L, Monrose F, *et al*. Language identification of encrypted VoIP traffic: Alejandray Robert or Alice and Bob? In: Proc. of the Usenix Security Symp. 2007. 4.

[46] Wiley B. Blocking-Resistant protocol classification using Bayesian model selection. Technical Report, University of Texas at Austin, 2011.

[47] Houmansadr A, Brubaker C, Shmatikov V. The parrot is dead: Observing unobservable network communications. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE Computer Society, 2013. 65–79. [doi: 10.1109/SP.2013.14]

[48] Wu Z, Liu XB, Tong XM. Traffic identification method based on information entropy. Computer Engineering, 2009,35(20): 115–117 (in Chinese with English abstract).

[49] Barker J, Hannay P, Bolan C. Using traffic analysis to identify tor usage—A proposed study. In: Proc. of the 2010 Int'l Conf. on Security & Management, SAM 2010, Vol.2. 2010.

[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.

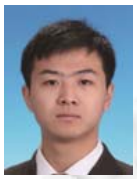
[44] 鲁刚,张宏莉,叶麟.P2P 流量识别.软件学报,2011,22(6):1281−1298. http://www.jos.org.cn/1000-9825/3995.htm [doi: 10.3724/SP.J.1001.2011.03995]

[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.