$$CCE=H(X_i|X_{i-1},\ldots,X_1)+p(X_i)\cdot H(X) \tag{12}$$

Archibald 等人[103]使用 K-L 离散对时间隐蔽信道进行检测.K-L 离散又被称为相对熵,是一种描述两个概率密度函数分布差异的方法,用来度量两个随机变量的距离,表示为对两个概率分布为 $P$ 和 $G$ 的非对称性的度量:

$$D_{KL}(P\,\|\,G)=\sum_x p(x)\cdot\log\left(\frac{p(x)}{g(x)}\right) \tag{13}$$

(4) 基于机器学习的检测

Shresth 等人[126]提出了一个基于机器学习检测网络时间隐蔽信道的框架,使用支持向量机方法对通信流量中的时间隐蔽信道进行检测,使用统计方法将通信流量的时间信息分为 4 个统计指纹类型:K-S 统计评分、规律性评分、熵评分和修正条件熵评分,并使用支持向量机的方法,基于这 4 类统计指纹对时间隐蔽信道进行训练和检测.

Zseby 等人[127]使用了 3 种基于密度的计算 $K$ 距离($k$-distance)的非监督学习方法:基于连通性的离群因子(connectivity-based outlier factor)、受影响的离群性(influenced outlierness)、基于直方图的离群评分(histogram-based outlier score,简称 HBOS)对 7 种不同时间隐蔽信道生成技术生成的隐蔽信道进行异常检测,发现尽管能将正常信道和隐蔽信道区分出来,但是无法区分出使用了哪种时间隐蔽信道技术生成了隐蔽信道.

Iglesias 等人[38]通过流量描述分析(descriptive analytics of traffic,简称 DAT)将网络通信数据转换为便于使用的特征向量,通过核密度估计和帕累托分析(Pareto analysis)挖掘基于描述性统计、聚合、自相关指数、多模态计算相结合的字段特征,为进一步使用基于机器学习对隐蔽信道的分析奠定了基础.之后,Iglesias 等人在文献[38]的基础上,使用流量描述分析技术对 8 个网络时间隐蔽信道生成技术生成的隐蔽信道网络流量进行特征提取,并用决策树(decision tree)方法对网络隐蔽信道进行检测[46].进一步按照最大化基于熵的增益比的原则选择并排序特征,并使用 C4.5 决策树分类器对基于包间隔的时间隐蔽信道进行检测[128].

(5) 对检测方法的评估

Archibald 等人[120]对 3 大类统计性分析方法进行了评估,通过对以 SSH 和 HTTP 两种协议作为公开信道,构建的 JitterBug 时间型网络隐蔽信道、重放时间型隐蔽信道和基于模型的时间型隐蔽信道这 3 类时间隐蔽信道的检测效率进行评估,评估指标包括适用性、计算复杂度、分类速度等方面.另外,Shrestha 等人[129]发现:如果把数据块变得过小(如 100 bits),基于熵的检测方法的可靠性就会下降.

综合相关研究,对于单一的时间型网络隐蔽信道的检测方法来说,没有哪种检测方法能够对所有类型的时间隐蔽信道都获得理想的效果.形态检测对 JitterBug 时间型网络隐蔽信道有较好的检测效果,但无法检测出基于重传的时间型隐蔽信道,因为基于重传的时间型隐蔽信道的时间间隔分布与合法的通信是一致的,对基于模型的时间型网络隐蔽信道的检测效果也不理想;规律性检测可以对基于模型的时间型网络隐蔽信道有较好的检测效果,但是对 JitterBug 时间型网络隐蔽信道的检测效果并不理想,因为 JitterBug 时间型网络隐蔽信道并不是根据某种统计模型生成的,对基于重传的时间型隐蔽信道的检测效果也不好;熵检测对基于重传的时间型隐蔽信道和基于模型的时间型网络隐蔽信道有较好的效果,但是对 JitterBug 时间型网络隐蔽信道检测效果不好,因为 JitterBug 时间型网络隐蔽信道是通过增加时间间隔的方式改变了时间间隔的分布而不改变熵.基于多特征的机器学习的时间型网络隐蔽信道检测方式,在准确率和适用范围上要优于基于单一检测技术的网络隐蔽信道检测方式.

### 4.4 小 结

本节从消除、限制、检测这 3 个方面分析了网络隐蔽信道的对抗技术.网络隐蔽信道构建研究的重心从最初的消除、限制技术,逐渐过渡到对网络隐蔽信道的检测技术.对于存储型网络隐蔽信道检测技术来说,一般采用对某一特定网络对象(例如网络协议)的特征(例如协议字段)进行训练建模,再通过机器学习的方式进行检测.对于时间型网络隐蔽信道来说,最初采用一阶统计技术和高阶统计技术进行单一技术检测的方式,之后逐渐转变为多种检测手段和特征进行建模和联合检测的方式.针对时间型网络隐蔽信道的基于统计学的检测指标也可以看作网络信息特征,因此从本质上来说,无论是存储型网络隐蔽信道检测技术还是时间型网络隐蔽信道检

测技术,现阶段研究的关键都是对特定网络隐蔽信道载体的特征提取和建模,进而提升检测的准确率和效率.

## 5 总结与展望

### 5.1 新计算环境下的网络隐蔽信道

新的通信载体下的网络隐蔽信道构建是很重要的研究方向[56,59,130,131].现阶段,大部分的网络隐蔽信道都是基于 TCP/IP 层的网络协议,随着新的计算环境的发展,新的通信环境可作为新的网络隐蔽信道技术构建的载体,发展出新的网络隐蔽信道构建技术及与之对应的对抗技术,例如工业控制系统(industrial control systems,简称 ICS)网络[131]、移动电话网络[132−134]、车载无线网络(vehicular ad hoc network,简称 VANET)[135]、云环境下的虚拟网络[136]等.

### 5.2 多样性和动态性的网络隐蔽信道

现阶段,大部分网络隐蔽信道都建立在单一不变的技术基础上,这使得审查方很容易针对特定类型的网络隐蔽信道采取相应的措施.当前的研究热点已经从网络隐蔽信道的码元设计逐渐转换到信道优化,特别是利用多样性和动态性的功能保障网络隐蔽信道传输[10,86,92,94].类型多样是网络隐蔽信道的一大特点,如何利用类型多样这一特点进行有针对性地动态调配通信手段,从而更好地保障隐蔽性,是网络隐蔽信道研究面临的挑战[45].

### 5.3 构建网络隐蔽信道通信网络

目前,网络隐蔽信道构建方法的研究重点偏向于网络隐蔽信道的隐蔽性,特别是在点对点的通信模式下,使用新的网络载体和新的构建技术构建网络隐蔽信道.然而真实网络环境复杂多变,点对点通信易于被针对,也难以应对真实网络环境的变化;另一方面,网络隐蔽信道的容量也是其发展的瓶颈之一,需要与信道载体(例如通信协议)争抢有限的带宽和计算资源.网络隐蔽信道通信网络针对点对点通信的弊端,以一组通信节点组成的网络隐蔽信道通信网络作为通信载体,实施多中转节点通信,从而提升了网络隐蔽信道的隐蔽性、鲁棒性和传输效率[24,86,92].

### 5.4 海量网络数据网络隐蔽信道检测技术

网络环境存在着大量的通信数据,这些通信数据都有存在网络隐蔽信道的潜在可能,而网络隐蔽信道的类型又很多样和复杂,这进一步增加了网络隐蔽信道检测的难度.如何从海量网络数据中快速、高效、准确地找出网络隐蔽信道,成为很有挑战的问题[107].目前,机器学习方法被越来越多地在这个方面使用[38,46,126−128].

## 6 结束语

网络隐蔽信道越来越多地应用在网络信息安全的攻击方面和安全传输方面,因此受到越来越多的关注.本文首先介绍了网络隐蔽信道的基本概念,将网络隐蔽信道相关研究按照构建、评估、对抗这 3 个方面进行了总结.网络隐蔽信道构建方面,将网络隐蔽信道构建技术划分为码元设计、信息编码、信道优化这 3 个技术环节,围绕 3 个能力维度,对存储型网络隐蔽信道和时间型网络隐蔽信道的构建技术进行了对比、整理、分析;网络隐蔽信道评估方面,对网络隐蔽信道隐蔽性、鲁棒性、传输效率的评估方法进行了汇总;网络隐蔽信道对抗方面,将现有技术分为消除、限制、检测这 3 个方面进行归纳分析.最后,对网络隐蔽信道未来研究方向进行了展望.试图为网络隐蔽信道研究方向勾勒出一个较为全面和清晰的概况,为相关领域的研究者提供参考.

**References**:

[1] Schechter SE, Smith MD. Access for sale: A new class of worm. In: Proc. of the ACM Workshop on Rapid Malcode. 2003. 19–23.

[2] Mazurczyk W, Caviglione L. Information hiding as a challenge for malware detection. IEEE Security & Privacy, 2015,13(2): 89–93.

[3] Li Z, Goyal A, Chen Y. Honeynet-based botnet scan traffic analysis. Botnet Detection, 2008,36:25–44.

[4] Gu G, Perdisci R, Zhang J, *et al*. BotMiner: Clustering analysis of network traffic for protocol-and structure-independent botnet detection. In: Proc. of the Usenix Security Symp. 2008. 139−154.

[5] Henry P. Covert channels provided hackers the opportunity and the means for the current distributed denial of service attacks. In: Proc. of the CyberGuard Corporation. 2000. 1−7.

[6] Freiling FC, Holz T, Wicherski G. Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. In: Proc. of the European Conf. on Research in Computer Security. 2005. 319−335.

[7] Singh A, Nordström O, Lu C, *et al*. Malicious ICMP Tunneling: Defense against the Vulnerability. Berlin, Heidelberg: Springer-Verlag, 2003. 226−235.

[8] Young A, Yung M. Deniable password snatching: On the possibility of evasive electronic espionage. In: Proc. of the IEEE Symp. on Security and Privacy. 1997. 224−235.

[9] Dabeer O, Sullivan K, Madhow U, *et al*. Detection of hiding in the least significant bit. IEEE Trans. on Signal Processing, 2004, 52(10):3046−3058.

[10] Xie H, Han Q. The research on hopping covert channel technique based on multi-protocol. In: Proc. of the 2016 2nd Int'l Conf. on Mechanical, Electronic and Information Technology Engineering. 2016. 227−231.

[11] Lou JP, Zhang M, Fu P, *et al*. Design of network covert transmission scheme based on TCP. Netinfo Security, 2016,16(1):34−39 (in Chinese with English abstract).

[12] Zander S, Armitage G, Branch P. A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Press, 2007. 44−57.

[13] Moskowitz IS, Newman RE, Syverson PF. Quasi-anonymous channels. In: Proc. of the CNIS. 2003. 126−131.

[14] Xu J, Fan J, Ammar MH, *et al*. Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme. Computer Networks, 2004,46(2):253−272.

[15] Bethencourt J, Franklin J, Vernon M. Mapping Internet sensors with probe response attacks. In: Proc. of the Usenix Security Symp. 2005. 193−208.

[16] Degraaf R, Aycock J, Jacobson M. Improved port knocking with strong authentication. In: Proc. of the Computer Security Applications Conf. 2005. 451−462.

[17] Mazurczyk W, Kotulski Z. New security and control protocol for VoIP based on steganography and digital watermarking. Annales UMCS Informatica, 2006,4(5):9−11.

[18] Mazurczyk W, Kotulski Z. New VoIP traffic security scheme with digital watermarking. In: Proc. of the 25th Int'l Conf. on Computer Safety, Reliability, and Security (SAFECOMP 2006). LNCS 4166, 2006. 170−181.

[19] Borders K, Prakash A. Web tap: Detecting covert Web traffic. In: Proc. of the ACM Conf. on Computer and Communications Security. 2004. 110−120.

[20] Feamster N, Balazinska M, Harfst G, *et al*. Infranet: Circumventing Web censorship and surveillance. In: Proc. of the Usenix Security Symp. 2008. 247−262.

[21] Bernstein DJ, Heninger N, LOU P, *et al*. Post-quantum RSA. IACR Cryptology ePrint Archive, 2017. 311−329.

[22] Beckman D, Chari AN, Devabhaktuni S, *et al*. Efficient networks for quantum factoring. Physical Review A, 1996,54(2): 1034−1063.

[23] Bernstein DJ, Breitner J, Genkin D, *et al*. Sliding right into disaster: Left-to-right sliding windows leak. In: Cryptographic Hardware and Embedded Systems. 2017. 555−576.

[24] Wendzel S, Keller J. Hidden and under control: A survey and outlook on covert channel-internal control protocols. Annals of Telecommunications—Annales Des Télécommunications, 2014,69:417−430.

[25] Hai JX, Ji ZZ. A lightweight identity authentication method by exploiting network covert channel. Peer-to-peer Networking and Applications, 2015,8(6):1038−1047.

[26] Lampson BW. A note on the confinement problem. Communications of the ACM, 1973,16(10):613−615.

[27] Millen J. 20 years of covert channel modeling and analysis. In: Proc. of the '99 IEEE Symp. on Security and Privacy. 1999. 113−114.

[28] Wang YJ, Wu JZ, Zeng HT, *et al*. Covert channel research. Ruan Jian Xue Bao/Journal of Software, 2010,21(9):2262−2288 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3880.htm [doi: 10. 3724/SP.J.1001.2010.03880]

[29] Epishkina AV, Kogos KG. Study of countermeasures against covert channels in IP networks. Automatic Control & Computer Sciences, 2015,49(8):785−789.

[30] Cai Z, Zhang Y. Entropy based taxonomy of network convert channels. In: Proc. of the Int'l Conf. on Power Electronics and Intelligent Transportation System. 2009. 451−455.

[31] Cabuk S, Brodley CE, Shields C. IP covert timing channels: Design and detection. In: Proc. of the ACM Conf. on Computer and Communications Security. 2004. 178−187.

[32] Murdoch SJ, Lewis S. Embedding covert channels into TCP/IP. In: Proc. of the Int'l Workshop on Information Hiding (Ih 2005). Barcelona, 2005. 247−261.

[33] Llamas D, Allison C, Miller A. Covert channels in Internet protocols: A survey. In: Proc. of the 6th Annual Postgraduate Symp. about the Convergence of Telecommunications, Networking and Broadcasting (PGNET). 2005. 1−5.

[34] Handel TG, Sandford MT. Hiding data in the OSI network model. In: Proc. of the Int'l Workshop on Information Hiding. LNCS 1174, 1996. 23−38.

[35] Petitcolas F, Anderson RJ, Kuhn MG. Information hiding—A survey. Proc. of the IEEE, 1999,87(7):1062−1078.

[36] Jones RH, Goodrich JK, Sabiston DC. Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model. Information Technology & Standardization, 2009,15(7):598−604.

[37] Zeng HT, Wang YJ, Zu W, *et al*. New definition of small message criterion and its application in transaction covert channel mitigating. Ruan Jian Xue Bao/Journal of Software, 2009,20(4):985−996 (in Chinese with English abstract). http://www.jos.org.cn/ 1000-9825/3246.htm [doi: 10.3724/SP.J.1001.2009.03246]

[38] Iglesias F, Annessi R, Zseby T. DAT detectors: Uncovering TCP/IP covert channels by descriptive analytics. Security & Communication Networks, 2016,9(15):3011−3029.

[39] Simmons GJ. The prisoners' problem and the subliminal channel. In: Advances in Cryptology. 1984. 51−67.

[40] U.S. Department of Defense. Trusted computer system evaluation criteria. In: Proc. of the DoD 5200.28-STD. 1985. 1−78.

[41] Nikoo A, Kahoo AR, Hassanpour H, *et al*. Using a time-frequency distribution to identify buried channels in reflection seismic data. Digital Signal Processing, 2016,54:54−63.

[42] Girling CG. Covert channels in LAN's. IEEE Trans. on Software Engineering, 1987,SE-13(2):292−296.

[43] Shen Y. Research on network protocol hidden channel detection and new construction scheme [Ph.D. Thesis]. Hefei: China University of Science and Technology, 2017 (in Chinese with English abstract).

[44] Houmansadr A, Borisov N. CoCo: Coding-based covert timing channels for network flows. In: Proc. of the Int'l Conf. on Information Hiding. 2011. 314−328.

[45] Wendzel S, Zander S, Fechner B, *et al*. Pattern-based survey and categorization of network covert channel techniques. ACM Computing Surveys, 2015,47(3):Article No.50.

[46] Iglesias F, Bernhardt V, Annessi R, *et al*. Decision tree rule induction for detecting covert timing channels in TCP/IP traffic. In: Proc. of the Int'l Cross-domain Conf. for Machine Learning and Knowledge Extraction. 2017. 105−122.

[47] Luo X, Chan EWW, Chang RKC. Cloak: A ten-fold way for reliable covert communications. In: Proc. of the European Conf. on Research in Computer Security. 2007. 283−298.

[48] Ahsan K, Kundur D. Practical data hiding in TCP/IP. In: Proc. of the Workshop on Multimedia Security at ACM Multimedia. 2002. 1−8.

[49] Nair AS, Kumar A, Sur A, *et al*. Length based network steganography using UDP protocol. In: Proc. of the IEEE Int'l Conf. on Communication Software and Networks. 2011. 726−730.

[50] Ji L, Jiang W, Dai B, *et al*. A novel covert channel based on length of messages. In: Proc. of the Int'l Symp. on Information Engineering and Electronic Commerce. 2009. 551−554.

[51] Lucena NB, Lewandowski G, Chapin SJ. Covert channels in IPv6. In: Proc. of the Int'l Workshop on Privacy Enhancing Technologies. 2005. 147−166.

[52] Zhang L, Liu G, Dai Y. Network packet length covert channel based on empirical distribution function. Journal of Networks, 2014,9(6):1440−1446.

[53] Fisk G, Fisk M, Papadopoulos C, *et al*. Eliminating steganography in Internet traffic with active wardens. In: Proc. of the Revised Papers from the Int'l Workshop on Information Hiding. 2002. 18−35.

[54] Trabelsi Z, El-sayed H, Frikha L, *et al*. Traceroute based IP channel for sending hidden short messages. In: Proc. of the Int'l Conf. on Security. 2006. 421−436.

[55] Shah G, Molina A, Blaze M. Keyboards and covert channels. In: Proc. of the Conf. on Usenix Security Symp. 2006. 59−75.

[56] Archibald R, Ghosal D. Design and analysis of a model-based covert timing channel for skype traffic. In: Proc. of the Communications and Network Security. 2015. 236−244.

[57] Zander S, Armitage G, Branch P. An empirical evaluation of IP time to live covert channels. In: Proc. of the IEEE Int'l Conf. on Networks. 2007. 42−47.

[58] Brodley CE, Spafford EH, Cabuk S. Network covert channels: Design, analysis, detection, and elimination. In: Proc. of the Dissertations & Theses—Gradworks. 2006.

[59] Archibald R, Ghosal D. Design and performance evaluation of a covert timing channel. Security & Communication Networks, 2016,9(8):755−770.

[60] Wu J, Wang Y, Ding L, *et al*. Improving performance of network covert timing channel through Huffman coding. Mathematical & Computer Modelling, 2012,55(1-2):69−79.

[61] Zander S, Armitage G. CCHEF-covert channels evaluation framework design and implementation. Technical Report, 080530A, Centre for Advanced Internet Architecture (CAIA), 2008.

[62] Zander S, Armitage G. Covert channels in the IP time to live field. In: Proc. of the Network Security Technology & Application. 2010. 1−6.

[63] Swinnen A, Strackx R, Philippaerts P, *et al*. ProtoLeaks: A reliable and protocol-independent network covert channel. In: Proc. of the Int'l Conf. on Information Systems Security. 2012. 119−133.

[64] Wolf M. Covert channels in LAN protocols. In: Proc. of the Local Area Network Security, Workshop Lansec'89. European Institute for System Security. 1989. 91−101.

[65] Mazurczyk W, Szczypiorski K. Evaluation of steganographic methods for oversized IP packets. Telecommunication Systems, 2012,49(2):207−217.

[66] Ji L, Liang H, Song Y, *et al*. A normal-traffic network covert channel. In: Proc. of the Int'l Conf. on Computational Intelligence and Security. 2010. 499−503.

[67] Schulz S, Varadharajan V, Sadeghi AR. The silence of the LANs: Efficient leakage resilience for IPsec VPNs. IEEE Trans. on Information Forensics & Security, 2014,9(2):221−232.

[68] Alex D, Simon C. Exploitation of data streams authorized by a network access control system for arbitrary data transfers: Tunneling and covert channels over the HTTP protocol. Technical Report, 2005. http://gray-world.net/projects/papers/covert_paper.txt

[69] Rios R, Onieva JA, Lopez J. HIDE_DHCP: Covert communications through network configuration messages. In: Proc. of the IFIP Int'l Information Security Conf. 2012. 162−173.

[70] Zou XG, Li Q, Sun SH, *et al*. The research on information hiding based on command sequence of FTP protocol. In: Proc. of the Int'l Conf. on Knowledge-based Intelligent Information and Engineering Systems. 2005. 1079−1085.

[71] Trabelsi Z, Jawhar I. Covert file transfer protocol based on the IP record route option. Journal of Information Assurance and Security, 2010,5:64−73.

[72] Mavani M, Ragha L. Covert channel in IPv6 destination option extension header. In: Proc. of the Int'l Conf. on Circuits. 2014. 219−224.

[73] Lucena NB, Pease J, Yadollahpour P, *et al*. Syntax and semantics-preserving application-layer protocol steganography. In: Proc. of the Int'l Workshop on Information Hiding. LNCS 3200, 2004. 164−179.

[74] Muchene DN, Luli K, Shue CA. Reporting insider threats via covert channels. IEEE Cs Security & Privacy Workshops, 2013, 42(6):68−71.

[75] Patuck R, Hernandezcastro J. Steganography using the extensible messaging and presence protocol (XMPP). arXiv:1310.0524, 2013. 360−366.

[76] Servetto SD, Vetterli M. Communication using phantoms: Covert channels in the Internet. In: Proc. of the IEEE Int'l Symp. on Information Theory. 2001. 229.

[77] Dittmann J, Lang A. WLAN steganography: A first practical review. In: Proc. of the Workshop on Multimedia and Security. 2006. 17−22.

[78] Mileva A, Panajotov B. Covert channels in TCP/IP protocol stack—Extended version. In: Proc. of the Versita. 2014. 45−66.

[79] Wendzel S, Zander S. Detecting protocol switching covert channels. In: Proc. of the Local Computer Networks. 2013. 280−283.

[80] Wendzel S, Kahler B, Rist T. Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet. In: Proc. of the IEEE Int'l Conf. on Green Computing and Communications. 2013. 731−736.

[81] Ji L, Fan Y, Ma C. Covert channel for local area network. In: Proc. of the IEEE Int'l Conf. on Wireless Communications, Networking and Information Security. 2010. 316−319.

[82] Giffin J, Greenstadt R, Litwack P, *et al*. Covert messaging through TCP timestamps. In: Proc. of the Int'l Conf. on Privacy Enhancing Technologies. 2002. 194−208.

[83] Stødle D. Ping tunnel—For those times when everything else is blocked. http://www.mit.edu/afs.new/sipb/user/golem/tmp/ptunnel-0.61.orig/web/

[84] Jankowski B, Mazurczyk W, Szczypiorski K. Information hiding using improper frame padding. In: Proc. of the Telecommunications Network Strategy and Planning Symp. 2010. 1−6.

[85] Szczypiorski K, Margasinski I, Mazurczyk W. Steganographic routing in multi agent system environment. In: Proc. of the Computer Science. 2009. 1−9.

[86] Backs P, Wendzel S, Keller J. Dynamic routing in covert channel overlays based on control protocols. In: Proc. of the 2012 Int'l Conf. for Internet Technology and Secured Transactions. 2012. 32−39.

[87] Kaur J, Wendzel S, Eissa O, Tonejc J, Meier M. Covert channel-internal control protocols: Attacks and defense. Security and Communication Networks, 2016,9(15):2986−2997.

[88] Wendzel S. Novel approaches for network covert storage channels. In: Proc. of the FernUniversität in Hagen. 2013.

[89] Wendzel S, Keller J. Systematic engineering of control protocols for covert channels. In: Proc. of the IFIP Int'l Conf. on Communications and Multimedia Security. 2012. 131−144.

[90] Ray B, Mishra S. A protocol for building secure and reliable covert channel. In: Proc. of the 6th Conf. on Privacy, Security and Trust (PST 2008). 2008. 246−253.

[91] Jacobson V. Compressing TCP/IP headers for low-speed serial links. Request for Comments, 1990,2(2):37−42.

[92] Szczypiorski K, Mazurczyk W, Cabaj K. TrustMAS: Trusted communication platform for multi-agent systems. In: Proc. of the Otm 2008 Confederated Int'l Conf., Coopis, Doa, Gada, Is, and Odbase. 2008. 1019−1035.

[93] Yarochkin FV, Dai SY, lin CH, *et al*. Towards adaptive covert communication system. In: Proc. of the IEEE Pacific Rim Int'l Symp. on Dependable Computing. 2008. 153−159.

[94] Wendzel S, Keller J. Low-attention forwarding for mobile network covert channels. In: Proc. of the 12th Communications and Multimedia Security (CMS). 2011. 122−133.

[95] El-Atawy A, Al-Shaer E. Building covert channels over the packet reordering phenomenon. In: Proc. of the Int'l Conf. on Computer Communications. 2009. 2186−2194.

[96] Herzberg A, Shulman H. Limiting MitM to MitE covert-channels. In: Proc. of the Int'l Conf. on Availability, Reliability and Security. 2013. 236−241.

[97] Mazurczyk W, Smolarczyk M, Szczypiorski K. Retransmission steganography and its detection. Soft Computing, 2011,15(3): 505−515.

[98] Gianvecchio S, Wang H, Wijesekera D, *et al*. Model-based covert timing channels: automated modeling and evasion. In: Proc. of the Int'l Symp. on Recent Advances in Intrusion Detection. 2008. 211−230.

[99] Liu G, Zhai J, Dai Y. Network covert timing channel with distribution matching. Telecommunication Systems, 2012,49(2): 199−205.

[100] Liu Y, Ghosal D, Armknecht F, *et al*. Robust and undetectable steganographic timing channels for i.i.d. traffic. In: Proc. of the Int'l Conf. on Information Hiding. 2010. 193−207.

[101] Liu Y, Ghosal D, Armknecht F, *et al*. Hide and seek in time—Robust covert timing channels. In: Proc. of the European Conf. on Research in Computer Security. 2009. 120−135.

[102] Sellke SH, Wang CC, Bagchi S, *et al*. TCP/IP timing channels: Theory to implementation. In: Proc. of the INFOCOM. 2007. 2204−2212.

[103] Archibald R, Ghosal D. A covert timing channel based on fountain codes. In: Proc. of the IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. 2012. 970−977.

[104] Wang P. A hidden channel method based on TCP timestamp option [Ph.D. Thesis]. Nanjing: Nanjing University of Science and Technology, 2015 (in Chinese with English abstract)

[105] Wang J, Gao N, Lin JQ, *et al*. Research on network covert timing channel. Netinfo Security, 2012,12(8):160−163 (in Chinese with English abstract).

[106] Walls RJ, Kothari K, Wright M. Liquid: A detection-resistant covert timing channel based on IPD shaping. Computer Networks, 2011,55(6):1217−1228.

[107] Handley M, Paxson V, Kreibich C. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics. In: Proc. of the Conf. on Usenix Security Symp. 2001. 1−17.

[108] Lewandowski G, Lucena NB, Chapin SJ. Analyzing network-aware active wardens in IPv6. In: Proc. of the Int'l Workshop on Information Hiding (IH 2006). 2006. 58−77.

[109] Proctor NE, Neumann PG. Architectural implications of covert channels. In: Proc. of the 15th National Computer Security Conf. 1992. 28−43.

[110] Giles J, Hajek B. An information-theoretic and game-theoretic study of timing channels. IEEE Trans. on Information Theory, 2002,48(9):2455−2477.

[111] Wendzel S, Keller J. Preventing protocol switching covert channels. Int'l Journal on Advances in Security, 2012,5(3):81−93.

[112] Kang MH, Moskowitz IS. A pump for rapid, reliable, secure communication. In: Proc. of the Computer and Communications Security. 1993. 119−129.

[113] Kang MH, Moskowitz IS, Chincheck S. The pump: A decade of covert fun. In: Proc. of the Annual Computer Security Applications Conf. 2005. 352−360.

[114] Sohn T, Seo JT, Moon J. A study on the covert channel detection of TCP/IP header using support vector machine. In: Proc. of the Int'l Conf. on Information and Communications Security. 2003. 313−324.

[115] Sohn T, Moon J, Lee S, *et al*. Covert channel detection in the ICMP payload using support vector machine. In: Proc. of the Int'l Symp. on Computer and Information Sciences. LNCS 2869, 2003. 828−835.

[116] Shon T, Noh T, Moon J. Support vector machine based ICMP covert channel attack detection. In: Proc. of the 2nd Int'l Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2003). St. Petersburg, 2003. 461−464.

[117] Guang XF, Qing BL, Zhi FC, Guang YZ, Juan JG. Network storage covert channel detection based on data joint analysis. In: Proc. of the Int'l Conf. on Cloud Computing, 2018. 346−357.

[118] Yao S, Liu SH, Xiao RL, Wei Y. A novel comprehensive steganalysis of transmission control protocol/Internet protocol covert channels based on protocol behaviors and support vector machine. Security and Communication Networks, 2015,8(7):1279−1290.

[119] Krzysztof C, Wojciech M, Piotr N, Piotr Z. Towards distributed network covert channels detection using data mining-based approach. In: Proc. of the ARES. 2018. 12:1−12:10

[120] Archibald R, Ghosal D. A comparative analysis of detection metrics for covert timing channels. Computers & Security, 2014, 45(8):284−292.

[121] Li GH. Research and implementation of network covert communication [Ph.D. Thesis]. Guilin: Guilin University of Electronic Technology, 2015 (in Chinese with English abstract).

[122] Gianvecchio S, Wang H. Detecting covert timing channels: an entropy-based approach. In: Proc. of the ACM Conf. on Computer & Communications Security. 2007. 307−−316.

[123] Peng P, Ning P, Reeves DS. On the secrecy of timing-based active watermarking trace-back techniques. In: Proc. of the IEEE Symp. on Security and Privacy. 2006. 334−349.

[124] Fahimeh R, Michael H, Hamid S. Towards a reliable detection of covert timing channels over real-time network traffic. IEEE Trans. on Dependable and Secure Computing, 2017,14(3):249−264.

[125] Gianvecchio S, Wang H. An entropy-based approach to detecting covert timing channels. In: Proc. of the ACM Conf. on Computer and Communications Security (CCS 2007). Alexandria, 2011. 307−316.

[126] Shresth PL, Hempel M, Rezaei F, *et al*. A support vector machine-based framework for detection of covert timing channels. IEEE Trans. on Dependable & Secure Computing, 2016,13(2):274−283.

[127] Zseby T. Are network covert timing channels statistical anomalies? In: Proc. of the Int'l Conf. on Availability, Reliability and Security. 2017. 81−89.

[128] Iglesias F, Annessi R, Zseby T. Analytic study of features for the detection of covert timing channels in network traffic. Journal of Cyber Security and Mobility, 2018,6(3):225−270.

[129] Shrestha PL, Hempel M, Rezaei F, *et al*. Leveraging statistical feature points for generalized detection of covert timing channels. In: Proc. of the IEEE Military Communications Conf. 2014. 7−11.

[130] Ameri A, Johnson D. Covert channel over network time protocol. In: Int'l Conf. on Cryptography Security and Privacy. 2017. 62–65.

[131] Lemay A, Knight A. A timing-based covert channel for SCADA networks. In: Int'l Conf. on Cyber Conflict. 2017. 8–15.

[132] Liang C, Tan YA, Zhang XS, Wang XM, Zheng J, Zhang QX. Building packet length covert channel over mobile VoIP traffics. Journal of Network and Computer Applications, 2018,118:144–153.

[133] Peng CC, Wei WL, Guang JL, Xiao PJ, Jiang TZ. A wireless covert channel based on constellation shaping modulation. Security and Communication Networks, 2018,2018:Article ID 1214681.

[134] Guang LX, Wei Y, Liu SH. Hybrid covert channel in LTE-A: Modeling and analysis. Journal of Network and Computer Applications, 2018,111:117–126.

[135] Samira T, Mojtaba M, Neda M. A dynamic timing-storage covert channel in vehicular ad hoc networks. Telecommunication Systems, 2018,69(4):415–429.

[136] Daniel S, Jörg K, Tobias E. Towards covert channels in cloud environments: A study of implementations in virtual networks. In: Proc. of the IWDW. 2017. 248–262.

**附中文参考文献:**

[11] 娄嘉鹏,张萌,付鹏,等.一种基于 TCP 协议的网络隐蔽传输方案设计.信息网络安全,2016,16(1):34–39.

[28] 王永吉,吴敬征,曾海涛,等.隐蔽信道研究.软件学报,2010,21(9):2262–2288. http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]

[37] 曾海涛,王永吉,祖伟,等.短消息指标新定义及在事务信道限制中的应用.软件学报,2009,20(4):985–996. http://www.jos.org.cn/1000-9825/3246.htm [doi: 10.3724/SP.J.1001.2009.03246]

[43] 沈瑶.网络协议隐信道检测与新型构建方案研究[博士学位论文].合肥:中国科学技术大学,2017.

[104] 王鹏.一种基于 TCP 时间戳选项的隐蔽信道方法[博士学位论文].南京:南京理工大学,2015.

[105] 汪婧,高能,林璟锵,等.网络时间隐蔽信道研究.信息网络安全,2012,12(8):160–163.

[121] 李光辉.网络隐蔽通信的研究与实现[博士学位论文].桂林电子科技大学,2015.

**李彦峰**(1984－),男,山东济宁人,博士生,工程师,主要研究领域为网络隐蔽信道构建与分析.

**刘雪花**(1986－),女,博士生,工程师,主要研究领域为数字取证,系统安全与可信计算.

**丁丽萍**(1965－),女,博士,研究员,博士生导师,主要研究领域为数字取证,系统安全,可信计算.

**关贝**(1986－),男,博士,助理研究员,主要研究领域为人工智能方法和大数据分析方法,网络安全分析技术,操作系统虚拟化技术和安全操作系统.

**吴敬征**(1982－),男,博士,副研究员,CCF 专业会员,主要研究领域为系统安全,漏洞挖掘,移动安全.

**王永吉**(1962－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为实时系统,网络优化,智能软件工程,优化理论,信息系统安全,控制理论.

**崔强**(1985－),男,博士,主要研究领域为机器学习,推荐算法,众测.