软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(8):2470−2490 [doi: 10.13328/j.cnki.jos.005859]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

网络隐蔽信道关键技术研究综述*

李彦峰[1,2], 丁丽萍[1,3], 吴敬征[4,5], 崔 强[6], 刘雪花[1,2], 关 贝[4,7], 王永吉[4,7]

[1](中国科学院 软件研究所 并行软件与计算科学实验室,北京 100190)

[2](中国科学院大学,北京 100049)

[3](广州中国科学院 软件应用技术研究所 电子数据取证实验室,广东 广州 511458)

[4](计算机科学国家重点实验室(中国科学院 软件研究所),北京 100190)

[5](中国科学院 软件研究所 智能软件研究中心,北京 100190)

[6](中国科学院 软件研究所 互联网软件技术实验室,北京 100190)

[7](中国科学院 软件研究所 协同创新中心,北京 100190)

通讯作者: 丁丽萍, E-mail: dingliping@gz.iscas.ac.cn

摘 要: 网络隐蔽信道是在网络环境下违反通信限制规则进行隐蔽信息传输的信息通道,为网络信息安全带来了新的挑战,也为数据传输的安全性和隐私性带来了新的研究方向.首先介绍了网络隐蔽信道的定义、分类、能力维度等基本概念;进而从码元设计、信息编码和信道优化这 3 个方面归纳分析了存储型和时间型两类网络隐蔽信道的构建技术,从隐蔽性、鲁棒性和传输效率这 3 个方面总结了网络隐蔽信道评估方法,从消除、限制、检测这 3 个方面梳理了网络隐蔽信道的对抗技术;最后,对未来的研究方向进行了展望.

关键词: 网络隐蔽信道;信息隐藏;网络隐蔽信道构建;网络隐蔽信道对抗

中图法分类号: TP393

中文引用格式: 李彦峰,丁丽萍,吴敬征,崔强,刘雪花,关贝,王永吉.网络隐蔽信道关键技术研究综述.软件学报,2019,30(8):2470−2490. http://www.jos.org.cn/1000-9825/5859.htm

英文引用格式: Li YF, Ding LP, Wu JZ, Cui Q, Liu XH, Guan B, Wang YJ. Survey on key issues in networks covert channel. Ruan Jian Xue Bao/Journal of Software, 2019,30(8):2470−2490 (in Chinese). http://www.jos.org.cn/1000-9825/5859.htm

Survey on Key Issues in Networks Covert Channel

LI Yan-Feng[1,2], DING Li-Ping[1,3], WU Jing-Zheng[4,5], CUI Qiang[6], LIU Xue-Hua[1,2], GUAN Bei[4,7], WANG Yong-Ji[4,7]

[1](Laboratory of Parallel Software and Computational Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[2](University of Chinese Academy of Sciences, Beijing 100049, China)

[3](Digital Forensics Laboratory, Institute of Software Application Technology, Guangzhou & Chinese Academy of Sciences (GZIS), Guangzhou 511458, China)

[4](State Key Laboratory of Computer Science (Institute of Software), Chinese Academy of Sciences, Beijing 100190, China)

* 基金项目: 国家重点研发计划(2016QY01W0200); 国家自然科学基金(61772507); 广东省省级科技计划(2017B050506002); 羊城创新创业领军人才支持计划(2016008); 广州市科技计划(201802020015)

Foundation item: National Key Research and Development Program of China (2016QY01W0200); National Natural Science Foundation of China (61772507); Science and Technology Planning Project of Guangdong Province (2017B050506002); Scheme of Guangzhou for Leading Talents in Innovation and Entrepreneurship (2016008); Science and Technology Planning Project of Guangzhou Municipality (201802020015)

收稿时间: 2018-12-14; 修改时间: 2019-03-21; 采用时间: 2019-04-25; jos 在线出版时间: 2019-05-22

CNKI 网络优先出版: 2019-05-22 15:26:20, http://kns.cnki.net/kcms/detail/11.2560.TP.20190522.1525.013.html

[5](Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[6](Laboratory for Internet Software Technologies, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[7](Collaborative Innovation Center, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Network covert channel is the information channel that carries on covert information transmission in violation of the communication restriction rules under the network environment. It brings new challenges to the network information security and provides new research point for ensuring the security and privacy of data transmission. Firstly, the basic concepts of network covert channel are introduced, such as definition, classification, capability dimension. Then, network covert storage channel and network covert timing channel construction technologies are sorted out from three aspects of symbol design, information coding and channel optimization. Then the evaluation methods of network covert channel are summarized from three aspects of covertness, robustness, and transmission efficiency. Furthermore, the countermeasure technology of network covert channel is sorted from three aspects of elimination, restriction, and detection. Finally, some future research directions are prospected.

Key words: network covert channel; information hiding; network covert channel construction; network covert channel countermeasure

随着网络技术的发展,网络信息传输安全越来越受到重视.一方面,需要检测和阻断通过网络传输的恶意信息(例如网络攻击、病毒、木马程序等);另一方面,需要保障通过网络传输的正常通信信息(例如商业信息、个人隐私信息等)的安全性和隐私性.网络隐蔽信道因其隐蔽通信的特性,越来越多地应用在网络信息传输安全的这两个方面.

网络隐蔽信道是网络环境下违反通信限制规则进行隐蔽信息传输的通信信道,使用网络信息载体(例如网络协议、网络数据包等)的载体特征(例如协议字段、时间特征等)的特征模式(例如值调制模式、时间间隔模式等)进行隐蔽信息传输,防止信息被发现.

在恶意信息传输方面,由于网络通信的审查随着网络安全技术的发展越来越严格,传统基于正常通信协议的传输方式的网络恶意行为往往易于发现和控制,因此,攻击者会利用网络隐蔽信道绕过网络审查机制隐蔽传输信息的特点实施网络恶意行为,例如蠕虫病毒传播[1,2]、秘密构建“僵尸网络”[3,4]、发起分布式拒绝服务攻击(distributed denial of service,简称 DDoS)[5−7]、隐蔽地泄露数据或敏感信息[8,9]、被木马程序利用进行隐蔽通信[10,11]、破坏匿名网络的匿名性[12−15]、被攻击者用来发送认证信息[12,16−18]等.

在保障网络通信的安全性和隐私性[19,20]方面,由于计算能力的提升和新的计算架构的发展(例如并行计算、分布式计算等),以及针对加密算法和应用的攻击[21−23],传统的保护数据传输安全性和隐私性的加密技术面临越来越大的挑战.加密技术的目的是通过使信息变得不可读从而防止第三方读取数据,网络隐蔽信道技术的目的是防止信息本身被发现[24],作为新的通信方式和通信策略,可以对传统加密通信进行有力的补充,例如进行军用通讯[24]、记者用网络隐蔽信道绕过舆论审查发布自由言论[12]、安全身份认证[25]等.由于网络隐蔽信道在网络信息传输安全性的两方面应用,对网络隐蔽信道研究非常必要.

目前,对网络隐蔽信道的研究和综述大多成文较早,且关注于一项具体的技术方面[12,26−34],缺乏从全局把握整个网络隐蔽信道领域的研究,对于网络隐蔽信道构建方法多关注技术细节而缺少体系架构,从而无法对网络隐蔽信道技术向系统化、规模化发展提供支持.本文尝试从构建、评估、对抗这 3 个方面对网络隐蔽信道相关研究进行全面的归纳和分析.第 1 节介绍了网络隐蔽信道的定义、分类、能力维度等基本概念.第 2 节从码元设计、信息编码和信道优化这 3 个方面归纳分析了存储型和时间型两类网络隐蔽信道构建技术.第 3 节从隐蔽性、鲁棒性和传输效率这 3 个方面总结了网络隐蔽信道评估方法.第 4 节从消除、限制、检测这 3 个方面梳理了网络隐蔽信道的对抗技术.最后总结全文,并对未来研究方向进行了展望.

1 网络隐蔽信道基本概念

1.1 网络隐蔽信道定义

网络隐蔽信道是隐蔽信道的一个分支,属于信息隐藏技术(information hiding)[35],以使数据难以被察觉和发现为主要目的[2].隐蔽信道的概念最初是由 Lampson 等人于 1973 年提出的,定义为本意不是被设计用来传输信

息的、破坏通信安全策略的通信信道[26−28].国际标准化组织(ISO)发布的《信息技术安全评估通用准则》(ISO/IEC 15408,简称 CC 标准)[36]对隐蔽信道的定义是,允许进程以违背安全策略的方式传输信息的通信通道[28,37].Iglesias 等人[38]将隐蔽信道定义为寄生在正常通信通道中,绕过安全防护隐蔽传输信息的通信通道.使用非信息传输通道、违反安全策略、寄生于正常通信是隐蔽信道的主要特点.网络隐蔽信道作为隐蔽信道的一个分支,同样具有这些特点.

随着计算机网络的发展,隐蔽信道的研究也扩展到了网络环境中.网络隐蔽信道定义为:在网络环境下,违反通信限制规则进行隐蔽信息传输的通信信道[24,27],使用网络信息载体(例如网络协议、网络数据包等)的载体特征(例如协议字段、时间特征等)的特征模式(例如值调制模式、时间间隔模式等)进行隐蔽信息传输[24].网络隐写术是与网络隐蔽信道相近的技术,网络隐写术指通过人能够理解的数据载体进行信息传输(例如文字、音频、视频等)[24],而网络隐蔽信道通过机器“理解”的协议载体进行信息传输(例如网络协议头字段),二者使用的网络资源载体不同,因此使用网络信息数据部分进行隐藏信息传输的方法不在网络隐蔽信道研究范围内.

囚徒模型是隐蔽信道的经典对抗模型[39]:两个囚徒 Alice 和 Bob 被关进监狱并且计划逃跑,为了协商逃跑的计划,他们需要进行通信.但是看守 Wendy 监视着他们之间所有的通信信息,一旦发现任何可疑信息,就会断绝他们与外界的通信.因此,Alice 和 Bob 必须使隐藏信息包含在表面上看起来无害和正常的信息之中,使 Wendy 无法发现.不同计算环境下的隐蔽信道都遵循囚徒模型[40−43].Handel 等人[34]将隐蔽信道的囚徒模型进行了扩展,将这个场景引入到了计算机网络通信中:Alice 和 Bob 使用两台联网的计算机进行通信,在看起来正常的公开信道(overt channel)中包含了隐蔽信道(covert channel),Alice 和 Bob 共享一个秘密信息,用来编码、解码、解密或认证这些隐藏信息.Wendy 对网络进行管理并监视通过的流量,对隐蔽通信进行消除或限制.

囚徒模型如图 1 所示.

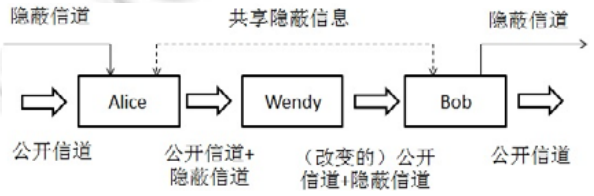

Fig.1 Prisoner problem

图 1 囚徒问题

1.2 网络隐蔽信道分类

不同的研究者从不同的角度对网络隐蔽信道进行了分类,从不同的角度归纳了隐蔽信道的特征和差异,包括存储型/时间型网络隐蔽信道分类、基于 OSI 通信模型的分类、基于构建技术模式的分类和基于信道特征的分类.

Llamas 等人[33]依据传统隐蔽信道的分类方法将网络隐蔽信道分为存储型网络隐蔽信道和时间型网络隐蔽信道两大类:存储型网络隐蔽信道使用协议数据单元内部的信息传输隐蔽数据(例如网络协议头),而时间型网络隐蔽信道使用协议数据单元的时间特性(例如数据包间隔)传输隐蔽数据.存储型/时间型是网络隐蔽信道最基本的分类方法,区分了两类构建机制截然不同的隐蔽信道,大部分研究都接收了这个分类,并在这个分类的基础上开展研究[44−47].

Handel 等人[34]基于开放系统互连参考模型(open system interconnect,简称 OSI)对网络隐蔽信道进行了分类,对应 OSI 通信模型的 7 层,将网络隐蔽信道分为 7 类,并对每一层可用来传递隐蔽数据的资源和方法做了分析.基于 OSI 通信模型的分类对网络隐蔽信道的载体进行划分,可以更加直观地了解网络隐蔽信道使用的网络资源.

Wendzel 等人[45]使用模式语言标记语言(pattern language markup language,简称 PLML)方法将 1987 年~2013 年的 109 个隐蔽信道构建技术分为 11 个不同的模式,并且大部分(69.7%)隐蔽信道构建技术都可以归在 4

个类别中.基于模式的分类在存储型/时间型网络隐蔽信道分类方法基础上进行了细化,通过构建技术将网络隐蔽信道进一步划分,打破了使用网络载体类型的限制,从形式上对网络隐蔽信道隐藏信息的技术方法进行了归纳和总结,使网络隐蔽信道的构建可以更方便地从一种网络载体迁移到另一种网络载体中.

除了以上主要分类外,还有一些基于网络隐蔽信道不同特征的分类方法.Iglesias 等人[38]以检测视角对利用传输控制协议/互联协议(transmission control protocol/internet protocol,简称 TCP/IP)的网络隐蔽信道的编码特征分为了 5 类,包括使用一个或多个协议头字段的值与隐蔽信息符号进行对应[48−50]的值与符号对应方式、使用协议字段值的范围作为隐蔽信息符号[51,52]的值的范围作为符号方式、使用一个数据包发送隐蔽信息并用特殊的标识字段对隐蔽信道的数据包进行标识[53,54]的容器字段方式、利用网络通信的时间属性隐藏信息[55,56]的时间信道方式、把隐蔽信息隐藏在一系列数据包中的变化中[51,57]的派生方式.Cai 等人[30]提出了基于熵特征的网络隐蔽信道分类,由于隐蔽信道受限于所使用的公开资源,而公开资源可使用熵进行描述,因此可以使用熵对隐蔽信道进行分类,并可以根据隐蔽信道,利用公开资源的方法进行进一步细分.Brodley 等人[58]基于噪声特征将网络隐蔽信道分为有噪声信道和无噪声信道,其中,有躁声信道和无躁声信道是通过信道是否包含正常噪声和通信噪声进行区分的,有噪声信道会包含网络共享资源自身产生的噪声,从而影响信息传递的准确性和信道容量.这些机遇不同特征的分类方法是对以上 3 个主要分类方法的补充,从不同侧面描述了网络隐蔽信道的特点.

1.3 网络隐蔽信道能力维度

网络隐蔽信道的能力维度是网络隐蔽信道所应具备的能力方面.Archibald 等人[59]认为,时间隐蔽信道应具有 4 个方面的特征:抗检测性(non-detectability)、抗暴露性(non-disclosure)、抗干扰性(non-disruptability)、吞吐量(throughput).其中:抗检测性指隐蔽信道无法被监测者发现;抗暴露性指即使信道被检测到隐蔽信息也无法被解码;抗干扰性指信道抵抗网络环境变化的能力,例如网络延迟、抖动、丢包等,在类似情境下能够正确传递隐蔽信息的能力;吞吐量指单位时间内传输的最大数据量.其他研究者大都以类似的能力维度为目标设计和构建网络隐蔽信道[60−62].归纳和总结相关研究,隐蔽性、鲁棒性和传输效率是网络隐蔽信道最常用的 3 个能力维度:隐蔽性指网络隐蔽信道不被发现的能力,鲁棒性指网络隐蔽信道抗干扰和准确传输数据的能力,传输效率用来指网络隐蔽信道单位时间内传输数据量的能力.网络隐蔽信道的能力维度为网络隐蔽信道的构建、评估和对抗提供了目标和方向.

2 网络隐蔽信道构建

2.1 网络隐蔽信道构建的技术环节

网络隐蔽信道的本质是信息传输,从技术环节上可分为码元设计、信息编码和信道优化 3 个方面.

- 码元是承载信息量的基本信号单位,网络隐蔽信道码元设计指选取具有隐蔽特性的网络信息载体、载体特征及特征模式作为隐蔽信息的码元携带隐蔽信息的方法,是网络隐蔽信道构建最核心的部分.其中,网络隐蔽信道的信息载体包括网络协议、网络数据包等,载体特征包括协议字段、时间属性等,特征模式包括值调制模式、时间间隔模式等.简而言之,网络隐蔽信道的码元是网络信息载体、载体特征、特征模式的组合.
- 信息编码指信息从一种形式或格式转换为另一种形式或格式的过程,网络隐蔽信道信息编码指使用网络隐蔽信道码元进行编码,从而生成隐蔽信息的过程,往往用来提升网络隐蔽信道的鲁棒性和传输效率.
- 信道优化指在码元设计和信息编码生成隐蔽信息的基础上,通过其他技术手段提升隐蔽信道的能力(隐蔽性、鲁棒性或传输效率),例如为网络隐蔽信道提供额外功能.

2.2 存储型/时间型网络隐蔽信道特性点对比

网络隐蔽信道从构建机制上可分为存储型和时间型网络隐蔽信道两类,这两种隐蔽信道有着各自的优缺点.Wendzel 等人[45]和 Swinnen 等人[63]认为:存储型网络信道容量较大,可以利用载体信道的可靠性传输(如

TCP/IP 协议)受网络条件的影响较小,但是易于被基于内容的检测方法进行针对性检测[53];而时间型网络隐蔽信道较难以检测,但是信道容量小而且发送者和接受者往往需要同步,并且很容易受网络条件的变化(如延迟、丢包、噪音)的影响.综上所述,存储型隐蔽信道的特点是隐蔽性较低、鲁棒性较高、传输效率较高,时间型隐蔽信道的特点是隐蔽性较高、鲁棒性较低、传输效率较低.因此在构建网络隐蔽信道时,应根据网络隐蔽信道类型特点进行有针对性的设计.

- 码元设计方面,存储型网络隐蔽信道使用的网络载体一般为网络协议,利用的载体属性为协议字段,类型多样的网络协议为存储型网络隐蔽信道设计提供了充分的信息载体空间和设计素材,因此,网络隐蔽信道的传输效率较高,种类也较多;但由于网络协议的类型和和属性有限,易于被针对,因此,存储型网络隐蔽信道需要其他手段对隐蔽性方面进行补充.而时间隐蔽信道使用的信道载体一般为网络数据包,利用的载体属性为时间特性,可选择的方法较少;另一方面,由于网络数据包的时间特性不易检测,为时间型网络隐蔽信道提供了相对充分的隐蔽性.
- 信息编码方面,存储型网络隐蔽信道和时间型网络隐蔽信道都会利用编码方式提高传输效率,而时间型网络隐蔽信道在鲁棒性方面更倚重信息编码.Wendzel 等人[45]认为:由于存储型隐蔽信道可以利用公开信道的可靠性传输机制(例如 TCP 协议),因此信息编码主要用来提升网络隐蔽信道的传输效率.时间型隐蔽信道的传输依赖于数据帧、数据包或信息的时间属性,很容易受噪声影响,而且传输效率不高,因此在编码方面会着重提升信道的鲁棒性和传输效率.
- 信道优化方面,大量的网络协议和属性可以给存储型网络隐蔽信道优化带来充分的空间提供新的功能,从而弥补存储型网络隐蔽信道易被针对的特点.时间型网络隐蔽信道并没有充分的载体提供额外的优化功能,但是可以通过改进时间特性的使用进一步提升隐蔽性.

存储型/时间型网络隐蔽信道构建技术环节与网络隐蔽信道能力维度的匹配见表 1.

Table 1 Network storage/timing covert channel construction technical process and capability dimension

表 1 存储型/时间型网络隐蔽信道构建技术环节与能力维度

技术环节	存储型网络隐蔽信道	时间型网络隐蔽信道
码元设计	隐蔽性,鲁棒性,通信效率	隐蔽性
信息编码	通信效率	鲁棒性,通信效率
信道优化	隐蔽性,鲁棒性,通信效率	隐蔽性,通信效率

2.3 存储型网络隐蔽信道构建

2.3.1 码元设计

丰富的网络协议和网络协议的特性,为存储型网络隐蔽信道的构建提供了大量的素材.Wendzel 等人[63]按照网络隐蔽信道构建技术将存储型隐蔽信道构建技术分为 7 个模式.

(1) 调制大小模式:使用协议头元素或 PDU 的大小进行隐蔽信息编码,例如调制 LAN 帧的数据块大小编码[42]、调制 IEEE 802.3 帧的填充字段大小填充编码[64]、调制 IP 分片的大小编码[32,65]、使用网络数据包的信息长度编码[66]、使用 IPsec 信息的长度编码[67]、使用 VPN 的 MTU 的大小编码[67]等.

(2) 序列模式:通过改变协议头元素或 PDU 元素的序列传递隐蔽信息,例如改变 HTTP 协议头字段序列[68]、改变 DHCP 选项序列[69]、改变 FTP 协议命令序列[70]等.序列模式包含两个子类:第 1 个子类被称为位置模式,通过改变协议头或 PDU 元素的位置对隐藏信息进行编码,例如改变 DHCP 选项列表中某一选项的位置[69]等;第 2 个子类被称为元素数量模式,例如改变 DHCP 数据包中选项的数量[69]、改变 IP 数据包分片的数量[65]等.

(3) 增加冗余模式:在协议头或 PDU 内增加新的空间用于隐藏数据,如构建在选项中嵌入隐藏数据 IPv4 数据包[71]、增加新的 IPv6 目的地址选项嵌入隐藏数据[72]、通过增加额外的字段扩展 HTTP 协议头[68]、修改 IPv4 协议头的 record route option 的指针和长度的值构造新的空间隐藏数据[71]、增加随机位加密 SSH 信息[73]、SMTP 数据包头增加额外的字段、在 DHCP 的 chaddr 字段的未使用位中隐

藏数据[69]、在 IP 数据包中封小于以太帧的空间[74]、XMPP 的 leading/trailing 选项的空白空间[75]等.

(4) PDU 错误/丢失模式:构建包含隐藏数据的错误的 PDU,或主动利用数据包的丢失进行信息隐藏,例如在 broadcast erasure channels 中构建错误信息[76]、在 IEEE 802.11 中构建错误帧[77]、利用 VPN 丢包传递隐藏信息[65]等.

(5) 随机值模式:通过在数据包头元素中嵌入的随机值传递隐藏数据,例如利用 IPv4 协议的 Identifier 字段[78]、TCP 连接的 ISN 序列号[78]、DHCP 的 xid 字段[69]、SSH 协议的 MAC 字段[73]等.

(6) 值调制模式:从 n 个值中挑选一个能够用来编码隐藏信息的头元素值,例如在本地网络中的 n 个地址中挑选一个发送数据帧[42]、利用 n 个可能的 IP 头的 TTL 值进行编码[62]、通过 n 个 IPv6 数据包头的 Hop Limit 值进行编码[51]、通过从 n 个应用层协议中选择一个协议发送数据包编码[79]、通过向 n 个应用层协议端口选择一个端口发送数据包编码在 BACnet 协议中从 n 个信息类型中选择一个信息类型编码[80]、通过目标 IP 的 ARP 信息编码[81]、修改 XMPP 协议的“type”或“xml:lang”属性[75]等.值调制模式又包含两个子类:一个子类被称为 CASE(common application service element)模式,利用头元素中的 CASE 隐藏信息,例如修改 HTTP 头文件中的 CASE[68]、修改 XMPP 协议中“type”或“id”属性的 CASE[75];另一个子类被称为 LSB(least significant bit,最低有效位)模式,使用头文件中的 LSB 编码隐藏数据,例如通过 IPv4 时间戳选项的奇偶时间编码[34]、修改 TCP 数据包时间戳选项的低阶位[82]、使用 DHCP 协议头 secs 字段的 LSB[69]、使用 IPv6 数据包 Limit 字段的 LSB[51]、使用 XMPP 协议“id”属性的 LSB[68]等.

(7) 保留/未使元素模式:使用协议头或数据包的保留或未使用元素(例如保留字段、保留位等)进行隐藏数据的编码,例如利用 IEEE 802.5 或数据链路层数据帧的保留字段[34]、使用 IPv4 协议的未使用字段[34]、使用 IPv6 协议头的保留字或未用字段[51]、使用 TCP 协议头的未使用位[34]、使用 ICMP 协议的 echo payload[83]、使用 IEEE802.3 的填充字段[84]、使用 BACnet 协议头的未用字段[80]、DHCP 协议的 sname 和 file 字段的终止标识位[69]、IPSec 协议的 DS 字段[65]、IPSec 协议的 ECN 字段[65]等.

存储型网络隐蔽信道选择的信息载体、载体特征和特征模式会对鲁棒性和通信效率产生影响.不同的载体协议的特性不同:有的通信协议可以提供可靠传输(例如 TCP 协议),因此具有较高的鲁棒性;如果选择非可靠协议(例如 UDP 协议),则无法保证鲁棒性.另外,不同协议的载体特征和模式包含的信息量不同(例如保留/未使用元素模式选取不同字段的值范围不同),这些因素会对通信效率产生影响.

2.3.2 信息编码

如文献[45,85]所述,存储型网络隐蔽信道依赖于信道载体的特性,有较大的传输空间,并且信道载体往往可以给网络隐蔽信道提供大量的辅助功能(例如可靠性传输),因此,存储型网络隐蔽信道对信息编码的依赖较小,专门研究存储型网络隐蔽信道编码的文献较少.Iglesias 等人[38]以检测的视角对利用 TCP/IP 协议的网络隐蔽信道的编码特征分为了 5 类,其中包括值与符号对应方法,使用 1 个或多个协议头字段的值与隐蔽信息符号进行对应编码[48−50].

2.3.3 信道优化

丰富的网络协议和特性使得存储型网络隐蔽信道可以通过更丰富的手段进行优化,进而提供新的功能或特性提升自身的隐蔽性、鲁棒性和通信效率,包括微协议技术、动态路由技术、多协议传输技术.

(1) 微协议技术

微协议是用来规范网络隐蔽信道通信过程的一组压缩编码[86−88],微协议的协议头往往嵌入在网络隐蔽信道的隐藏信息中[45].Wendzel 等人[89]对存储型网络隐蔽信道的结构进行了划分,把隐蔽信道利用的公开协议(例如 TCP 协议、ICMP 协议等)称为底层协议(underlying protocol),把隐蔽数据嵌入的部分称作上层协议(cover protocol),在上层协议中放置微协议(micro-protocol)和隐蔽数据(payload).微协议能够对网络隐蔽信道进行增强,可以提供的功能包括可靠性、动态路由、代理功能、同步连接、段管理、自动适应网络配置等[24],从而提高网络隐蔽信道在真实网络环境下的适应性和灵活性.

ping tunnel[83]利用 ICMP 的“Echo Request”报文和“Echo Reply”报文构建微协议,但是占用空间较大,因此易于检测.Degraaf 等人[16]将 UDP 协议目标端口字段分为数据部分和序列号部分,保证隐蔽信道数据包的顺序不被打乱.Ray 等人[90]在 ICMP 协议“expected sequence number”字段插入 2 比特的序列号字段实现了收发确认功能,用“1”表示成功接收数据,用“2”表示等待下一条数据,从而提高了隐蔽信道的可靠性.Trabelsi 等人[71]实现了 CFTP(隐藏数据传输协议),利用 IP 协议的“record route”选项实现类似 FTP 协议的文件隐蔽传输协议.Mazurczyk 等人[17]将隐蔽信道与数字水印技术结合,将 6 比特的控制信息协议头嵌入到 IP 协议、UDP 协议、RTP 协议的协议头,实现对隐蔽传输的控制.

Wendzel 等人[89]提出了针对微协议的设计方法,将协议分为用来构建隐蔽信道的公开协议、包含隐蔽信道数据部分和隐蔽信道控制部分的隐蔽协议、用来控制隐蔽信道的微协议这 3 类;使用表层协议位到隐蔽协议位、隐蔽协议位到微协议位的映射,使隐蔽协议和微协议满足公开协议的标准行为.制定了微协议构建的 6 个设计步骤,包括定义表层协议并确定隐蔽协议使用的区域、评估隐蔽协议的可用位数以确定可用来构建隐蔽协议的值的范围、设计微协议相关功能和规则、评估微协议的可用位数确定可用来构建微协议的值的范围、建立公开协议与微协议的映射、使用形式化方法验证微协议是否满足公开协议的标准行为.

微协议面临的问题包括协议优化问题,由于微协议的控制信息和隐蔽数据的数据信息往往都要使用公开协议的协议头部分,如果微协议过大就会减少隐蔽数据携带的空间,降低传输效率,并且会更易容易被发现[23].Backs 等人[86]和 Ray 等人[90]针对优化协议头问题提出了动态协议头方法,由于微协议和隐蔽信道数据部分并不是要使用协议头的所有部分,为了不重复传递不使用的这部分协议头,通过串行线路接口协议压缩(compress for serial line interface protocol,简称 CSLIP)[91]方法优化协议空间,新的数据包只传输协议头发生改变的部分,从而节省了协议空间,使网络隐蔽信道不易被检测.

(2) 动态路由技术

动态路由可以使隐蔽信道在较大且动态的网络环境下(例如互联网环境)进行通信,通信路径不再是通信双方直接通信,而是通过很多跳转进行间接通信;并且通信路径也不再是静态的,而是依据一定规则动态变化.从而使通信双方不会直接暴露在监控者的面前,提高了隐蔽数据传输的隐蔽性、鲁棒性和传输效率[86].

Szczypiorski 等人[92]第一次提出了网络隐蔽信道中的动态路由技术.利用随机游走算法随机选择下一跳的通信节点,从而构建完全随机的隐蔽传输网络拓扑,每一次传输过程都是随机的,无法监控和预测隐蔽信道传输的路径,从而提高了隐蔽信道的隐蔽性.

Backs 等人[86]实现了一种基于 OLSR(optimized link-state routing)的动态路由协议.选择隐蔽性和连接质量最优的信道,被称为 SCCT 架构.引入隐蔽性质量(quality of covertness,简称 QoC)的概念对通信节点间的隐蔽性进行度量,与通信质量(quality of service,简称 QoS)一起构成通信节点间通信的两个度量指标,从而形成网络隐蔽信道的节点表和网络拓扑表,使用状态升级的方法对这两张表进行维护,从而保障通信质量.

(3) 多协议传输技术

与传统的只通过某一特定通信协议构建隐蔽信道的方法不同,多协议隐蔽信道提供多种通信协议进行隐蔽数据传输,从而获得更好的网络环境适应能力,提高了隐蔽信息传输成功的可能,同时也降低被检测的可能.

Yarochkin 等人[93]提供了多种应用层的通信协议作为构建隐蔽信道的底层协议,将这些协议组成多协议的协议栈,每种协议会被专门的事件触发.协议的执行分为网络环境学习阶段和数据传输两个阶段:在网络环境学习阶段,通信节点会被动监听网络流量确定可用的网络协议集合,使用成功率评分算法进行协议选择,使通信过程的数据包被过滤的数量达到最小;在数据传输阶段,发送方会根据网络环境学习阶段的学习结果选择底层网络协议进行数据传输,并监控整个通信过程,如果传输中断或是被过滤,会切换其他通信协议进行传输,从而绕过针对特定协议的网络审查机制.

Wendzel 等人[94]会在每个数据包发送前,从多个可用于构建网络隐蔽信道的协议中挑选一个,之后再发送数据.隐蔽数据可以通过分片的方式分配到不同的传输协议构建的隐蔽信道中,监控者只有将各个传输协议传输的隐蔽数据收集齐,才能拼凑出一条完整的隐蔽数据,降低了隐蔽信道被发现的可能性,提高了隐蔽信道的隐

蔽性.

Xie 等人[10]基于跳频通信(frequency hopping communication)的思路设计了多协议转换的网络隐蔽信道,使用伪随机码序列构建跳转指令,用来控制频率同步,并使用移频键控(frequency shift keying,简称 FSK)在多个频率中进行选择.由于通信双方有相同的跳频模式,因此可以使用预先定义的跳频序列,在不同网络协议构成的网络隐蔽信道间进行切换,并通过发送方缓存计算的 hash 值进行差错控制,保证网络隐蔽信道的鲁棒性.

2.4 时间型网络隐蔽信道构建

2.4.1 码元设计

时间型网络隐蔽信道使用网络通信载体的时间特性进行隐蔽信息传输,Wendzel 等人[45]按照网络隐蔽信道构建方法将时间型隐蔽信道分为 4 个模式.

(1) 时间间隔模式:利用 PDU 不同的时间间隔进行隐藏信息编码,例如改变 LAN 数据帧的发送间隔[42]、改变 BACnet 协议数据包或 IP 数据包的时间间隔[80]、针对键盘输入对 SSH 数据包进行延迟[55]、接收 IEEE 802.2 I 格式的数据帧后延迟确认[64]、改变 VPN 数据包的间隔时间[65]、记录分割合法通信序列并依据间隔时间重放这些合法通信片段[58]等.

(2) 速率模式:改变通信数据流中的数据速率,例如通过 Clear to Send 或 Ready to Send 指令延迟一系列通信端口的吞吐量[34].

(3) PDU 顺序模式:通过改变 PDU 顺序编码隐藏数据,例如改变 IPSec AH 包的顺序[48]、改变 IPSec ESP 包的顺序[48]、改变 TCP 包的顺序[47,95]、改变 VPN 数据包的顺序[96]、改变 IPSec 数据包的顺序[65]、改变 CSMA/CD 网络中合法数据帧的顺序[34]等.

(4) 重传模式:重传之前发送或接收的数据包,例如通过发送 DNS 请求 1 次或两次进行编码、复制 IEEE 802.11 数据包[77]、通过重传选定的 TCP 数据段编码、接收方通过不发送确认信息迫使发送方重发数据包[97]等.

目前,时间型网络隐蔽信道使用最多的模式是时间间隔模式,大量研究都是基于网络数据包间隔(inter-packet-delay,简称 IPD)进行的[31,58,98,99].另外,Archibald 等人[59]对网络数据包间隔方法进行了改进,使用多个网络数据包间隔(m-IPD)作为码元,从而提高时间型网络隐蔽信道的鲁棒性.

2.4.2 信息编码

由于网络时间型隐蔽信道能够用来传输信息的载体特性只有时间特性,可以利用的资源较少,因此编码就成了时间型网络隐蔽信道重要的环节.由于时间型网络隐蔽信道的鲁棒性和通信效率相对较低,因此时间型网络隐蔽信道的信息编码主要目标是提高信道传输效率和鲁棒性.

较早的网络时间型隐蔽信道利用网络数据包间隔时间进行简单的二进制编码,例如数据包间没有时间间隔编码为 0,数据包间有时间间隔编码为 1[31].这种编码方式传输效率较低,且没有任何可靠性保障机制,很容易受到网络噪声的干扰.Wu 等人[60]使用霍夫曼编码对时间隐蔽信道的隐蔽信息进行编码.霍夫曼编码可对隐藏信息进行无损压缩,可有效提高传输效率,但是在鲁棒性方面并没有考虑.Archibald 等人[56]、Liu 等人[100,101]使用扩频码对时间隐蔽信道进行编码,提高信道的鲁棒性,可以使用有效的扩频因子抵御信道噪声.Sellke 等人[102]以几何码的方式,将不同的数据率 L 比特的隐藏数据映射到 n 个数据包中,以牺牲隐蔽信道数据率为代价,使得通信模式无法被辨别,以此提高信道的隐蔽性.Archibald 等人[103]使用喷泉码对时间隐蔽信道进行编码,通过喷泉码引入的大量冗余增加网络隐蔽信道的鲁棒性,用随机生成的线性码符号增加隐蔽信道的抗检测性.Houmansadr 等人[44]使用多种线性编码对网络隐蔽信道进行编码,包括 RS 码、Golay 码、两个类型的 Turbo 码(分组 Turbo 码和卷积 Turbo 码)、低密度奇偶校验码(LDPC),并对每种类型编码的网络隐蔽信道做鲁棒性评估和抗检测性评估.

2.4.3 信道优化

(1) 基于统计学的时间隐蔽信道

时间型网络隐蔽信道又可分为基于统计学的时间型网络隐蔽信道和非基于统计学的时间型网络隐蔽信

道,还可以利用一组码元的统计学特征进行隐蔽信息传输[104].基于统计学等时间型网络隐蔽信道的主要目的是提升网络隐蔽信道的隐蔽性[11,105].

早期的网络时间型隐蔽信道是直接使用编码元素(例如网络数据包时间间隔)进行编码的.Cabuk 等人[31]提出了基于数据包时间间隔的网络时间型隐蔽信道(inter-packet covert timing channel,简称 IPCTC),利用时间窗口内是否包含数据包进行二进制编码,将时间分成连续相等不相交的时间窗口,在时间窗口内发送数据包代表比特“1”,不发送数据包代表比特“0”.Sha 等人[55]提出了 JitterBug 时间型网络隐蔽信道,终端每次敲击键盘的行为都会向服务器端发送一个小幅度延时的数据包,使网络数据包间隔时间具有特殊的意义,从而泄露终端信息.

随着时间的发展,出现了隐蔽性更强的基于统计学的时间型网络隐蔽信道.Brodley 等人[58]提出了基于重传的时间型隐蔽信道(time-replay covert timing channel,简称 TRCTC),收集合法信道的网络数据包间隔时间为编码提供样本,对收集的网络数据包间隔时间排序,并将它们平均分为两个部分,并与二进制编码的值对应,从网络数据包间隔时间较大的部分随机取出一个网络数据包间隔时间代表比特“1”,从较小的部分取出随机值发送代表比特“0”.

Gianvecchio 等人[98]提出了基于模型的时间型隐蔽信道(model-based covert timing channel,简称 MBCTC),以网络数据包间隔时间分布模型的形式模拟合法信道:首先,准备几种待选的分布模型(例如指数分布、正态分布等);之后,统计合法信道的网络数据包间隔时间,根据最大似然估计出的待选分布模型的参数,使用标准差最小的模型作为最佳拟合模型,利用该分布模型的分布逆函数进行编码[11,105].

Liu 等人[99]提出了基于分布匹配的时间型隐蔽信道(distribution-matching covert timing channel,简称 DMCTC),对特定的分布模型进行模拟,将统计的合法信道网络数据包间隔时间按粒度非常小的区间统计成直方图,然后将区间均分为两个区间集,从较大部分的区间集中随机取出一个区间,并从区间内随机取出一个网络数据包间隔时间作为比特“1”,从较小部分区间内的随机区间的数据包间隔时间作为比特“0”.当发送比特 0 时,从较小部分的区间集中随机取出一个区间,然后从该区间内随机取出一个网络数据包间隔时间,当区间内所有网络数据包使用完后进行重新采样.

(2) 降低统计性规律

网络时间隐蔽信道的检测往往针对网络载体时间特性的统计性规律进行,一些研究者针对这一特点采取了相应的研究.Walls 等人[106]针对熵检测的检测方法提出了熵抚平的方法,将隐蔽信息发送过程分为发送和抚平两个阶段:在发送阶段,用来传输隐蔽信息的网络数据包间隔时间会造成整个信道熵率的改变,使隐蔽信道容易被检测出来;在抚平阶段,向外发送用以抚平熵率的数据包,使得整体的网络数据包间隔时间的熵值回归于合法信道.

(3) 多链路传输

传统的网络隐蔽信道是通过一条通信链路进行隐蔽信息传输的,这种单链路的传输方式存在一些弊端,例如需要同步、信道容量较低、可以通过规律性检测发现、较容易针对等[32].多链路传输使用多条传输链路进行隐蔽信息传输,降低通信被发现的可能,传输效率也更为高效.

Murdoch 等人[32]提出了一种多连接隐蔽信道,信息发送者与信息接收者之间建立多个活动的连接,通过这些连接发送数据包的顺序和特定的传输模式进行编码,从而使隐蔽信道不依赖于特定的信道条件,也不包含特征较强的统计规律.

Luo 等人[47]提出了一种多链路传输的时间隐蔽信道构建机制,使用 TCP 包和 TCP 流作为两类编码对象,每条信息使用 N 个 TCP 包和 X 条 TCP 流进行编码,通过 TCP 包在 TCP 流上分配的组合进行编码,并给予组合数学提供了 10 类编码方式.由于使用了 TCP 作为传输协议,可以保证传输的可靠性.这种多链路的传输方式提高了信道的容量,也降低了单一链路信息过于密集导致隐蔽信道被发现的可能.

2.5 小 结

本节从码元设计、信息编码和信道优化这 3 个方面归纳分析了存储型和时间型两类网络隐蔽信道构建技术.网络隐蔽信道的构建研究的重心从最初的以实现隐蔽传输基本功能、在网络环境下寻找可用来作为隐蔽信

息载体的存储属性和时间属性并设计相应的码元模式,逐渐过渡到增强信道的功能和性能上.存储型网络隐蔽信道面对的主要挑战是,如何弥补只使用单一存储属性作为隐蔽信息载体时隐蔽性较差的问题.目前采用的主要手段是增强信道的功能,例如微协议技术、动态路由技术、多协议传输技术.时间型网络隐蔽信道面临的主要挑战是,如何弥补信息携带能力低、只能串行通信的时间属性带来信道容量低、鲁棒性差的问题.目前主要采用的是编码手段.另外,由于时间间隔已经作为时间型网络隐蔽信道的最常见的传输载体,已经出现了大量的基于统计学的检测方法,因此需要进一步提升时间型网络隐蔽信道相对于统计学检测方法的抗检测性.

3 网络隐蔽信道评估

3.1 评估指标

与网络隐蔽信道能力维度相同,网络隐蔽信道的评估指标包含 3 个方面:隐蔽性、鲁棒性和传输效率.隐蔽性指网络隐蔽信道不被发现的能力,鲁棒性指网络隐蔽信道抗干扰和准确传输数据的能力,传输效率用来指网络隐蔽信道单位时间内传输数据量的能力.

3.2 评估方法

3.2.1 隐蔽性

由于存储型隐蔽信道具有一定的技术特异性,因此没有统一的隐蔽性评估方法.使用针对特定存储型网络隐蔽信道检测技术进行隐蔽性评估的方法,详见本文第 4.3.1 节.目前,大部分隐蔽性评估的研究都是针对时间型网络隐蔽信道的.

Wu 等人[60]使用网络隐蔽信道的特定属性的离散程度对隐蔽性进行评估,针对时间隐蔽信道可以使用标准差进行评估,其中,C_t表示隐蔽性,将传输的时间段平均分为 $s\omega$个非交叠的窗口,x_i表示第 i 个窗口内的被测属性(例如数据包时间间隔):

$$\sigma = STDEV(X) = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n}} \tag{1}$$

$$C_t = STDEV\left(\frac{\sigma_i - \sigma_j}{\sigma_j}\right), i < j < s\omega, \forall i, j \tag{2}$$

Houmansadr 等人[44]使用双样本 K-S 检测(kolmogorov-smirnov test)评估抗检测性.K-S 检测用来检验连续的一维概率分布是否相等,其中,$F(x)$和 $G(x)$分别为合法通信数据和隐蔽信道的网络数据包间隔时间分布:

$$D_{KS}=\sup_x|F(x)-G(x)| \tag{3}$$

Archibald 等人[103]使用 K-S(kolmogorov-smirnov test)检测和 K-L 离散度检测(kullback-leibler divergence measure)对隐蔽信道的隐蔽性进行量化.其中,K-L 离散度检测相对熵,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:

$$D_{KL}(P \| G) = \sum_x p(x) \cdot \log\left(\frac{p(x)}{g(x)}\right) \tag{4}$$

3.2.2 鲁棒性

王鹏等人[104]使用误码率(bit error rate,简称 BER)对网络隐蔽信道的鲁棒性进行测量:

误码率=错误码元数/传输总码元数.

Houmansadr 等人[44]也使用误码率作为鲁棒性的测量指标,将误码率定义为将原始信息通过编码传输后再解码的最终信息比较得到的错误概率:

$$BER = \frac{\sum_{i=1}^{k} e(m(i), m'(i))}{k} \tag{5}$$

其中,k 为解码后的信息长度;$m(i)$为第 i 位原始信息;m'为第 i 位传输后获得的信息;e 为两个信息的比较函数,两

个信息相同值为 0,不相同值为 1.

Liu 等人[100]使用引入网络噪声的方法做鲁棒性测试,网络噪声包括数据包丢失、延迟、抖动以及人为的干扰噪声,然后测量信道的误码率,以此来表示网络隐蔽信道的鲁棒性.

综上所述,对鲁棒性的评估都是使用误码率作为评测指标的.

3.2.3 传输效率

Houmansadr 等人[44]将传输效率定义为每个隐蔽数据流包传递的隐蔽信息的比特数,其中,K 是使用 N+1 个隐蔽信息数据流发送的隐蔽信息的比特数:

$$r=\lim_{N\to\infty}\frac{K}{N} \tag{6}$$

王鹏等人[104]使用信道容量作为测量时间型隐蔽信道通信效率的方法.信道容量指单位时间通信信道传输数据信息量的上限,时间型网络隐蔽信道容量取决于每个数据包间隔时间携带的信息量 bit 和平均网络数据包间隔时间 $\overline{ipd}$:

$$capacity=\frac{bit}{\overline{ipd}} \tag{7}$$

Wu 等人[60]考虑了用来对原始信息编码的码元数量和编码优化后的码元数量之间的关系,将传输效率定义为最大可能的无错信息速率,用比特/秒(bits/s,bps)表示.其中,N 表示 N 元编码在时间 t 内传输的信息量:

$$C=\frac{N(t)}{t} \tag{8}$$

综上所述,网络隐蔽信道的传输速率使用单位码元内包含的信息量或单位时间内传递的信息量进行评估.

3.3 小 结

本节从隐蔽性、鲁棒性和传输效率这 3 个方面总结了网络隐蔽信道评估方法.目前,网络隐蔽信道的鲁棒性和传输效率已经有了相对统一的评估方法,而隐蔽性则还没有统一的评估方法.造成隐蔽性没有统一评估方法的原因首先是因为各类网络隐蔽信道的差异较大,特别是存储型网络隐蔽信道的隐蔽性来自于隐蔽信息载体的未知和不确定,因此很难用同一种方法对网络隐蔽信道的隐蔽性进行评估;另一方面,网络隐蔽信道的评估方法来自于网络隐蔽信道的检测方法,由于网络隐蔽信道的检测方法还在发展和完善中,没有形成统一的方法,因此,网络隐蔽信道的隐蔽性评估方法也相应地没有统一.

4 网络隐蔽信道对抗

网络隐蔽信道对抗指破坏、削弱、发现网络隐蔽信道的方法.Zander 等人[12]把网络隐蔽信道对抗技术分为消除技术、限制技术、检测技术这 3 类:网络隐蔽信道消除技术指从原理上消除网络隐蔽信道的存在,对于一些早期的网络隐蔽信道可以达到这个效果;网络隐蔽信道限制技术指限制隐蔽信道的容量,这意味着会引入噪声,同时也降低了系统的性能;网络隐蔽信道检测技术指发现隐蔽信道的存在.王鹏等人[104]认为,针对时间型网络隐蔽信道的对抗有两种思路:一种是通过剥夺目标信道中隐蔽信道所需的网络共享资源,从而限制隐蔽信道的存在;一种是检测出隐蔽信道的存在,进而消除隐蔽信道的影响.

网络隐蔽信道对抗的 3 类技术分别对应了网络隐蔽信道需求和评估的 3 项能力维度:消除技术针对网络隐蔽信道的鲁棒性,用以破坏隐蔽信道构成的基础条件;限制技术针对网络隐蔽信道的传输效率,用来降低网络隐蔽信道的带宽和传输能力;检测技术针对网络隐蔽信道的隐蔽性,用来发现网络隐蔽信道的存在.

4.1 网络隐蔽信道消除技术

通过对可疑的网络协议或网络端口阻塞的方式,可以消除基于这些网络协议的网络隐蔽信道(例如 ICMP 协议),但是对于一些基于重要网络协议的网络隐蔽信道(例如 IP 协议、TCP 协议、DNS 协议),则无法采取这样的方式[12]消除.

通信归一化(traffic normalization)方法[107,108]是一种移除网络通信中模糊和破坏通信原则元素的方法,网络

隐蔽信道往往利用网络通信协议头的保留字段或未用字段构建的网络隐蔽信道,通信归一化方法将这些字段设置为 0,并移除未知协议头的扩展部分.网络归一化方法可分为无状态和有状态两类[51]:无状态归一化方法只考虑一个时间点的数据包,不考虑之前的数据包;有状态归一化方法会缓存之前收到的数据包,因此可对抗更多的隐蔽信道.通信归一化方法可消除很多基于网络层(例如将 IP 的 ID 设置为 0、设置段的偏移量为 0、保证校验值的正确等)、通信层(例如重写 TCP 协议的 ISN、源 IP 地址、源端口、TTL 等)、应用层(例如限制 HTTP 协议只能以特定的集合和顺序应答请求)协议的协议头字段及特征构造的网络隐蔽信道,对于网络存储型隐蔽信道更为有效.网络归一化的缺陷是:有可能将 PDU 头字段设置成错误的值导致不可用;无法对使用合法协议头字段值的隐蔽信道起作用(例如使用不同协议编码);缓存有限,导致只能在计算资源没有耗尽时起作用[107].

网络隐蔽信道消除技术对存储型网络隐蔽信道更有效,受限于计算资源,如何在不破坏通信协议语义的基础上高效处理海量网络数据,是个很大的挑战.

4.2 网络隐蔽信道限制技术

Proctor 等人[104,109]认为:当隐蔽信道的容量小于一定的程度时,即使出现网络隐蔽信道也是可以容忍的.也就是说,隐蔽信道所处环境噪声足够大时,使得信噪比很低时,使得信息的准确度低至无法容忍的地步,网络隐蔽信道是不能造成威胁的.因此,可以通过在信道中添加延时的方式造成时间型网络隐蔽信道的解码错误.Giles 等人[110]提出了网络干扰(network jammer)的方法,利用随机延迟网络数据包的方式,限制网络时间型隐蔽信道的容量.这种方法虽然可以干扰时间型隐蔽信道的通信,但也会影响合法通信的性能,特别会对实时通信网络造成严重影响.Wendzel 等人[111]针对使用一系列不同协议进行编码的隐蔽信道进行限制,可针对协议切换的行为加入延迟,从而降低这类网络隐蔽信道的容量.Kang 等人[112,113]提出了网络泵(network pump)技术,可以使网络数据包的间隔时间随机化或均匀分布,从而干扰网络时间隐蔽信道.这种方法虽然可以有效地干扰网络时间隐蔽信道,但是也会影响对服务质量有较高要求的服务,例如 VoIP、视频流、SSH 协议等.

网络隐蔽信道限制技术对时间型网络隐蔽信道更有效,但这种方式同时也会影响合法网络通信的质量,存在一定的副作用.

4.3 网络隐蔽信道检测技术

网络隐蔽信道检测技术是网络隐蔽信道对抗中研究最多的技术,本文把网络隐蔽信道检测技术分为存储型网络隐蔽信道检测和时间型网络隐蔽信道检测两个部分进行梳理.

4.3.1 存储型网络隐蔽信道检测

Sohn 等人[114]使用支持向量机(support vector machine,简称 SVM)方法对 TCP/IP 协议中的存储型隐蔽信道进行检测,将 TCP/IP 数据包头中的标识字段(identification)和 IP 数据包中的序列字段(sequence)的值作为特征,使用线性和多项式两类核函数对对隐蔽信道进行模式分类.之后,Sohn 等人[115,116]又使用支持向量机方法对 ICMP 数据包中的存储型隐蔽信道进行检测,将 ICMP 数据包分为两种情况进行检测:第 1 种情况,根据 ICMP 数据包负载部分(payload)的字段值分为 13 个维度;第 2 种情况,除了负载部分,还包含 4 byte 的包头字段共 15 个维度,并使用支持向量机的线性和多项式两类核函数对 ICMP 数据包进行训练和模式分类.Bethencourt 等人[15]使用神经网络对不同操作系统的 ISN 序列进行训练,针对基于 TCP ISN 的存储型网络隐蔽信道进行检测,取得了很高的准确率.Borders 等人[19]使用 HTTP 协议的请求字段大小、请求时间间隔、发送时间、出站带宽占用等特征进行建模,对基于 http 的网络隐蔽信道进行检测.Guang 等人[117,118]为了解决同时兼顾检测速度与计算复杂性的问题,对 TCP 协议的字段数据进行联合分析,分析数据包和数据包之间每个字段相关属性的规律,所有属性通过核密度估计、变异系数、自相关系数转换为特征向量矩阵,并使用 SVM 分类器训练特征向量矩阵,获得了较快的检测速度,并降低了计算复杂度.Krzysztof 等人[119]使用数据挖掘方法寻找多个数据流中 IPv4 TTL 字段的频繁项集,以此作为隐藏信息模式检测分布式隐蔽信道.

综上所述,针对存储型网络隐蔽信道的检测方法主要采用对某一通信载体的正常通信特征进行训练建模的方式训练分类器,然后利用分类器对网络隐蔽信道进行检测,可以获得较好的效果.

4.3.2 时间型网络隐蔽信道检测

时间型网络隐蔽信道检测技术是近年来网络隐蔽信道检测研究最多的方向,时间型隐蔽信道检测方法大致分为 3 个大方向[105,120]:形态检测(shape test)、规律性检测(regularity test)和熵检测(entropy test).所有的检测方法都是围绕提取网络流量信息、鉴别网络数据包间隔时间(IPD)分布的改变和统计异常进行的,使用一阶统计特性(例如平均值、方差和分布函数等)表示网络数据流的形态特征(例如 K-S 检测),使用二阶或者多阶统计特性(例如自相关、互相关等)表示数据流的规律性(例如熵检测)[28,121,122].近年来又出现了基于机器学习的时间型网络隐蔽信道机器学习的检测技术.本文按照形态检测、规律性检测、熵检测和基于机器学习的检测对网络隐蔽信道检测技术进行梳理.

(1) 形态检测

形态检测[31]指构建一个指标体系,将当前信道通信流量的 IPD 分布与已知合法的公开信道通信流量样本的 IPD 分布进行对比,以验证二者是否有显著的差异.

常用的形状测试是 K-S 检测(kolmogorove-smirnov tests)[100],K-S 检测可用来检验连续的一维概率分布是否相等,可用来区分合法的公开信道和隐蔽信道.其中,$F(x)$和 $G(x)$分别为合法通信数据和隐蔽信道的网络数据包间隔时间分布:

$$D_{KS}=\sup_x|F(x)-G(x)| \tag{9}$$

Peng 等人[123]使用 K-S 检测可以检测出水印 IPD,从而证明 K-S 检测可有效检测重放型时间隐蔽信道.

Archibald 等人[120]使用韦尔奇 t 检验(Welch's t-test)对时间隐蔽信道进行检测.一般的形状检测基于密度函数提取公开合法信道和隐蔽信道测量指标,这个方法存在两个问题:经验密度函数生成成本很高,把样本转换为密度函数会带来偏差.使用 Welch t 检验可以避免这两个缺陷.t 检验一般用于统计假设检验确定两个数据集是否存在显著差异,而韦尔奇 t 检验对于两个样本量大于 30 的标准分布的标准差计算有很好的鲁棒性,定义为

$$t=\frac{\bar{X}_1-\bar{X}_2}{\sqrt{\frac{S_1^2}{N_1}+\frac{S_2^2}{N_2}}} \tag{10}$$

Fahimeh 等人[124]用威尔科克森符号秩检验(Wilcoxon signed rank test)、斯皮尔曼等级相关检验(Spearman Rho correlation test)、曼-惠特尼-威尔科克森秩和检验(Mann-Whitney-Wilcoxon rank sum test)这 3 种统计方法分别对正常通信和隐蔽信道通信进行检验并得到统计评分,并以此为检测维度对时间型网络隐蔽信道进行实时检测,具有很高的检测效率.

(2) 规律性检测

规律性检测[31]指将数据流变化的统计学特征规律当做检测指标对隐蔽信道进行检测,对网络数据流的网络数据包间隔时间的标准差的变化进行了量化,定义为

$$Reg=StdDev\left(\frac{\sigma_i-\sigma_j}{\sigma_j}\right),i<j,\forall i,j \tag{11}$$

在每个时间窗口内都会计算网络数据包间隔时间的标准差σ_i,并进行规律性计算.规律性检测适用于基于模型的网络时间型隐蔽信道(MBCTC)和重放型网络时间隐蔽信道(TRCTC)这些使用规律性方法生成的隐蔽信道,它们在长时间的通信特征是符合正常的公开信道的,但是在较小的窗口内就会呈现出统计学规律.

(3) 熵检测

熵检测[125]指使用熵作为评测指标对 IPD 分布的随机性进行检测的方法,包括修正条件熵检测(corrected conditional entropy test,简称 CCE)、K-L 离散检测(Kullbacke-Leibler divergence test).

修正条件熵最早用来做生物学研究,Gianvecchio 等人[125]使用修正条件熵作为检测指标对 MB-CTC 和 TR-CTC 类型的隐蔽信道进行检测.这两种隐蔽信道生成的流量中的 IPD 符合独立同分布(independent and identically distributed),而合法的公共信道中的数据流量符合条件分布,通过这种检测方式对 HTTP 和 SSH 中的时间隐蔽信道进行检测.定义为

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

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.