泛在网络环境下隐蔽通道关键技术研究综述

李凤华[1,2]，李超洋[1,2]，郭超[3]，李子孚[1]，房梁[1]，郭云川[1,2]

（1. 中国科学院信息工程研究所，北京 100093； 2. 中国科学院大学网络空间安全学院，北京 100049；
3. 北京电子科技学院电子与通信工程系，北京 100070）

摘 要：在泛在网络环境下，隐蔽通道通过修改系统共享资源，绕开系统的安全策略传输隐蔽信息，给计算机和网络系统造成了严重的安全威胁。针对此问题，主要从度量、构建和检测 3 个方面对泛在网络环境下的隐蔽通道相关研究进行归纳和分析。首先，总结归纳了典型的隐蔽通道度量指标，包括隐蔽通道的容量、稳健性、抗检测性、规律性和形状。其次，归纳整理了隐蔽通道的构建方法，并从共享资源、容量、稳健性、抗检测性、优点和缺点 6 个方面对隐蔽通道构建技术进行了对比分析。再次，从隐蔽通道类型、准确率、是否能盲检、优点和缺点 5 个方面对比分析了隐蔽通道的检测技术。最后，总结了隐蔽通道的发展趋势并展望了未来研究方向。

关键词：泛在网络；隐蔽通道度量；隐蔽通道构建；隐蔽通道检测

中图分类号：TP393

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022072

Survey on key technologies of covert channel in ubiquitous network environment

LI Fenghua[1,2], LI Chaoyang[1,2], GUO Chao[3], LI Zifu[1], FANG Liang[1], GUO Yunchuan[1,2]

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: In the ubiquitous network environment, covert channel bypasses the system's security strategy to transmit covert information by modifying the system's shared resources, which poses a serious security threat to the computer and network system. The researches on covert channel in ubiquitous network environment were summarized and analyzed from three aspects of measurement, construction and detection. First, the typical covert channel metrics including the capacity, robustness, anti-detection, regularity and shape were summarized. Second, the construction technologies of covert channel were summarized and analyzed from six aspects of resource sharing, capacity, robustness, anti-detection, advantages and disadvantages in the first time. Third, the detection technologies of covert channel were compared and analyzed from five aspects of the type of covert channel, accuracy, whether it can be blind detection, the advantages and disadvantages. Finally, the development trends of covert channel were summarized and future research directions were prospected.

Keywords: ubiquitous network, covert channel measurement, covert channel construction, covert channel detection

0 引言

隐蔽通道是指恶意通信双方通过修改共享资源的数值、特性或状态等属性，编码和传输隐蔽信息的通道，以此绕开系统安全策略[1-2]。随着网络环境日益复杂及隐蔽通信技术的不断发展，各种隐蔽

收稿日期：2021−12−15；**修回日期**：2022−03−09

通信作者：郭云川，guoyunchuan@iie.ac.cn

基金项目：国家重点研发计划基金资助项目（No.2019YFB2101702）；国家自然科学基金资助项目（No.U1836203）；广东省重点领域研发计划基金资助项目（No.2019BP010137005）；中国科学院青年创新促进会人才基金资助项目（No.2019160）

Foundation Items: The National Key Research and Development Program of China (No.2019YFB2101702), The National Natural Science Foundation of China (No.U1836203), The Key-Area Research and Development Program of Guangdong Province (No.2019BP010137005), Talent Fund Program of the Youth Innovation Promotion Association CAS (No.2019160)

通道频繁出现，包括面向物理层（CVE-ID:CVE-2019-13270）、数据链路层（CVE-ID:CVE-2019-13271）、操作系统（CVE-ID:CVE-2020-0550）和网络层（CVE-ID:CVE-2019-13264）等的隐蔽通道。特别地，亚马逊云计算服务研究人员 Pawel 发现了一种名为 Snoop 的新型隐蔽通道攻击，该隐蔽通道可窃取 Intel 处理器内部缓存中的数据。

随着互联网及隐蔽通信技术的发展，隐蔽通道对泛在网络（如物联网、云计算和卫星互联网络等）产生了更严重的安全威胁。如在云环境中，由于其共享计算资源，具有较高权限的程序可通过隐蔽通道将数据泄露给具有较低权限的程序，从而打破逻辑隔离，这会给云安全带来巨大的挑战。攻击者可以通过路由器（CVE-ID:CVE-2019-13268）等基础网络设备中的隐蔽通道，窃取互联设备中的隐蔽信息，给物联网等网络环境带来巨大的安全威胁。

隐蔽通道的潜在威胁引起了研究者的广泛关注，多年以来，相关研究者通过对隐蔽通道的不断深入研究，使该领域有了实质性的研究进展。隐蔽通道研究可大致分为 3 个阶段。

1) 早期隐蔽通道的研究主要是利用操作系统中的共享资源，如硬件随机数生成器[3]、处理器缓存[4]、分支预测器[5]和 I/O 设备[6]等，构建时间或存储隐蔽通道[1]，即操作系统隐蔽通道。例如在 Sun Solaris 系统中，Solaris 内核允许 2 个非特权本地用户处理程序建立一个隐蔽通道来绕过系统安全策略（CVE-ID:CVE-2008-3875）。

2) 随着互联网的不断发展，研究重点逐渐转移到了网络隐蔽通道，网络隐蔽通道主要有存储隐蔽通道（CSC, covert storage channel）、时间隐蔽通道（CTC, covert timing channel）、混合隐蔽通道（CHC, covert hybrid channel）、行为隐蔽通道（CBC, covert behavior channel）4 种[1]。典型的网络隐蔽通道多数是基于 TCP/IP 协议栈来构建的[7]，这些隐蔽通道往往通过使用网络协议[8]或数据包[9-10]的协议字段[11]和时间特征[12-15]，进行隐蔽通信。

3) 近年来，物联网、云环境、移动通信网络、区块链等各种新型网络不断兴起，逐渐形成了泛在、复杂的网络环境，这使隐蔽通道有了更多的可乘之机。泛在网络环境下的隐蔽通道利用不同场景下共享资源的不同特性（如通过物联网协议[16-17]、云中的内存重复删除[18-19]、移动通信网络中的语音流数据[20]、Air-gap 系统中的磁信号[21]等）构建隐蔽通道，以达到提高隐蔽通道容量或者增强稳健性等目的，给日益复杂的网络环境带来了更大的安全挑战。

面对各种隐蔽通道产生的威胁，研究者提出了一系列消除或限制技术，以降低隐蔽通道的攻击风险，但是，随着隐蔽通信技术的不断发展，想要完全消除隐蔽通道非常困难。常见的隐蔽通道限制方案主要体现在 2 个方面。

1) 通过对通信环境施加限制策略，以破坏隐蔽通信，如对存储隐蔽通道添加噪声、对时间隐蔽通道和混合隐蔽通道增加时延和噪声、对 Air-gap 系统中的隐蔽通道还可以对隐蔽通信双方实施隔离[1]等。

2) 根据隐蔽通道的规律或特征，设计检测方法，以识别隐蔽通道，主要包括基于统计、基于机器学习、基于信息论、基于信息流分析等技术的检测方法。

通过干扰通信环境的隐蔽通道限制策略虽然可以降低隐蔽通信的风险，但是也会影响正常的通信质量。近年来，为限制隐蔽通道，研究者主要集中于隐蔽通道检测方法的研究。

在泛在网络环境下，用于构建隐蔽通道的共享资源和通信环境变得更加复杂多样。在不同网络环境下利用各种共享资源构建的隐蔽通道存在泛在性、差异性，难以用统一的框架或方法对其进行有效度量及准确检测。由于网络环境的特殊性，隐蔽通道构建研究也面对诸多困难，如由于区块链自有的加密属性和去中心化等特点，使区块链成为天然的隐蔽通信场景，但是由于其具有可追溯和抗篡改等特性，节点间交易信息会被区块链中的所有节点感知，这对构建具备抗检测性强的隐蔽通道带来了巨大的挑战；在云环境中，可以利用多种共享资源构建隐蔽通道，如 CPU、缓存或共享内存等，利用共享内存等资源构建的隐蔽通道虽然会有较大的隐蔽容量，但是往往易被检测；Air-gap 系统中的隐蔽通道多是利用电磁信号、功率等物理介质作为共享资源，此种隐蔽通道往往容量很小。

近年来，研究者针对泛在网络环境下隐蔽通道的度量、构建和检测问题，进行了深入研究，但是缺乏对此类隐蔽通道研究的综述分析。与已有的隐蔽通道研究综述相比，本文在分析已有研究成果的基础上，总结了隐蔽通道的常用度量指标及度量方法，重点对物联网、云环境、移动通信网络、Air-gap 系统、区块链和车载自组网（VANET, vehicular ad-hoc network）等网络环境下的隐蔽通道构建技术进行了多

维对比分析，系统分析了泛在网络环境下隐蔽通道的检测技术，并展望了未来的研究方向。

1 隐蔽通道度量

隐蔽通道度量是构建和检测隐蔽通道的基础，典型的隐蔽通道度量指标包括容量、稳健性、抗检测性、规律性和形状。容量指单位时间内隐蔽通道能够无差错传输的最大信息；稳健性指隐蔽通道存在干扰（如噪声和丢包等）时，准确传输数据的能力；抗检测性（也称隐蔽性）指隐蔽通道保持隐蔽通信且不被识别的能力；规律性和形状分别指时间隐蔽通道中包间时延（IPD, inter-packet delay）分布的规律和形状。

各度量指标存在如下影响与关联。容量、稳健性和抗检测性主要用于评估隐蔽通道的构建方法。一般情况下，当隐蔽通道的容量很大时，会表现出较强的稳健性；当稳健性差时也会降低隐蔽通道的容量。容量与抗检测性通常存在相互抑制的关系，容量增大会导致抗检测性降低；反之，若要提高抗检测性往往要降低容量。规律性和形状主要用于隐蔽通道的检测，规律性和形状的度量也能在一定程度上反映抗检测性，如对于时间隐蔽通道，当 IPD 分布的规律性或形状很明显时，会降低抗检测性。

1.1 隐蔽通道容量度量

在隐蔽通道容量的度量方面，面对复杂多样的信道环境，隐蔽通道容量度量可以分为：经典信道中的隐蔽通道容量度量[22-24]、量子信道中的隐蔽通道容量度量[25-27]、离散无记忆信道中的隐蔽通道容量度量[28-29]、噪声信道中的隐蔽通道容量度量[30-31]和其他信道中的隐蔽通道容量度量[32]。在经典信道中隐蔽通道容量的度量方面，多数研究者基于香农信息论对其进行度量[22-23,33]，如 Epishkina 等[22]利用互信息度量隐蔽通道的容量。El-Atawy 等[23]将基于数据包排序的隐蔽通道容量定义为每个数据包内编码隐藏信息的比特数，即

$$\text{Capacity}=\frac{H(P_L)}{k}\beta \tag{1}$$

其中，k 表示每个码字所包含的排序数据包个数；P_L 表示码字的概率分布；$H(P_L)$表示 P_L 的熵，代表每个码字的平均信息；β 表示一个数据包所包含的比特数。

Zhang 等[24]将基于编码语音数据流的隐蔽通道容量定义为单位时间内隐蔽信息的大小，即

$$C=\frac{N_C l_b}{T_C} \tag{2}$$

其中，N_C 表示隐藏消息的位置数，l_b 表示每个位置隐蔽信息的长度，T_C 表示语音静默周期。当 l_b 不同时，N_C 也不同，因为并不是所有的静默期都可以延迟和扩展。

在量子信道和离散无记忆信道中的隐蔽通道容量度量方面，经典无记忆信道和量子有损噪声玻色子信道（具有量子强噪声）的隐蔽通信的基本极限是平方根定律[25-27]，即在 n 个信道中可以可靠地传输高达 $O(\sqrt{n})$ bit 的隐蔽信息。Bloch 等[28]研究表明，在离散无记忆信道中，如果发送方和接收方共享 $\sqrt{n}$ 个密钥位，则可以在 n 个信道上实现容量达 $\sqrt{n}$ bit 的可靠隐蔽通信。对于复合离散无记忆信道中的隐蔽通道，Ahmadipour 等[29]考虑 2 个覆盖率度量。在第一个度量中，使用具有固定分布的每个状态的通道输出边缘的 K-L 散度（KLD, Kull-back-Leibler divergence）来度量覆盖度，根据不同分布，建立对应的最大容量。在第二个度量中，通过使用 2 种状态的通道输出边缘的总变化距离来度量覆盖率，给出了最优传输隐蔽率的上下界。

在噪声环境下隐蔽通道的容量度量方面，在加性白高斯噪声（AWGN, additive white Gaussian noise）的隐蔽通道中，发送方可以可靠地将 $O(\sqrt{n})$ bit 信息发送给 n 个预期接收方，该过程有极低的被检测概率，接收方通过单独的 AWGN 信道接收发送方的隐蔽信息[30]。离散无记忆信道和加性高斯白噪声信道的最大隐蔽编码速率随着消息块长度的减小而减慢，Bendary 等[31]研究表明，多输入多输出（MIMO, multiple-input multiple-output）AWGN 信道的隐蔽容量在一定条件下收敛到 MIMO AWGN 信道的容量。

此外，对于非相干快速瑞利衰落无线信道（NCFRFWC, non-coherent fast Rayleigh-fading wireless channel），Tahmasbi 等[32]研究表明，隐蔽容量是由有限个质点（包括一个质点）组成的振幅约束输入分布来实现的，并给出了数值边界。Ta 等[34]研究表明，信道衰落是隐蔽信号传输的关键，噪声不确定性越大，信道不确定性对检测误差平均概率和隐蔽容量的影响越显著。

1.2 隐蔽通道稳健性度量

稳健性已被广泛应用于隐蔽通道的度量。度量隐

蔽通道稳健性的相对统一的指标是误码率[24, 35]。

Zhang 等[24]利用误码率来评估长期演进语音承载（VoLTE, voice over long-term evolution）中隐蔽通道的稳健性，定义为

$$P_{\mathrm{e}}=\frac{N_{\mathrm{sp}}R_{\mathrm{l}}}{N_{\mathrm{C}}l_{\mathrm{b}}} \tag{3}$$

其中，R_{l} 表示 VoLTE 流量的丢包率，$N_{\mathrm{sp}}R_{\mathrm{l}}$ 表示在静默期结束时丢失的数据包数。

Zhang 等[36]基于误码率讨论了隐蔽通道的稳健性，稳健增益 γ（$\gamma\in\mathrm{R}^{+}$）定义为

$$\gamma=\frac{\widehat{P}_{\mathrm{e}}}{P_{\mathrm{e}}}=\frac{\sum_{j=1}^{NR_{\mathrm{l}}}e_j}{NR_{\mathrm{l}}},1\leqslant e_j\leqslant L(n_i) \tag{4}$$

其中，$\widehat{P}_{\mathrm{e}}$ 表示不编码的直接调制的误码率，P_{e} 表示在相同的网络条件下用特定的编码方案进行编码和调制后的误码率，N 表示静默期的数目，R_{l} 表示丢包率，e_j 表示第 j 次丢包导致的错误隐藏信息比特数，$L(n_i)$ 表示第 i 个静默周期中静默插入描述符（SID, silence insertion descriptor）数据包数目的码长。当 $\gamma\to\infty$ 时，可以认为隐蔽通道是完全稳健的。

1.3　隐蔽通道抗检测性度量

在隐蔽通道抗检测性度量方面，研究者主要利用基于多项式时间统计检验的度量方法，即对于隐蔽流量的数据流样本 n 和合法流量的数据流样本 n'，若存在一个任意小的函数 $f(\delta)$，使不等式 $\left|T(n)-T(n')\right|\leqslant f(\delta)$ 成立，则隐蔽通道相对于安全参数 δ 是多项式不可检测的[37]，其中，T 表示多项式时间统计检验。基于多项式时间统计检验的抗检测性度量方法包括 K-L 散度[37-38]和 K-S 检验（KST, Kolmogorov-Smirnov test）等[37-39]。

Archibald 等[38]使用 K-L 散度（又称相对熵）和 K-S 检验来度量隐蔽通道的抗检测性。K-S 检验和 K-L 散度都是用来比较合法流量和隐蔽流量的 IPD 分布差异的方法。K-L 散度具有非对称性，定义为

$$D_{\mathrm{KL}}(P\,\|\,G)=\sum_{x}P(x)\log\left(\frac{p(x)}{g(x)}\right) \tag{5}$$

其中，P 和 G 分别表示隐蔽流量和合法流量的 IPD 分布。

Wang 等[39]利用 K-S 检验度量隐蔽通道的抗检测性，定义为

$$D_{\mathrm{KS}}=\sup_x\left|F(x)-G(x)\right| \tag{6}$$

其中，$F(x)$和 $G(x)$分别表示隐蔽通信和合法通信的 IPD 分布。K-S 检验是一种稳健的非参数检验方法，对尺度变化不敏感而对分布函数的位置和形状参数敏感，该方法是比较两样本差异的常用方法。

此外，李彦峰等[40]使用熵率（ER, entropy rate）度量区块链隐蔽通道的抗检测性，定义为

$$\mathrm{ER}=\min_{i=1,2,\cdots,m}(\mathrm{CCE}(X_i\mid X_{i-1})) \tag{7}$$

其中，CCE 是修正条件熵（CCE, corrected conditional entropy）。熵率是对无穷序列不确定性的度量，熵率越小越能表现出序列规律。在实际中，可采用有限采样的方式，利用 CCE 计算熵率[40]。

K-L 散度、K-S 检验和熵率均可用于度量隐蔽通道的抗检测性。其中，K-L 散度和 K-S 检验都是基于合法流量 IPD 分布和隐蔽流量 IPD 分布的差异来评估隐蔽通道的抗检测能力。但是两者也有区别：与 K-S 检验相比，K-L 散度对样本的尺度变化更敏感。基于熵率的抗检测性度量依赖于大量正常通信的样本来确定检测对象的检测阈值[40]，与 K-L 散度和 K-S 检验相比，熵率更适用于通信样本量较大的情况。

1.4　隐蔽通道规律性度量

规律性的度量是指采用统计特征对网络流量变化的规律性进行度量。通过度量网络流量的规律性，统计合法流量和隐蔽流量的差异，以区分出合法流量和隐蔽流量。

Cabuk 等[13]通过统计网络数据流的网络数据包间隔时间的标准差的变化，来度量隐蔽数据流的规律性。具体地，将流量分成固定大小的非重叠窗口，统计每对窗口间的标准差变化，定义为

$$\mathrm{Reg}=\mathrm{StdDev}\left(\frac{\sigma_i-\sigma_j}{\sigma_j}\right),i<j,\forall i,j \tag{8}$$

其中，σ_i 表示第 i 个时间窗口内网络数据包间隔时间的标准差，StdDev 表示标准差函数（计算标准差）。Chow 等[41]利用 K-L 散度来度量隐蔽通道的不规律性。Cabuk 等[42]将分组数据流划分为非重叠窗口，并计算每个窗口的 IPD 的标准差，通过计算流量中窗口的标准差的差异来度量规律性。

1.5 隐蔽通道形状度量

形状度量是将隐蔽 IPD 分布与合法 IPD 分布中的已知指纹进行比较，度量 2 个分布之间的形状差异。常用的形状度量方法是基于计算描述合法流量和隐蔽流量的密度函数进行度量的，如基于 K-S 检验的形状度量[37]和基于韦尔奇 t 检验（WTT, Welch's t-test）的形状度量[43]。

K-S 检验通过取所有流量数据 x 的绝对差的上确界来区分隐蔽 IPD 分布 $F(x)$和合法 IPD 分布 $G(x)$ [37]。因为 K-S 检验对 2 种分布的形状参数敏感，所以也被用于隐蔽通道形状的度量。

Archibald 等[43]提出了一种基于韦尔奇 t 检验的形状度量方法，即

$$t=\frac{\overline{x_1}-\overline{x_2}}{\sqrt{\frac{s_1^2}{N_1}+\frac{s_2^2}{N_2}}} \tag{9}$$

其中，x_i 、s_i 和 $N_i(i=1,2)$ 分别是 2 种分布的样本均值、标准差和样本大小。为了生成 p 值（表示假设被接受或拒绝的概率）度量，从合法的网络流量中创建一个综合样本，并从观察到的网络流量中提取一个相对较小的样本。使用这些样本，在 p 值上创建阈值，p 值低于阈值的样本被归类为隐蔽流量。

K-S 检验和韦尔奇 t 检验的相同之处在于两者都是基于隐蔽 IPD 分布和合法 IPD 分布之间的差异来度量隐蔽流量的形状，区别在于基于 K-S 检验的形状度量方法直接根据合法 IPD 分布与隐蔽 IPD 分布的差值上界来区分合法流量与隐蔽流量，而基于韦尔奇 t 检验的形状度量方法基于合法 IPD 的先验分布先建立 p 值假设，再基于阈值对隐蔽流量进行归类，该方法可基于更多的合法 IPD 样本建立先验分布以创建更完整的流量指纹。当样本大小不均衡时，基于韦尔奇 t 检验的形状度量效果优于基于 K-S 检验的形状度量效果。

2 隐蔽通道构建

2.1 物联网隐蔽通道构建

物联网中的大多数设备都不具备由经验引发的抵御入侵和破坏攻击的能力；相反，它们表现出相当程度的脆弱性。物联网脆弱的安全表现为隐蔽通道的构建提供了可能。

在物联网隐蔽通道的构建方面，Velinov 等[17]将消息队列遥测传输（MQTT, message queuing telemetry transport）协议应用于物联网中，描述了 7 个直接和 6 个间接的隐蔽通道，并使用网络信息隐藏技术对它们进行评估和分类。信息隐藏技术被广泛用于构建物联网隐蔽通道[44]，如 Mileva 等[45]提出了一种利用约束应用协议（COAP, constrained application protocol）构建的物联网隐蔽通道。COAP 是一种用于约束设备和网络的专用 Web 传输协议，通过将秘密数据隐藏在 COAP 的协议数据单元（PDU, protocol data unit）中实现隐蔽通信。Tan 等[46]提出了一种物联网时间隐蔽通道的系统模型（如图 1 所示），并分析了基于分组间时延的时间隐蔽通道在 4G/5G 网络中的应用。Ho 等[47]将序贯概率比检验（SPRT, sequential probability ratio test）应用于物联网中的隐蔽通道，能够在隐蔽通道中实现快速的编码和解码。物联网应用程序通过连接各种其他未连接的服务来授权用户。这些应用程序由外部信息源触发，以在外部信息接收器上执行操作。流行的物联网应用平台，包括 IFTTT、Zapier 和 Microsoft Flow 都容易受到恶意 Applet 制造商的攻击，包括过滤私人照片、泄露用户位置和窃听用户输入语音控制助理的消息等隐蔽通道攻击[48]。

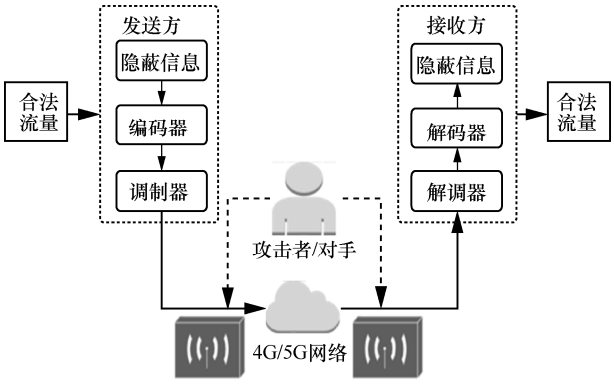


图 1 物联网时间隐蔽通道系统模型

2.2 移动通信网络隐蔽通道构建

在移动通信网络中，为了保护用户隐私，许多智能手机系统采用了一种基于许可的机制，用户可以在安装手机应用程序之前评估来自该应用程序的隐私信息请求的风险。然而，基于许可的机制很容易受到应用程序的合谋攻击，因为 2 个独立的应用程序可以建立一个隐蔽通道，并使用它来泄露机密信息。Qi 等[49]在安卓智能手机上构建了基于用户行为的隐蔽通道，如图 2 所示，该隐蔽通道不易被检测。

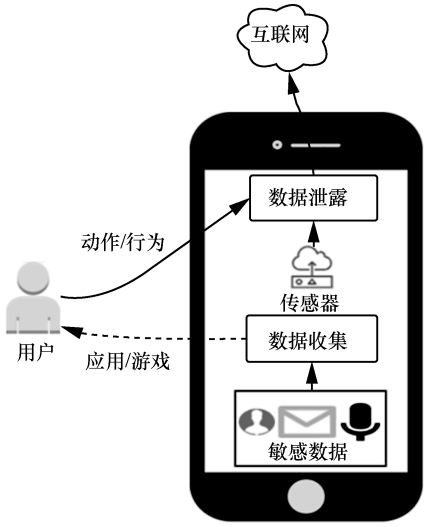


图 2　基于用户行为的智能手机隐蔽通道

Aloraini 等[20]提出了一种智能手机网络隐蔽通道，通过接收的蜂窝语音流来研究智能手机中的应用程序泄露信息的能力。Zhang 等[24]通过延迟或延长语音流量的静音周期来调节隐蔽信息，使用灰度编码对隐藏消息进行编码，能够实现良好的隐蔽性和稳健性。Zhang 等[36]提出了一种适应移动网络环境的双向 VoLTE 隐蔽通道，它包括发送方到接收方的时间隐蔽通道，以及一个反向存储隐蔽通道。其中，时间隐蔽通道通过在静默期内主动丢弃分组来调制隐蔽消息，反向存储隐蔽通道将秘密消息作为反馈信息隐藏到实时传输控制协议（RTCP, real-time transport control protocol）的反馈控制信息字段中。该方案不仅可以保持语音质量，也能同时保持隐蔽通道的抗检测性和稳健性。Tan 等[50]提出了一种基于视频流的时间隐蔽通道，通过故意丢弃视频数据包来调制隐蔽消息，基于二维映射矩阵将隐蔽消息块映射为丢包序列号，接收方检索丢失数据包的序列号，并将其翻译成隐藏的信息。Novak 等[51]设计了一种移动设备信息泄露软件，通过声音或光线等媒介构建隐蔽通道，能够绕过系统的特权升级和信息泄露的防御机制。Schulz 等[52]在智能手机中构建了一个隐蔽通道，该隐蔽通道先对 Wi-Fi 帧进行预过滤，然后在 2 个设备之间秘密交换隐蔽信息。

Android 等移动操作系统通过限制设备内应用程序之间的通信来提供数据保护机制。然而，恶意应用仍然可以通过各种方式克服这些限制，如利用系统中的软件漏洞或使用隐蔽通道进行数据传输。在 Android 系统中，电池和电话等资源可以用于隐蔽通信，恶意应用程序利用这些资源可以实现高容量的隐蔽数据传输[53-54]。

基于物理行为的隐蔽通道可以通过改变应用程序的内部状态或用户的行为来实现信息泄露。Wu 等[55]使用全球定位系统（GPS, global positioning system）欺骗技术设计了一种基于物理行为的智能移动设备隐蔽通道，该设计充分考虑了非握手、离线传输和低怀疑等特性，具有良好的隐蔽性。

2.3　云环境下隐蔽通道构建

云环境下的隐藏通道规避了云中多方之间的隔离机制。在不同虚拟机上的非特权用户程序可以通过隐蔽通道传输隐蔽信息。

Clementine 等[4]通过共享处理器的最后一级缓存在不同内核上的虚拟机之间建立了更快速的隐蔽通道 C5，C5 能够通过同一处理器的任一内核传输硬件上的信息。内存重复数据删除技术已被广泛应用于各种虚拟化管理程序。虽然这种技术提高了内存效率，但它对系统安全性有影响。内存重复删除通常使用写时复制技术的一种变体来实现，与写入非共享页面相比，写入共享页面会导致更长的访问时延[18]。基于此特性，Rong 等[19]设计了一种高效、可靠的基于内存重复数据删除的云隐蔽通道（CCCMD, cloud covert channel based on memory deduplication）协议，建立了一个名为 WindTalker 的隐蔽通道模型，在低误码率的情况下，WindTalker 具有更好的性能，并能实现在噪声环境下的合理自适应传输速度。

Maurice 等[56]基于无线传输协议建立了一个稳健的高容量隐蔽通道，该隐蔽通道能够实现错误纠正，并可以在 2 个虚拟机之间建立安全外壳（SSH, secure shell）连接。Sullivan 等[57]提出了一种基于处理器内存顺序缓冲（MOB, memory order buffer）的微体系结构时间隐蔽通道。Wu 等[58-59]利用内存总线作为隐蔽通道传输介质，在云环境中实现了高带宽和可靠的隐蔽数据传输。Lipinski 等[60]提出了一种名为 CloudSteg 的隐写方法，该方法基于驻留在同一物理机器上的 2 个云实例之间的硬盘争用，创建一个隐蔽通道。跨虚拟机攻击使恶意租户能够利用各种形式的隐蔽通道窃取受害者的敏感信息，如图 3 所示。Tahir 等[61]提出了一个跨虚拟网络的时间隐蔽通道，它依赖于数据中心网络的底层共享网络资源在逻辑隔离的虚拟网络之间传输数据，该隐蔽通道有很大的隐蔽容量。

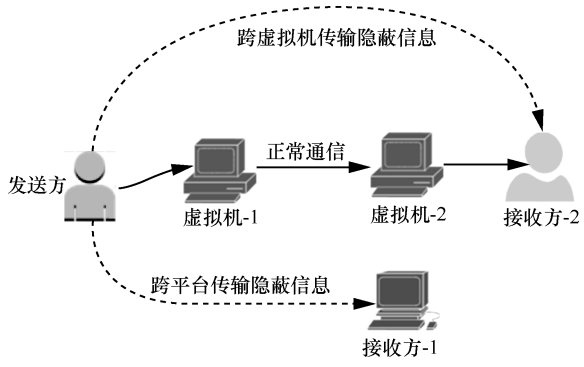


图 3　跨虚拟机隐蔽通道示例

随着云现场可编程门阵列（FPGA, field programmable gate array）的广泛应用，云计算基础设施中的 FPGA 可以通过转换通道发生信息泄露。云 FPGA 利用用户之间 FPGA 资源的临时共享，使一个用户产生的热量可以被后来使用同一 FPGA 的另一个用户观察到，其通过简单的开关键控（OOK, on-off keying）可以实现隐蔽的数据传输，并且并行使用多个 FPGA 板可以显著提高数据吞吐量[62]。

2.4　Air-gap 系统隐蔽通道构建

系统的物理实现（如电磁铁）产生的电磁信号、功率、声音和温度等也可以作为信息传输的介质，利用这些通信介质，攻击者可以设计间谍软件向外部传输敏感数据，给系统带来安全威胁。

在 Air-gap 系统隐蔽通道的构建方面，Guri 等[21]通过调节 CPU 内核上的工作负载来控制计算机发出的磁场，利用磁信号编码并传输隐蔽信息。对于多核计算平台，即使是基于专用核的强大隔离技术也可以被热通道绕过，即使在系统具有很强的时间和空间分块能力的情况下，处理器的内核温度也可以作为一个隐蔽通道[63]。Guri 等[64]通过使用计算机的热发射和内置的热传感器来创建一个隐蔽通道以弥合相邻受损计算机之间的气隙。该方法支持双向通信，并且它不需要额外的专用外围硬件。Krishnamurthy 等[65]利用网络物理系统（CPS, cyber physical system）中控制器的动态特性和闭环特性，将模拟信号作为隐蔽通道发送到远程接收器，在程序逻辑控制器（PLC, programmable logic controller）的驱动下，实现了 2 个反馈回路。

2.5　其他网络隐蔽通道构建

区块链作为一种新型的分散式公共网络，它的开放性和强大的抗篡改能力使其成为构建隐蔽通道的天然平台。

为在区块链上实现隐蔽通信，李彦峰等[40]构建了一种区块链网络隐蔽通道模型，并研究了其抗干扰、抗篡改等特性。Partala 等[66]提出了区块链隐蔽通道（BLOCCE, blockchain covert channel），该方案将区块链使用的加密哈希函数建模为一个随机预言机，并制定一个简化的理想区块链，使用提交给区块链的支付为每个块嵌入一个比特的隐蔽信息，以实现可靠的隐蔽通道。Tian 等[67] 提出了 DLchain，该方案使用动态标签代替固定标签，并设计了一种基于实际事务数据统计分布的动态标签生成算法，以保证动态标签的隐蔽性。DLchain 具有不可检测性、抗跟踪性和稳健性强等特点。Gao 等[68]利用窃密技术设计了一种区块链隐蔽数据传输方案，在开放网络条件下，该隐蔽传输机制具有很强的隐蔽性和兼容性，可以实际应用于许多流行的区块链系统。

车载自组网使高速车辆能够相互通信，也为隐蔽通道提供了新的通信介质。Taheri 等[69]在 VANET 中开发了一种混合（时间和存储）隐蔽通道，通过改变服务和控制包的时间模式来传输隐蔽消息，同时设计了一种用于隐蔽数据嵌入的编码算法，该编码算法具有较高的嵌入容量。

综合上述通信环境下隐蔽通道的构建方法特点，可将其划分成基于信息编解码、基于时间模式调节、基于协议扩展填充、基于恶意软件行为、基于流媒体调制、基于系统资源共享和基于物理介质调节七大类方法，如表 1 所示。表 1 中，在物联网环境下，主流的隐蔽通道构建方法包括基于信息编解码和基于协议扩展填充的方法；在移动通信网络中，主流的隐蔽通道构建方法包括基于流媒体调制和基于信息编解码的方法；在云环境下，主流的隐蔽通道构建方法为基于系统资源共享的方法；在 Air-gap 系统中，主流的隐蔽通道构建方法为基于物理介质调节的方法；在车载自组网中，主流的隐蔽通道构建方法包括基于信息编解码和基于时间模式调节的方法。表 2 展示了隐蔽通道构建方法的细粒度对比分析结果，主要从隐蔽通道的共享资源、容量、稳健性、抗检测性和优缺点 6 个方面进行比较，通过对现有研究的综合分析，将稳健性和抗检测性都分为弱、较弱、较强和强 4 个等级。稳健性等级主要是基于文献中给出的误码率来划分的，具体地，误码率小于 5%定为强，5%～10%定为较强，10%～20%定为较弱，其余定为弱，对于部分文献的构建方法，也会考虑隐蔽通道在噪声环境下的丢

包率（抗噪性）变化，对稳健性综合定级。抗检测性主要是基于文献中给出的检测精度结果来划分的，具体地，检测精度小于 50%定为强，50%～65%定为较强，65%～80%定为较弱，其余为定为弱，对于部分文献的检测方法，也会结合检测开销对抗检测性综合定级。

表 1　　各类隐蔽通道构建方法特点

构建方法类别	文献	隐蔽通道类型	应用环境	特点
基于信息编解码	文献[24,47,69]	存储隐蔽通道	物联网 移动通信网络 车载自组网	发送方对隐蔽信息进行编码，接收方对隐蔽信息同步解码，获取隐蔽信息，通常隐蔽容量的大小取决于编解码速度
基于时间模式调节	文献[46,69]	时间隐蔽通道	物联网 车载自组网	通过调节数据包的发送时间模式传输隐蔽信息，如包间间隔、包间时延等，通常具有较强的抗检测性，不过噪声等干扰易对该类隐蔽通道造成影响
基于协议扩展填充	文献[17,36,45]	存储隐蔽通道	物联网 移动通信网络	通过扩展协议、填充空余字段等来隐藏隐蔽信息，该方法具有可拓展性，一般可以构建多个隐蔽通道，但隐蔽容量受限于具体协议的填充字段
基于恶意软件行为	文献[48-49]	行为隐蔽通道	物联网 移动通信网络	恶意软件基于系统漏洞、用户行为等特性或行为特征，传输隐蔽信息，通常具有较强的抗检测性
基于流媒体调制	文献[20,24,36,50]	时间隐蔽通道 存储隐蔽通道	移动通信网络	利用蜂窝语音流、视频流等流媒体作为通信载体，传输隐蔽信息，但是隐蔽通道容量往往较小
基于系统资源共享	文献[4,19,56-60]	存储隐蔽通道	云环境	通过共享或修改内存、缓存等系统资源实现隐蔽通信，通常能实现较大的隐蔽容量
基于物理介质调节	文献[21,64-65]	存储隐蔽通道	Air-gap 系统	主要基于电磁信号、功率和温度等共享资源构建，往往隐蔽容量很小，且通信强度对距离存在较强的依赖性

表 2　　隐蔽通道构建方法细粒度对比分析

方法类别	构建方法	共享资源（通信环境）	容量	稳健性	抗检测性	优点	缺点
基于信息编解码	基于数据包顺序编解码[23]	数据包（传统网络）	1.2 Mbit/s	强	弱	数据包合理排序可以实现大容量和低错误率的隐蔽传输	传输数据量越大越容易被检测，且开销大
	编解码 SPRT 传感器信号[47]	SPRT 传感器（物联网）	4 097.5～9 061.67 bit/s	强	—	隐蔽通道容量大，编/解码速度快	检测开销大
基于时间模式调节	基于包间时延[10]	包间时延（传统网络）	—	较强	较强	稳健性较强，丢包率较低	没有充分研究隐蔽通道的容量
基于协议扩展填充	基于信息隐藏[17]	MQTT 协议（物联网）	1～1 048 560 Tbit/s	较强	较强	设计隐蔽通道种类较多，可扩展到其他类似协议中构建	当网络时延增加时，误码率会增加
基于恶意软件行为	基于用户行为[49]	智能手机（移动通信网络）	1～1.67 bit/s	较强	较强	有较强的抗检测性	检测开销大
基于流媒体调制	调制蜂窝语音流[20]	蜂窝语音流（移动通信网络）	13 bit/s	强	—	有较大的隐蔽容量且稳健性强	没有充分研究隐蔽通道的抗检测性
基于系统资源共享	基于硬件随机数生成器[3]	硬件随机数生成器（操作系统）	7～200 kbit/s	强	—	隐蔽通道容量大、误差小，不易产生噪声	当木马和间谍进程同时执行时，隐蔽容量会减少
	基于分支预测器[5]	分支预测器（操作系统）	—	较强	—	隐蔽通道容量大、稳健且抗噪声	没有充分研究隐蔽通道的抗检测性
	基于内存重复删除[18]	内存（云环境）	1.24～90 bit/s	—	—	当系统工作量增加时，隐蔽通道容量下降不明显	选择构建隐蔽通道的内存越大，越容易被检测
	基于缓存[56]	缓存（云环境）	34.27～45.09 kbit/s	强	—	容量大且稳健性强，错误传输率极低，且有较强的抗噪性	通信端点设计不支持分组交换，不能同时拥有多个套接字
	基于内存总线[58]	内存总线（云环境）	至少 100 bit/s	较强	—	隐蔽通道容量大且可靠	由于内存访问的不确定性，使检测开销大；抗噪性较差，当噪声严重时，误码率会升高
	基于云实例硬盘争用[60]	云实例（云环境）	0.1 bit/s	较强	较强	因不知隐蔽传输位何时启动，故有较强的抗检测性和稳健性	隐蔽容量较小，检测开销大，当云实例频繁访问硬盘时，误码率会升高
基于物理介质调节	调节磁信号[21]	磁信号（Air-gap）	至多 5 bit/s	较弱	—	当无线通信距离较近时有较大的传输速率，且误码率低	随着无线通信距离增大，误码率会增加

3 隐蔽通道的检测方法

3.1 基于统计的检测方法

基于统计的检测方法通常利用统计学的特征规律来分析合法数据流和隐蔽数据流的分布差异或异常，从而检测出非法数据流。

Cabuk 等[13]采用数据流变化的统计特征规律作为隐蔽通道的检测指标，量化了网络数据包间隔时间的标准差的变化。Archibald 等[43]提出了一种基于韦尔奇 t 检验的形状检测方法，该方法具有相对较低的计算成本，而且韦尔奇 t 检验在检测基于时延的时间隐蔽通道方面优于修正条件熵检验。Nafea 等[70]提出了一种包含连续数据监控、阈值等元素的新框架和一种基于统计测度的隐蔽数据泄露检测模型，特别是针对非线性混沌数据，该模型能够更有效地提供具有容差/阈值的结果。Rezaei 等[71]提出了一种基于网络流量 IPD 分布的时间隐蔽通道实时检测方法，并利用 3 种不同的非参数统计测试，为合法和隐蔽网络流量 IPD 生成不同的统计测试分数，该方法能够可靠地检测出实时网络流量中的隐蔽通道。

基于统计的检测方法主要是通过统计学分析隐蔽通道的形状或规律指标，以检测出隐蔽通道。表 3 展示了部分基于统计的检测效果，分别从隐蔽通道类型、准确率、是否能盲检、形状指标和规律指标 5 个方面对检测方法进行对比分析。表 3 中，Jitterbug 是一种典型的基于时延的时间隐蔽通道，以被动的方式提供可靠的隐蔽通信。TR-CTC-HTTP 和 TR-CTC-SSH 分别是基于时间重放的时间隐蔽通道（TR-CTC, time replay covert timing channel）中的 HTTP 和 SSH 流量，MB-CTC-HTTP 和 MB-CTC-SSH 分别是基于模型的时间隐蔽通道（MB-CTC, model-based covert timing channel）中的 HTTP 流量和 SSH 流量。

表 3 基于统计的检测效果

检测方法	隐蔽通道类型	准确率	是否能盲检	形状指标	规律指标
K-S 检验[43]	Jitterbug	66%	是	√	—
韦尔奇 t 检验[43]	Jitterbug	86%	是	√	—
	TR-CTC-HTTP	67%	是	√	—
	TR-CTC-SSH	56%	是	√	—
	MB-CTC-HTTP	92%	是	√	—
	MB-CTC-SSH	95%	是	√	—
规律性检测[43]	TR-CTC-HTTP	60%	是	—	—
	TR-CTC-SSH	69%	是	—	—
	MB-CTC-HTTP	60%	是	—	—
	MB-CTC-SSH	91%	是	—	—

3.2 基于机器学习的检测方法

目前，机器学习方法被广泛应用于隐蔽通道的检测研究中，主要通过发现网络流量的规律或异常来检测隐蔽通道。通过提取正常流量和隐蔽流量的特征，对网络流量进行分类识别，从而实现隐蔽通道的检测。基于机器学习的时间隐蔽通道检测的复杂性取决于流量样本的可用性，以及攻击者改变隐蔽通道参数的可能性[72]。

Mohammed 等[73]基于随机森林算法对物联网设备在不同操作模式下的功率分布数据进行分类，以检测隐蔽通道和功率耗尽攻击。该算法有良好的检测结果，分类准确率为 95.5%。Vzquez 等[74]从统计的角度挖掘了包含时间隐蔽通道的数据流的形状，使用监督和非监督的机器学习算法，揭示了构建检测方法的推荐特征。Shrestha 等[75]提出了一种基于支持向量机（SVM, support vector machine）的隐蔽通道检测框架，该框架将从网络流量中提取的指纹分为显性和隐性，有较强的盲检能力和稳健性，即使是在隐藏消息大小减小的情况下，也有良好的检测效果。Wang 等[76]提出了一种基于机器学习的域名生成算法（DGA, domain generation algorithm）和域名系统（DNS, domain name system）隐蔽通道检测系统，其利用改进的 TF-IDF（term frequency-inverse document frequency）、特异度评分等算法检测恶意域名，有良好的检测效果。Darwish 等[77]提出了一种基于层次结构的时间隐蔽通道检测模型。该模型的检测过程包括：在到达时间流的连续层次上进行统计分析，创建合法通道和隐蔽通道的数据集实例，构建 5 层神经网络分类模型对隐蔽通道进行识别。与基于支持向量机的检测模型相比，该深度神经网络模型获得了更好的精度水平，模型训练时间明显缩短。Han 等[78]提出了一种基于 K 近邻（KNN, k-nearest neighbor）的时间隐蔽通道检测方法。该方法使用与时间间隔和有效载荷长度相关的一系列统计数据作为特征来训练模型，检测精度为 0.96。Alam 等[79]通过提取流量特征来构建签名，并通过统计测试分数来分析数据的分布差异，然后将上下文添加到签名中，最

后构建支持向量机模型，对云中的隐蔽流量进行分类。该方法的检测成本低且准确率较高。

基于机器学习的检测方法，主要通过机器学习算法分析流量数据的特征以检测出隐蔽通道，该类检测方法的评估指标与传统机器学习算法类似，包括召回率、精确率、准确率和 F1 指标，表 4 展示了部分基于机器学习的检测效果。表 4 中所有检测方法均是针对时间隐蔽通道进行检测的方法，其中，决策树[74]的检测结果是该类方法的最佳测试结果，支持向量机[75]的结果是 ON-OFF 隐蔽通道（2 000 个样本）的最佳检测结果（根据混淆矩阵计算得出）。

表 4　　基于机器学习的检测效果

检测方法	召回率	精确率	准确率	F1 指标
决策树[74]	95.17%	96.01%	99.71%	—
支持向量机[75]	97%	100%	98.5%	98.48%
神经网络[77]	97.56%	96.75%	97%	97.15%
支持向量机[78]	85%	88%	—	86%
KNN[78]	96%	96%	—	96%
朴素贝叶斯[78]	88%	89%	—	88%
Logistic 回归[78]	91%	91%	—	90%

3.3　基于信息论的检测方法

基于信息论的检测方法通常是比较合法流量和隐蔽流量之间的熵的差异。当将熵作为检测指标时，主要利用熵来衡量 IPD 分布的随机性。隐蔽流量往往比合法的显性流量有更高的熵水平[70]。

针对利用 TCP/IP 网络数据包中的 6 位 TCP 标志头部传输秘密消息的存储隐蔽通道，Chow 等[41]提出了一种基于 K-L 散度的检测方法，使用 K-L 散度来描述隐蔽流量与合法流量之间的不规则性，同时使用了不同的数据处理方法：一种方法是将一对 IP 地址的所有数据包总结为一个流，另一种方法是使用在这样一个流上的滑动窗口来生成多帧数据包。在检测过程中，计算每个唯一 IP 对的网络流量的 TCP 标志频率分布，K-L 散度可以揭示不同频率分布与这种正态分布的差异，利用这种差异可以区分出合法流量和隐蔽流量。

针对 Jitterbug，Wang 等[80]提出了一种基于部分熵检验的检测方法。该方法采用无训练样本的固定箱策略来获得箱的分布特征，计算几组部分连续箱的一阶熵，并利用加权均值计算最终熵值，以区分 Jitterbug 和合法流量。该方法有较好的检测效果，且受网络抖动的影响较小。针对 IP 时间隐蔽通道（IPCTC, IP covert timing channel）、基于重传的时间隐蔽通道（TRCTC, time replay covert timing channel）和 Jitterbug 隐蔽通道，Gianvecchio 等[81]和张宇飞等[82]分别提出了基于修正条件熵和基于差分信息熵的检测方法。其中，Gianvecchio 等[81]对 HTTP 和 SSH 中的上述时间隐蔽通道有良好的检测结果，张宇飞等[82]也能有效检测出上述 3 种时间隐蔽通道。

针对利用分组数据汇聚协议（PDCP, packet data convergence protocol）和无线链路控制层（RLC, radio link control）的序列号（SN, sequence number）字段构建的存储隐蔽通道，Wang 等[83]提出了一种基于熵的 CSC 检测方法。该方法对 PDCP 和 RLC 层的 SN 中的隐藏信息敏感，有很好的检测效果，并且可以实时在线和离线存储检测。Darwish 等[84]利用基于 MapReduce 技术的层次熵算法检测大数据中的时间隐蔽通道，该方法的检测速度很快，随着时延的增加，检测精度和准确率也会明显提高。基于信息论的检测方法主要是基于熵理论对隐蔽通道进行识别。表 5 展示了部分基于信息论的检测效果，分别从隐蔽通道类型、真阳率、假阳率和是否能盲检 4 个方面对检测方法进行比较。表 5 中，基于 K-L 散度[41]、基于修正条件熵[81,83]和基于香农熵[83]的真阳率及假阳率均是文献中所给出的最优检测结果。

表 5　　基于信息论的检测效果

检测方法	隐蔽通道类型	真阳率	假阳率	是否能盲检
基于 K-L 散度[41]	存储隐蔽通道	100%	0	否
基于修正条件熵[81]	时间隐蔽通道	100%	1%	是
基于修正条件熵[83]	存储隐蔽通道	97%	1%	是
基于香农熵[83]	存储隐蔽通道	85%	2%	是

3.4　基于信息流分析的检测方法

在基于信息流分析的检测方面，早期研究主要通过分析系统的无干扰性来发现隐蔽通道。无干扰性是指当系统中低安全级数据的输出不对高安全级的信息产生干扰时，系统是安全的。在基于无干扰性分析系统安全性时，可以将隐蔽通道的概率特性[85]和时间特性[86]加入信息流安全属性当中，通过分析信息流安全属性来检测隐蔽通道。

针对 Applet 对物联网应用平台发起的隐蔽通

道攻击，Bastys 等[48]开发了一个用于物联网应用程序中信息流跟踪的框架。该框架对 Applet 的反应性和计时行为进行建模，同时有效地捕捉到了由 applet 输出引起的攻击者行为的差异。Song 等[87]提出了一种利用信息流图（IFG, information flow graph）的图结构检测存储隐藏通道的技术。IFG 可以为隐蔽通道检测提供系统的信息流。通过搜索 IFG 的路径，可以得到操作序列，有助于分析者发现隐蔽通道。Wu 等[88]提出了一种基于有向信息流图的源代码分析方法。该方法将整个系统划分为若干独立的模块并分别进行分析。从源代码中找出所有共享变量及其调用函数，并将其建模为有向信息流图。当信息流分支在外部接口可见且可修改时，则存在一个潜在的隐蔽通道。该方案在 Linux 内核源代码中识别了 30 多个隐蔽通道。基于信息流分析的检测方法通过分析系统中的信息流，以识别潜在的隐蔽通道。表 6 分别从隐蔽通道类型、是否能盲检和优缺点 4 个方面对基于信息流分析的检测方法进行定性分析。其中，伪通信路径会影响检测的效率和效果。

3.5 其他检测方法

针对利用共享硬件资源等技术构建的隐蔽通道，还没有形成统一的分析检测方法，通常是针对某一隐蔽通道的具体构建技术进行分析，建立检测机制。如云环境中基于缓存的隐蔽通道，因为其构建技术不同，不能用统一的方法进行检测。

针对传统网络隐蔽通道，Wendzel 等[89]提出了一种不受协议约束的消息排序通道检测方法。该方法基于一个修正的可压缩性分数，分析了消息排序通道的可检测性，结果表明，消息排序通道的检测依赖于所使用的协议数据单元的数量。

针对云环境中的隐蔽通道威胁，Liu 等[90]实现了一种名为观测器的实时隐蔽通道检测系统。与其他检测系统不同，该观测器不需要历史数据来构建模型，观察者能够以较低的时延和开销来检测隐蔽通道。Wang 等[91]提出了一种隐蔽通道自动检测方法，设计了一种从行为角度准确定位和分析恶意隐蔽通道的全局检测方法。与目前流行的针对单一隐蔽通道的统计检验方法相比，该方法能够实时识别和检测更多的隐蔽通道。Wu 等[92]提出了一种名为 C2 检测器的隐蔽通道检测系统。C2 检测器包括位于管理程序中的捕获器和基于马尔可夫及贝叶斯检测实现的两阶段合成算法。Betz 等[93]提出了一个名为 C3-Sched 的级联云调度器，该调度器的目的是通过阻止进程交替访问缓存线路来减少客户数据通过 C3 缓存隐蔽通道泄露的威胁，在维护云的性能的同时最小化全局调度开销。Liu[94]提出了一种基于小波的时间隐蔽通道实时检测方法，该方法利用一个安全的虚拟机来模拟易受攻击的虚拟机，它的主要优点是不需要历史流量数据，并且具有较高的检测精度。

基于缓存的隐蔽通道攻击使用高度调优的共享缓存冲突将信息从木马传递给间谍进程。检测这样的攻击是非常具有挑战性的。为检测基于缓存的隐蔽通道攻击，Yan 等[95]提出了一种基于重放混淆的检测方法。该方法基于记录和确定性重放（RnR, record and deterministic replay）技术，在程序的执行被记录下来之后，使用不同的地址到缓存的映射来重新播放，再分析两次运行的缓存丢失率间的时间差。如果该差异是相当大的，并且表现出周期性的模式，则表示存在隐蔽通道攻击。

表 7 展示了各类隐蔽通道检测方法的特点总结，表 8 展示了典型隐蔽通道检测方法的细粒度对比分析。表 8 中，基于机器学习的检测方法[74]的准确率是该类方法的最佳测试准确率；基于支持向量机的检测方法[75]的准确率是 ON-OFF 隐蔽通道（2 000 个样本）的最佳检测准确率，和基于行为分析的检测方法[91]的准确率结果均是根据混淆矩阵计算得出的；基于重放混淆[95]的检测方法的准确率是根据最低误检率计算得出的。云环境下隐蔽通道主要基于 CPU 负载、缓存和共享内存等共享资源实现，鉴于云环境下隐蔽通道共享资源相对统一，表 9 单独展示了部分云环境下隐蔽通道检测方法的细粒度对比，主要从检测方法的检测通道类型、准确率、是否具有自动盲检功能（检测多隐通道）和优缺点 5 个方面对隐蔽通道检测方法进行对比分析。

表 6　　基于信息流分析的检测方法分析

检测方法	隐蔽通道类型	是否能盲检	优点	缺点
基于信息流图[87]	存储隐蔽通道	是	可以完整表示系统的信息流，不需要额外改变参数	信息流图存在伪通信路径问题且检测开销较大
基于有向信息流图[88]	操作系统隐蔽通道	是	该方法检测效率较高且适用于多个系统	当系统源代码量很大时，检测开销也会较大

表 7　　各类隐蔽通道检测方法特点

检测方法类别	隐蔽通道类型	特点
基于统计	时间隐蔽通道 存储隐蔽通道	主要通过统计隐蔽流量的规律性、形状特征或分析特殊字段的属性分布，以识别隐蔽通道
基于机器学习	时间隐蔽通道 存储隐蔽通道	主要通过挖掘隐蔽流量的特征，建立机器学习分类模型来发现隐蔽通道
基于信息论	时间隐蔽通道 存储隐蔽通道	主要基于熵理论来区分隐蔽流量和合法流量
基于信息流分析	时间隐蔽通道 存储隐蔽通道	主要通过分析系统中信息流属性来识别隐蔽通道
其他检测方法	时间隐蔽通道 存储隐蔽通道	主要针对具体通信环境下共享资源的特性进行分析，以检测隐蔽通道

表 8　　典型隐蔽通道检测方法细粒度对比分析

方法类别	检测方法	隐蔽通道类型	准确率	是否能盲检	优点	缺点
基于统计	基于统计[70]	存储隐蔽通道	100%	否	检测精度更高，假阳性率更低	需要较大的计算缓冲区，检测开销大
基于机器学习	基于机器学习[74]	时间隐蔽通道	99.71%	否	检测精度较高，且适合于特征明显的数据集	当网络流量多样化，特征不明显时，检测效果不佳，且不具备盲检能力
	基于支持向量机[75]	时间隐蔽通道	98.5%	是	通用检测框架具有盲检能力	对于网络抖动隐蔽通道的检测性能略差
	基于机器学习[76]	存储隐蔽通道	99.92%	否	算法采用动态识别模型，对于新生成的恶意域名可以更新识别	模型动态调整自己的识别模型对网络特性和需求的影响，检测率可能会降低
基于信息论	基于部分熵[80]	Jitterbug（时间隐蔽通道）	97.4%～100%	否	在网络抖动产生较高误码率的情况下也有较好的检测性能，在较短时间检测窗口下有较高的检测速度	不具备盲检能力
其他检测方法	基于可压缩修正分数[89]	存储隐蔽通道	94.81%	否	检测精度较高	检测依赖于 PDU 的数目，当检测的 PDU 较少时，精度会降低，不具备盲检能力
	基于重放混淆[95]	存储隐蔽通道	99.5%	否	检测方法覆盖率高，结果比较准确	抗噪性较差且检测开销大

表 9　　云环境下隐蔽通道检测方法细粒度对比分析

方法类别	检测方法	隐蔽通道类型	准确率			是否能盲检	优点	缺点
			基于 CPU 负载	基于缓存	基于共享内存			
基于机器学习	基于机器学习[79]	存储隐蔽通道	95.24%	93.33%	97.57%	是	动态检测，具有盲检能力且检测速度较快	若想提高检测覆盖率，会产生较大开销
其他检测方法	C2 检测器[92]	存储隐蔽通道	98%	95%	96.75%	是	具备盲检能力且检测精度较高	采用基于概率的误差校正算法来处理误差,容易影响检测精度
	基于事件关联分析[91]	存储隐蔽通道	97.52%	—	—	是	具备盲检能力且检测精度更高，开销较小	检测依赖共享资源矩阵的构建及属性的选取
	基于小波[94]	时间隐蔽通道	—	—	—	是	可实时动态检测，不依赖历史流量	检测开销较大

4　未来发展趋势

隐蔽通道虽然已有多年的研究历史，但是，国内外关于隐蔽通道的研究还不够深入，尚有很多挑战和研究方向需要继续探讨，主要包括以下几个方面。

1) 隐蔽通道的度量方法

隐蔽通道的度量作为隐蔽通道研究的关键技术，是评估隐蔽通道性能的重要方法。隐蔽通道的

度量指标也是隐蔽通道的构建与检测的重要参考。但是目前关于不同网络及信道环境下的隐蔽通道的度量尚未形成完全统一、合理有效的度量指标。

具体来讲，虽然隐蔽通道的容量和稳健性的度量方法已经相对统一，但是抗检测性、规律性和形状的度量方法尚未统一，主要是因为各类隐蔽通道的差异较大，不仅通信环境不同，隐蔽通道利用的共享资源也不尽相同，而且隐蔽通道的规律性和形状主要是时间隐蔽通道的度量指标，因此，如何用统一的方法对隐蔽通道的抗检测性、规律性和形状进行度量是该领域的一项重要挑战。

针对该挑战，可以从 2 个方面开展更深入的研究：一方面可以将隐蔽通道根据通信环境和共享资源的共性进行分类，针对相同网络环境下共享资源构建的同类隐蔽通道建立统一的度量标准；另一方面可以依赖隐蔽通道的分析与检测技术，结合共享资源的具体特性，增强度量指标的适用性，如在度量抗检测性时，除了评估隐蔽通道的检测效果还可以结合检测开销。

2) 隐蔽通道的构建方法

在隐蔽通道的构建方面，构建一个高容量、稳健且抗检测性强的隐蔽通道一直是研究者的重要目标。现有的隐蔽通道构建技术研究尚难以同时实现多个高性能指标，往往是在各个指标之间进行权衡，比如虽然修改硬件共享资源可以提高隐蔽通道的容量，但是往往会降低抗检测性；若要提高抗检测性，通常要减小容量。因此，如何构建同时具备多个高性能指标的隐蔽通道也是该领域亟须解决的重要问题。

若要提高隐蔽通道性能，一方面，通信双方可以同时利用多种共享资源进行隐蔽通信或者发掘更多高质量的共享资源；另一方面，可以利用网络环境的特点构建高性能隐蔽通道，如利用区块链固有的加密属性，选择高效的信息隐藏或加密算法，提高隐蔽通道的抗检测性。

3) 隐蔽通道的检测方法

在隐蔽通道的检测方面，因为各种隐蔽通道的差异较大，尚未形成相对统一的检测方法，现有的检测技术多为针对某一具体隐蔽通道的特性进行检测。如何实现一个高检测精度、抗噪且具备盲检功能的检测方法仍然是一个艰巨的挑战。

若想克服该挑战，可以针对具有相同或相似的共享资源的隐蔽通道，通过分析该共享资源的特点，建立通用的检测框架。如针对利用网络协议、数据包字段等共享资源建立的时间或存储隐蔽通道，可以基于熵、统计和机器学习方法分析协议或数据包字段的特征检测潜在的隐蔽通道。

5 结束语

隐蔽通道的存在是计算机系统和网络空间面临的一个巨大的安全挑战。随着网络的泛在化及隐蔽通信技术的发展，隐蔽通道给多种网络环境均带来了巨大的安全风险，泛在网络环境下隐蔽通道的研究变得尤为重要。本文首先介绍了泛在网络环境下的隐蔽通道的容量、稳健性、抗检测性、规律性和形状 5 个典型指标的度量方法；其次，系统分析了物联网、移动通信网络、云环境、Air-gap 系统、区块链和车载自组网中隐蔽通道的构建技术，并从共享资源、容量、稳健性、抗检测性、优点和缺点 6 个方面对隐蔽通道构建技术进行了对比分析；再次，从基于统计、基于机器学习、基于信息论、基于信息流分析和其他检测方法 5 个方面对泛在网络环境下隐蔽通道的检测技术进行归纳和多角度对比分析；最后，指出了现有技术的优缺点和存在的问题，针对隐蔽通道的构建和检测技术的不足，给出了具体建议，分析了隐蔽通道的未来研究方向。

参考文献：

[1] 王翀, 王秀利, 吕荫润, 等. 隐蔽信道新型分类方法与威胁限制策略[J]. 软件学报, 2020, 31(1): 228-245.
WANG C, WANG X L, LYU Y R, et al. Categorization of covert channels and its application in threat restriction techniques[J]. Journal of Software, 2020, 31(1): 228-245.

[2] The Department of Defense. Trusted computer system evaluation criteria: DoD 5200.28-STD[S]. 1985.

[3] EVTYUSHKIN D, PONOMAREY D. Covert channels through random number generator: mechanisms, capacity estimation and mitigations[C]//Proceedings of 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 843-857.

[4] CLEMENTINE M, NEUMANN C, HEEN O, et al. C5: cross-cores cache covert channel[C]//Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2015: 46-64.

[5] EVTYUSHKIN D, PONOMAREV D, ABU-GHAZALEH N. Covert channels through branch predictors: a feasibility study[C]//Proceedings of the Fourth Workshop on Hardware and Architectural Support for Security and Privacy, New York: ACM Press, 2015: 1-8.

[6] SHAH G, MOLINA A, BLAZE M. Keyboards and covert channels[C]//Proceedings of the 15th Conference on USENIX Security Symposium. Berkeley: USENIX Association, 2006: 59-75.

[7] 李彦峰, 丁丽萍, 吴敬征, 等. 网络隐蔽信道关键技术研究综述[J]. 软件学报, 2019, 30(8): 2470-2490.
LI Y F, DING L P, WU J Z, et al. Survey on key issues in networks

covert channel[J]. Journal of Software, 2019, 30(8): 2470-2490.

[8] AZADMANESH M, MAHDAVI M, SHAHGHOLI G B. A reliable and efficient micro-protocol for data transmission over an RTP-based covert channel[J]. Multimedia Systems, 2020, 26(2): 173-190.

[9] JOHNSON M, LUTZ P, JOHNSON D. Covert channel using man-in-the-middle over HTTPS[C]//Proceedings of 2016 International Conference on Computational Science and Computational Intelligence (CSCI). Piscataway: IEEE Press, 2016: 917-922.

[10] ZHANG L J, HUANG T W, RASHEED W, et al. An enlarging-the-capacity packet sorting covert channel[J]. IEEE Access, 2019, 7: 145634-145640.

[11] MURDOCH S J, LEWIS S. Embedding covert channels into TCP/IP[C]//Proceedings of the 7th International Information Hiding Workshop. Berlin: Springer, 2005: 247-261.

[12] HOVHANNISYAN H, LU K J, WANG J P. A novel high-speed IP-timing covert channel: design and evaluation[C]//Proceedings of 2015 IEEE International Conference on Communications. Piscataway: IEEE Press, 2015: 7198-7203.

[13] CABUK S, BRODLEY C E, SHIELDS C. IP covert timing channels: design and detection[C]//Proceedings of the 11th ACM Conference on Computer and Communications Security. New York: ACM Press, 2004: 178-187.

[14] ARCHIBALD R, GHOSAL D. Design and analysis of a model-based covert timing channel for skype traffic[C]//Proceedings of 2015 IEEE Conference on Communications and Network Security. Piscataway: IEEE Press, 2015: 236-244.

[15] LIU W W, LIU G J, JI X P, et al. Designing rich-secure network covert timing channels based on nested lattices[J]. KSII Transactions on Internet and Information Systems (TIIS), 2019, 13(4): 1866-1883.

[16] HO J S, YAN S H, ZHOU X B, et al. Covert communications without channel state information at receiver in IoT systems[J]. Internet of Things Journal, 2020, 7(11): 11103-11114.

[17] VELINOV A, MILEVA A, WENDZEL S, et al. Covert channels in the MQTT-based Internet of things[J]. IEEE Access, 2019, 7: 161899-161915.

[18] XIAO J D , ZHANG X , HUANG H , et al. A covert channel construction in a virtualized environment[C]//Proceedings of 2012 ACM conference on Computer and Communications Security. New York: ACM Press, 2012: 1040-1042.

[19] RONG H, WANG H M, LIU J, et al. WindTalker: an efficient and robust protocol of cloud covert channel based on memory deduplication[C]//Proceedings of 2015 IEEE Fifth International Conference on Big Data and Cloud Computing. Piscataway: IEEE Press, 2015: 68-75.

[20] ALORAINI B, JOHNSON D, STACKPOLE B, et al. A new covert channel over cellular voice channel in smartphones[J]. arXiv Preprint, arXiv: 1504.05647, 2015.

[21] GURI M. MAGNETO: covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields[J]. Future Generation Computer Systems, 2021, 115: 115-125.

[22] EPISHKINA A, KOGOS K. Covert channels parameters evaluation using the information theory statements[C]//Proceedings of 2015 5th International Conference on IT Convergence and Security (ICITCS). Piscataway: IEEE Press, 2015: 1-5.

[23] EL-ATAWY A, DUAN Q, AL-SHAER E. A novel class of robust covert channels using out-of-order packets[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(2): 116-129.

[24] ZHANG X S, TAN Y, LIANG C, et al. A covert channel over VoLTE via adjusting silence periods[J]. IEEE Access, 2018, 6: 9292-9302.

[25] WANG L G. Optimal throughput for covert communication over a classical-quantum channel[C]//Proceedings of 2016 IEEE Information Theory Workshop. Piscataway: IEEE Press, 2016: 364-368.

[26] SHEIKHOLESLAMI A, BASH B A, TOWSLEY D, et al. Covert communication over classical-quantum channels[C]//Proceedings of 2016 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2016: 2064-2068.

[27] BULLOCK M S, GAGATSOS C N, GUHA S, et al. Fundamental limits of quantum-secure covert communication over bosonic channels[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(3): 471-482.

[28] BLOCH M R. Covert communication over noisy channels: a resolvability perspective[J]. IEEE Transactions on Information Theory, 2016, 62(5): 2334-2354.

[29] AHMADIPOUR M, SALEHKALAIBAR S, YASSAEE M H, et al. Covert communication over a compound discrete memoryless channel[C]//Proceedings of 2019 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2019: 982-986.

[30] BASH B A, GOECKEL D, TOWSLEY D. Limits of reliable communication with low probability of detection on AWGN channels[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1921-1930.

[31] BENDARY A, ABDELAZIZ A, KOKSAL C E. Achieving positive covert capacity over MIMO AWGN channels[J]. IEEE Journal on Selected Areas in Information Theory, 2021, 2(1):149-162.

[32] TAHMASBI M, SAVARD A, BLOCH M R. Covert capacity of non-coherent Rayleigh-fading channels[J]. IEEE Transactions on Information Theory, 2020, 66(4): 1979-2005.

[33] MCIVER A, MORGAN C. Programming methodology[M]. New York: Springer, 2003: 441-460.

[34] TA H Q, KIM S W. Covert communication under channel uncertainty and noise uncertainty[C]//Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications. Piscataway: IEEE Press, 2019: 1-6.

[35] ZHANG X S, ZHU L H, WANG X M, et al. A packet-reordering covert channel over VoLTE voice and video traffics[J]. Journal of Network and Computer Applications, 2019, 126: 29-38.

[36] ZHANG X S, GUO L H, XUE Y, et al. A two-way VoLTE covert channel with feedback adaptive to mobile network environment[J]. IEEE Access, 2019, 7: 122214-122223.

[37] LIU Y L, GHOSAL D, ARMKNECHT F, et al. Robust and undetectable steganographic timing channels for i.i.d. traffic[C]//Proceedings of the 12th International Conference on Information Hiding. Berlin: Springer, 2010: 193-207.

[38] ARCHIBALD R, GHOSAL D. A covert timing channel based on fountain codes[C]//Proceedings of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE Press, 2012: 970-977.

[39] WANG P，LAN S H，ZHANG J，et al. A hidden channel method based on TCP time stamp option[D]. Nanjing: Nanjing University of Science and Technology, 2015.

[40] 李彦峰, 丁丽萍, 吴敬征, 等. 区块链环境下的新型网络隐蔽信道模型研究[J]. 通信学报, 2019, 40(5): 67-78.
LI Y F, DING L P, WU J Z, et al. Research on a new network covert channel model in blockchain environment[J]. Journal on Communications, 2019, 40(5): 67-78.

[41] CHOW J, LI X Y, MOUNTROUIDOU X. Raising flags: detecting covert storage channels using relative entropy[C]//Proceedings of 2017 IEEE International Conference on Intelligence and Security Informat-

ics. Piscataway: IEEE Press, 2017: 25-30.

[42] CABUK S. Network covert channels: design, analysis, detection, and elimination[D]. Indiana: Purdue University, 2006.

[43] ARCHIBALD R, GHOSAL D. A comparative analysis of detection metrics for covert timing channels[J]. Computers & Security, 2014, 45: 284-292.

[44] CAVIGLIONE L, MERLO A, MIGLIARDI M. Covert channels in IoT deployments through data hiding techniques[C]//Proceedings of 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). Piscataway: IEEE Press, 2018: 559-563.

[45] MILEVA A, VELINOV A, STOJANOV D. New covert channels in Internet of things[C]//Proceedings of the 12th International Conference on Emerging Security Information, Systems and Technologies-SECURWARE 2018. Piscataway: IEEE press, 2018: 30-36.

[46] TAN Y, ZHANG X S, SHARIF K, et al. Covert timing channels for IoT over mobile networks[J]. IEEE Wireless Communications, 2018, 25(6): 38-44.

[47] HO J W. Covert channel establishment through the dynamic adaptation of the sequential probability ratio test to sensor data in IoT[J]. IEEE Access, 2019, 7: 146093-146107.

[48] BASTYS I, BALLIU M, SABELFELD A. If this then what? controlling flows in IoT apps[C]//Proceedings of 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1102-1119.

[49] QI W, DING W F, WANG X Y, et al. Construction and mitigation of user-behavior-based covert channels on smartphones[J]. IEEE Transactions on Mobile Computing, 2018, 17(1): 44-57.

[50] TAN Y A, XU X T, LIANG C, et al. An end-to-end covert channel via packet dropout for mobile networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(5): 1-14.

[51] NOVAK E, TANG Y T, HAO Z J, et al. Physical media covert channels on smart mobile devices[C]//Proceedings of 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing. New York: ACM Press, 2015: 367-378.

[52] SCHULZ M, LINK J, GRINGOLI F, et al. Shadow Wi-Fi: teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over Wi-Fi[C]// Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services. New York: ACM press, 2018: 256-268.

[53] CHANDRA S, LIN Z Q, KUNDU A, et al. Towards a systematic study of the covert channel attacks in smartphones[C]//International Conference on Security and Privacy in Communication Networks, 2015: 427-435.

[54] QI W, XU Y C, DING W F, et al. Privacy leaks when you play games: a novel user-behavior-based covert channel on smartphones[C]//Proceedings of 2015 IEEE 23rd International Conference on Network Protocols. Piscataway: IEEE Press, 2015: 201-211.

[55] WU B, LIU H W. A behavior-based covert channel based on GPS deception for smart mobile devices[C]//Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications. Piscataway: IEEE Press, 2019: 1-6.

[56] MAURICE C, WEBER M, SCHWARZ M, et al. Hello from the other side: SSH over robust cache covert channels in the cloud[C]//Proceedings of Network and Distributed System Security Symposium. Reston: Internet Society, 2017: 8-11.

[57] SULLIVAN D, ARIAS O, MEADE T, et al. Microarchitectural minefields: 4K-aliasing covert channel and multi-tenant detection in Iaas clouds[C]//Proceedings of Network and Distributed Systems Security Symposium. Reston: Internet Society, 2018: doi.org/10.14722/ndss.2018.23231.

[58] WU Z Y, ZHANG X, WANG H N. Whispers in the hyper-space: high-speed covert channel attacks in the cloud[C]//Proceedings of USENIX Security Symposium. Berkeley: USENIX Association, 2012: 159-173.

[59] WU Z Y, XU Z, WANG H N. Whispers in the hyper-space: high-bandwidth and reliable covert channel attacks inside the cloud[J]. IEEE/ACM Transactions on Networking, 2015, 23(2): 603-615.

[60] LIPINSKI B, MAZURCZYK W, SZCZYPIORSKI K. Improving hard disk contention-based covert channel in cloud computing environment[C]//Proceedings of IEEE Security and Privacy Workshops. Piscataway: IEEE Press, 2014: 100-107.

[61] TAHIR R, KHAN M T, GONG X, et al. Sneak-Peek: high speed covert channels in data center networks[C]//Proceedings of the 35th Annual IEEE International Conference on Computer Communications. Piscataway: IEEE Press, 2016: 1-9.

[62] TIAN S, SZEFER J. Temporal thermal covert channels in cloud FPGAs[C]//Proceedings of 2019 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays. New York: ACM Press, 2019: 298-303.

[63] MASTI R J, RAI D, RANGANATHAN A, et al. Thermal covert channels on multi-core platforms[C]//Proceedings of the 24th USENIX Security Symposium. Berkeley: USENIX Association, 2015: 865-880.

[64] GURI M, MONITZ M, MIRSKI Y, et al. BitWhisper: covert signaling channel between air-gapped computers using thermal manipulations[C]//Proceedings of 2015 IEEE 28th Computer Security Foundations Symposium. Piscataway: IEEE Press, 2015: 276-289.

[65] KRISHNAMURTHY P, KHORRAMI F, KARRI R, et al. Process-aware covert channels using physical instrumentation in cyber-physical systems[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(11): 2761-2771.

[66] PARTALA J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18.

[67] TIAN J, GOU G P, LIU C, et al. DLchain: a covert channel over blockchain based on dynamic labels[C]//Information and Communications Security. Berlin: Springer, 2020: 814-830.

[68] GAO F, ZHU L H, GAI K K, et al. Achieving a covert channel over an open blockchain network[J]. IEEE Network, 2020, 34(2): 6-13.

[69] TAHERI S, MAHDAVI M, MOGHIM N. A dynamic timing-storage covert channel in vehicular ad hoc networks[J]. Telecommunication Systems, 2018, 69(4): 415-429.

[70] NAFEA H, KIFAYAT K, SHI Q, et al. Efficient non-linear covert channel detection in TCP data streams[J]. IEEE Access, 2019, 8: 1680-1690.

[71] REZAEI F, HEMPEL M, SHARIF H. Towards a reliable detection of covert timing channels over real-time network traffic[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(3): 249-264.

[72] EPISHKINA A, FINOSHIN M, KOGOS K, et al. Timing covert channels detection cases via machine learning[C]//Proceedings of 2019 European Intelligence and Security Informatics Conference (EISIC). Piscataway: IEEE Press, 2019: 139.

[73] MOHAMMED H, ODETOLA T A, HASAN S R, et al. (HIADIoT): hardware intrinsic attack detection in Internet of things; leveraging power profiling[C]//Proceedings of 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems. Piscataway: IEEE Press, 2019: 852-855.

[74] VZQUEZ F I, ANNESSI R, ZSEBY T. Analytic study of features for the detection of covert timing channels in network traffic[J]. Journal of Cyber Security and Mobility, 2017, 6(3): 225-270.

[75] SHRESTHA P L, HEMPEL M, REZAEI F, et al. A support vector machine-based framework for detection of covert timing channels[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 274-283.

[76] WANG Z Q, DONG H Y, CHI Y P, et al. DGA and DNS covert channel detection system based on machine learning[C]//Proceedings of the 3rd International Conference on Computer Science and Application Engineering. New York: ACM Press, 2019: 1-5.

[77] DARWISH O, AL-FUQAHA A, BEN-BRAHIM G, et al. Using hierarchical statistical analysis and deep neural networks to detect covert timing channels[J]. Applied Soft Computing, 2019, 82: 105546.

[78] HAN J X, HUANG C, SHI F, et al. Covert timing channel detection method based on time interval and payload length analysis[J]. Computers & Security, 2020, 97: 101952.

[79] ALAM M, SETHI S. Detection of information leakage in cloud[J]. arXiv Preprint, arXiv: 1504.03539, 2015.

[80] WANG H, LIU G J, LIU W W, et al. Detection of jitterbug covert channel based on partial entropy test[J]. Lecture Notes in Computer Science, 2017, 10603: 357-368.

[81] GIANVECCHIO S, WANG H N. An entropy-based approach to detecting covert timing channels[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(6): 785-797.

[82] 张宇飞, 沈瑶, 杨威, 等. 差分信息熵的网络时序型隐蔽信道检测[J]. 软件学报, 2019, 30(9): 2733-2759.
ZHANG Y F, SHEN Y, YANG W, et al. Detecting covert timing channels based on difference entropy[J]. Journal of Software, 2019, 30(9): 2733-2759.

[83] WANG Z K, HUANG L S, YANG W, et al. An entropy-based method for detection of covert channels over LTE[C]//Proceedings of 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design. Piscataway: IEEE Press, 2018: 872-877.

[84] DARWISH O, AL-FUQAHA A, BEN-BRAHIM G, et al. Using MapReduce and hierarchical entropy analysis to speed-up the detection of covert timing channels[C]//Proceedings of 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). Piscataway: IEEE Press, 2017: 1102-1107.

[85] ALDINI A, BRAVETTI M, GORRIERI R. A process-algebraic approach for the analysis of probabilistic noninterference[J]. Journal of Computer Security, 2004, 12(2):191-245.

[86] FOCARDI R, GORRIERI R, MARTINELLI F. Real-time information flow analysis[J]. IEEE Journal on Selected Areas in Communications, 2003, 21(1): 20-35.

[87] SONG X M, JU S G, WANG C D, et al. Information flow graph: an approach to identifying covert storage channels[C]//International Conference on Trusted Systems. Berlin: Springer, 2010: 87-97.

[88] WU J Z, DING L P, WANG Y J, et al. A practical covert channel identification approach in source code based on directed information flow graph[C]//Proceedings of 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement. Piscataway: IEEE Press, 2011: 98-107.

[89] WENDZEL S. Protocol-independent detection of “messaging ordering” network covert channels[C]//Proceedings of the 14th International Conference on Availability, Reliability and Security(ARES’19). New York: ACM Press, 2019: 1-8.

[90] LIU A Y, CHEN J, YANG L. Real-time detection of covert channels in highly virtualized environments[C]//Critical Infrastructure Protection V. Berlin: Springer, 2011: 151-164.

[91] WANG L N, LIU W J, KUMAR N, et al. A novel covert channel detection method in cloud based on XSRM and improved event association algorithm[J]. Security and Communication Networks, 2016, 9(16): 3543-3557.

[92] WU J Z, DING L P, WU Y J, et al. C2Detector: a covert channel detection framework in cloud computing[J]. Security and Communication Networks, 2014, 7(3): 544-557.

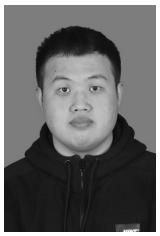
[93] BETZ J, WESTHOFF D. C3-Sched—a cache covert channel robust cloud computing scheduler[C]//Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014). Piscataway: IEEE Press, 2014: 54-60.

[94] LIU A Y, CHEN J, WECHSLER H. Real-time covert timing channel detection in networked virtual environments[C]//IFIP International Conference on Digital Forensics. Berlin: Springer, 2013: 273-288.

[95] YAN M J, SHALABI Y, TORRELLAS J. ReplayConfusion: detecting cache-based covert channel attacks using record and replay[C]//Proceedings of 2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). Piscataway: IEEE Press, 2016: 1-14.

[作者简介]

李凤华（1966− ），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、大数据安全与隐私保护、密码工程。



李超洋（1996− ），男，河北唐山人，中国科学院信息工程研究所硕士生，主要研究方向为网络与系统安全。

郭超（1987− ），女，江西九江人，博士，北京电子科技学院讲师，主要研究方向为空间信息网络、通信安全、传输控制。

李子孚（1992− ），女，内蒙古赤峰人，博士，中国科学院信息工程研究所工程师，主要研究方向为网络与系统安全、访问控制。

房梁（1989− ），男，山西太原人，博士，中国科学院信息工程研究所副研究员，主要研究方向为信息安全、访问控制。

郭云川（1977− ），男，四川营山人，博士，中国科学院信息工程研究所正高级工程师、博士生导师，主要研究方向为访问控制、网络安全。