**网络协议隐蔽信道：对策技术**

**摘要：**入侵检测系统（IDS）和计算机网络技术的先进发展促使黑客寻找新的方法在不被发现的情况下泄露机密信息。当系统采用的安全模型被两个用户或他们运行的进程之间的通信违反时，可以说两个用户之间是间接或秘密通信的。网络隐蔽信道是指任何信道都可以被一个进程以一种违反系统安全策略的方式传输信息。网络协议中的漏洞吸引了隐蔽信道的利用。本文介绍了网络隐蔽通道的对策和对于这种信道最新的检测和预防方法，并讨论了这些对策的成果和局限性。本文还进一步介绍了网络隐蔽通道三角形（DSM-开发、交换和微协议）的概念：在网络隐蔽通道环境中具有最直接积极影响的三个要素。此外，本文还反思了这种隐蔽渠道所带来的挑战。

**关键词：**隐蔽通道；安全；通道检测；预防；信道消除；信道容量；网络协议

**1. 导言**

隐蔽通道是一种通信通道，它允许在网络上的两个进程之间以破坏系统安全策略的方式传输信息[1，2]。它允许人们以一种不可察觉的方式进行交流，以发送和获取隐藏的信息。

当利用隐蔽通道被用来开展木马、病毒等恶意活动时，将其归类为严重威胁。在这种情况下，普通防火墙或检测系统无法检测到此类恶意活动。

通常，隐蔽信道存在于两种情况：独立系统和基于网络的系统[3]。最初，研究界关注的是所谓的局部秘密通道，其中两个具有不同安全级别的进程为泄露信息可以相互通信[4]。随着计算机网络的迅速发展，人们的注意力已经转移到网络上的一个秘密通道上，在这个通道中，隐蔽信息可以被编码到网络协议中[5]。

网络协议中的隐蔽通道看起来类似于隐写技术。两者都使用载体发送秘密信息，但载体的性质不同。在隐写技术的情况下，信息隐藏在诸如图像、视频、文本、声音等载体中，这种载体被称为“非结构化载体”。在网络隐蔽信道中，网络协议被用作载体，称为“结构化载体”[6，7]。一些研究者将网络隐蔽通道称为一种数据隐藏技术，并称之为网络隐写术[8，9]。据我们所知，术语网络隐蔽信道是在术语网络隐写术之前发明的。此外，Zander等人指出基于网络协议的第一个隐蔽通道是在“信息隐藏”一词还没有出现的时候提出的[7]。

本文的工作主要集中在隐蔽通道作为一种有效的工具来泄漏条件信息并且威胁网络安全，但是，从不同的角度来看，隐蔽通道的一些积极用途是网络管理员可以利用它来保护网络管理通信的安全[10]。Qian等人指出隐蔽通道技术已成为版权保护、网络认证、网络犯罪证据等安全手段的新方法[11]。此外，最近的一些工作还试图利用隐蔽信道技术来增强车载自组织网络的安全性，该领域被认为是一个包含许多挑战的热点研究领域[12]。在[14-21]中可以看到网络隐蔽通道的更多积极用途。

本节介绍了网络协议隐蔽通道，并给出了一般概述、定义和与之相关的重要问题。本文的其余部分结构如下：下一节讨论隐蔽信道类型。第三节介绍了常用的对抗隐蔽通道威胁的方法。随后，第四节对近年来有关反措施技术及其成果和局限性的相关工作进行了全面的论述。此外，本节还重点介绍了网络隐蔽通道技术的一些相关和最新趋势。第五节总结并介绍了一个崇高的概念：网络隐蔽通道三角（DSM）。最后，第六节提出了今后的工作建议。

1. **隐蔽通道类型**

本节介绍两种隐蔽通道：隐蔽存储通道和隐蔽定时通道。

*A、 隐蔽存储通道*

隐蔽存储通道涉及所有允许一个进程直接或间接地在共享存储位置中写入数据，并允许另一进程直接或间接地从该位置读取数据的方法[22]。这些进程可以在一台计算机，或者在多台通过网络（网络计算机）进行通信的计算机上。在网络方面，网络秘密存储通道包括将秘密信息编码到网络协议域（发送方）和检索秘密信息（接收方）的过程。它可以通过两种技术来实现：第一种是基于调制包头字段（例如服务类型（ToS）[24]、生存时间（TTL）[25]、因特网协议ID[26]等）；第二种是基于包长度修改。

显然，包长隐蔽信道的带宽明显高于隐蔽定时信道的带宽。因此，网络中的隐蔽存储信道比隐蔽定时信道受到了更多的关注。这是一个可能导致重大的安全破坏的严重威胁。

由于网络隐蔽存储通道的多样性，Wendzel等人将它们分为两类：（i）有效载荷隐蔽信道，其中隐蔽消息隐藏在协议的有效载荷部分中；（ii）非有效载荷隐蔽信道，其中改变非有效载荷部分，如头字段[5]。然后Wendzel等人将非有效载荷隐蔽通道分为七种模式[5]。

*B、 隐蔽定时通道*

隐蔽定时信道“包括允许一个进程通过调节其自身对系统资源的使用来向另一个进程发送信息的所有手段，其方式使得第二个进程观察到的响应时间的变化来提供信息”[1]。换句话说，在隐蔽定时信道中，发送方可以通过操纵包、帧或消息定时来发送信息；然后，预期的接收器观察并解码隐蔽信息[5，7]。与隐蔽存储通道类似，隐蔽定时通道可以在单个计算机设置或网络计算机设置中找到。在文泽尔等人的文献[5]中，可以看到对隐蔽定时信道的更多分类，并它们分成四类。

**3. 对策**

由于计算机网络技术的复杂性，网络隐蔽通道的检测和消除是一个现实的挑战。在大多数情况下，很难完全消除潜在的隐蔽信道[27，28]，因此，已经开发了许多方法来通过降低隐蔽信道带宽来减轻隐蔽信道的威胁。然而，由于这些方法在公开信道带宽上的影响，对系统的性能和可用性产生了影响。因此，在试图降低隐蔽信道带宽时，应注意公开信道带宽。

为了发展隐蔽通道对策，Zander提出了两个过程[7]。这些过程是：（i）识别所使用的隐蔽通道，然后（ii）应用合适的对策。

在设计阶段或已经部署的系统中，已经有许多正规方法来识别隐蔽通道。这些方法可分为以下几类：

* 无干扰分析，
* 信息流分析，
* 隐流树（CFT）方法，
* 共享资源矩阵（SRM）方法

然而，上述方法仅适用于单主机系统中的隐蔽信道识别，而专门用于识别基于网络的隐蔽信道的形式化技术还不多见[29]。

隐蔽通道对策分为四大类：消除、减少容量、审计和记录。感兴趣的读者可以在[7，30，31]中看到更多细节。

**4. 相关工作**

本节综述和讨论了近年来隐蔽通道对抗技术的相关工作及其取得的成就和局限性。此外，它还揭示了一些隐蔽信道的近期趋势。该部分分为以下三个部分：A部分全面介绍了当前的网络隐蔽信道检测方法，B部分介绍了网络隐蔽信道抑制技术，C部分将展示隐蔽信道的一些最新趋势。

*A、 网络隐蔽信道检测*

通常，基于特征的方法被用作网络隐蔽信道的检测方法。它区分了隐蔽流量和正常流量。Schear使用这种方法来检测隐蔽信道流量[32]。然而，这种方法无法检测到之前没有发现的任何隐蔽通道[33]。

Zhai[34]在马尔可夫模型的基础上，提出了一种TCP流中隐蔽通信的检测算法。这种检测方法在TELNET、SSH、SMTP、HTTP和FTP等多种应用中都能获得良好的隐蔽通信检测性能。上述算法的缺点是无法检测使用隧道技术的隐蔽通信。

众所周知，TCP/IP协议簇是internet通信的核心。然而，这套协议包含了最易受隐蔽通道威胁攻击的协议。作为这些协议的一个例子，TCP协议有很多字段很容易被用来传递秘密通信。与使用上述协议中的其他字段的隐蔽通道相比，使用TCP协议的初始序列号（ISN）字段的隐蔽通道似乎是最难检测的。针对基于支持向量机（SVM）的分类方法，Sohn等人提出了一种检测ISN秘密通信的方法[36]。然而，他们的方法需要大量的数据用于机器训练。这既费时又复杂。另一方面，Zhao和Shi等人提出了一种基于ISNs动态特性的ISN隐蔽通信检测方法。他们使用统计分类模型来识别隐蔽通信。Zhao和Shi称，这种方法在检测此类隐蔽信道时表现良好，只需少量计算开销。此外，该方法还可用于在线流量监测。

Tumorian和Anikeev提出了一种使用神经网络方法的ISN隐蔽通道检测方法[37]。由于操作系统具有各种不同的ISN值，因此训练阶段依赖于主机。实验结果表明，假阴性率略高，达10%。

另一方面，Murdoch和Lewis提出了两种基于OpenBSD和Linux操作系统生成编码数据的ISN隐蔽通道方法[38]。他们声称，除非检查者知道共享密钥，否则他们的方法很难被发现。原因是，通过上述方法生成的ISN数据通常与真正的TCP\IP堆栈生成的正常数据接近。因此很难检测出有助于隐蔽信道检测的变化。此外，作者还展示了他们的技术可以扩展到与其他操作系统的有效工作。

隐蔽通道技术的迅速发展增强了它们对检测方法的抵抗力。Rohankar等人指出了秘密信道技术发展背后的真正挑战，是基于用于隐蔽通信的协议上的不止一个区域[39]。这种方法会使这种隐蔽通道的检测变得非常复杂。此外，Dong等人采取了不同的方式，这是基于开发隐蔽通道，依赖于使用来自不同协议的多个字段来处理秘密消息[40]。Dong等人补充说，他们的隐蔽信道是非常难以发现或消除。

Wendzel等人做了一个值得注意的贡献，他们试图找出多个隐蔽通道的共同特征和行为，而不是像传统的检测方法那样聚焦于单个隐蔽通道。Wendzel等人研究了1978-2013年的隐蔽信道。他们提出，在特定时期，大约70%的隐蔽通道技术被分为四大类[5]。这一贡献将增强隐蔽信道检测方法的能力，并减少对每个隐蔽信道使用单一检测方法所造成的开销。

由于许多传输协议和应用程序都是基于生成随机长度的网络数据包，速记员通过使用这些长度来编码他们的秘密消息。换言之，包长度被改变以通过网络传输秘密消息--每个包长度可以编码一条信息。通常这种隐蔽技术称为包长隐蔽信道。Nair等人促进了这种隐蔽通道技术的广泛应用和日益广泛的发展[41]。

Yao等人提出了一种基于网络包长度对秘密消息进行编码的包长度秘密信道。发送者和接收者之间应该以某种方式交换具有一些独一无二的长度的秘密矩阵。发送者基于秘密矩阵对秘密消息进行编码，然后接收者使用相同的矩阵检索秘密消息[42]。然而，这种隐蔽技术很容易被基于比较正常和异常流量的检测方法检测到。他们的秘密交通与正常交通不太相似。相比之下，Zhang等人开发了一种包长隐蔽信道，该信道能够产生与正常业务非常接近的隐蔽业务，从而抵抗上述检测方法。Zhang等人验证了他们的方法抵抗检测[43]。

此外，Ji等人开发的另一种包长隐蔽信道，能够抵抗主动探测[44]。该方法是以正常流量为参考，形成隐蔽流量，使正常流量与异常流量的区分过程复杂化，但其技术未能完全模拟正常流量。因此，这削弱了他们抵抗侦查的技术。因此，Ji等人提出了另一个消息长度隐蔽通道。他们称之为正常流量网络隐蔽通道，这表明他们的隐蔽信息通常是正常流量[45]。他们声称他们的隐蔽通道对隐蔽通道检测方法有很高的抵抗力。以稍微不同的方式，Hussain等人提出了一种基于包长度和数据有效载荷的网络隐蔽信道[46]。它能够为网络检测器携带高带宽的隐蔽数据和抗回火能力。该方法利用正常的包长度特征，使秘密流量看起来与正常流量相似。

最近，Abdullaziz等人提出了两个使用UDP流量的基于包长度的隐蔽信道[47]。根据作者的说法，由上述方法产生的隐蔽流量非常接近于正常流量。因此，异常检测方法无法区分正常和异常流量。此外，这些方法在发送之前不需要接收者和发送者之间共享密钥，虽然许多基于包长度的秘密信道都需要这样的密钥。

在包长隐蔽信道检测的背景下，Nair等基于对包含隐蔽通信量的正常和恶意通信量的分类，提出了检测此类隐蔽信道存在的隐写分析方案[41]。利用二维特征空间对方案进行训练，丰富了方案的分类能力。然后利用分类器对正常和异常网络流量进行分离。基于作者的实验结果，提出了一种高精度的隐写分析方案。此外，Nair等人将其方案描述为第一种检测此类隐蔽信道的方法。如他们所指出的，以前没有提出这样的检测方案，因此，无法将其方案与现有方案进行比较。然而，它们的检测方案只涉及基于用户数据报协议流量的包长隐蔽信道。最近，基于这样的假设，任何对网络包长度的改变来编码秘密消息都可以改变网络流量的统计分布，即使这种改变的量太小。Sur等人提出了一种包长隐蔽信道检测方案[48]。该方案还通过获取一些特征来训练方案分类器，然后利用分类器检测包长隐蔽通道的存在。作者证明了他们的检测方案具有相当高的性能，并声称他们的方案可以扩展到检测所有类型的包长隐蔽信道。然而，他们的方案只在两种包长隐蔽信道下进行评估。因此，需要证明的是，包长度隐蔽信道具有不同的构造方案。

Lu等人探讨了现有的多种包长隐通道方法，并指出了其中存在的一些不足。作为这些缺点的一个例子，所研究的隐蔽信道要求隐蔽消息接收器按顺序接收所有分组[49]。因此，Lu等人提出了一种基于秘密共享方案的安全秘密信道。他们提出的方法使用网络包长度来发送秘密消息。作者指出，他们的秘密通道可以产生完全模仿正常流量的秘密流量，从而保证秘密通道不受拘禁。

Fraczek等人。提出了流控制传输协议（SCTP）中的多种信息泄漏技术。SCTP有望取代控制传输协议（TCP）和用户数据报协议（UDP）[50]，所提出的技术基于SCTP的特点（即多流和多宿）。这项工作在描述许多可能利用SCTP协议的安全攻击方面做出了重大贡献，从而有助于开发发现此类攻击的检测技术。

机器学习方法在处理信息技术的不同方面是一个很有前途的领域，它有望在检测网络隐蔽信道方面发挥重要作用[51]。Shen等人提出了一种基于支持向量机（SVM）的隐蔽信道检测方案[52]，它们是在评估网络分组相邻控制域之间的相关性的基础上，从而提取报头域的有效特征。然后，基于所提取的特征，利用支持向量机对隐蔽和正常业务进行分类或区分，从而检测出隐蔽信道的存在。成功地，此方法可以检测多达十种不同类型的隐蔽通道，它们基于作者声称的十种不同的TCP/IP头字段。然而，这种方法需要扩展，以确保其能够与利用更多不同头字段和不同协议的隐蔽信道一起工作。因为它的技术是基于机器学习的方法，可以自动学习并采取行动。

Goher等人综述了几种隐蔽信道检测方法，并对其技术进行了综合分析[53]。研究表明，隐蔽信道检测方法主要分为两类：基于特征的检测方法和异常检测方法。因此，他们对调查方法进行了分类。根据他们的调查，Goher等人指出混合隐蔽信道的检测是相当困难的，因为这种隐蔽信道是多个隐蔽信道（定时隐蔽信道和存储隐蔽信道）的组合。

Rezaei等人介绍了一种能够自动建模隐蔽通信算法的框架[54]。该框架为实现隐蔽通信技术提供了可靠的方法。基于隐蔽通道的共同特征和行为，该框架可以定义一些共同的任务和事件，然后将它们转换为可执行代码。作者通过实现两种选择的隐通道算法验证了模型的正确性。他们保证从模型中提取的对策和参数与理论预期结果一致。此外，该模型还通过实际的网络平台进行了评估[55]。拥有这样的模型可以帮助分析和评估秘密通信算法，从而更好地理解其功能，从而帮助发现其漏洞。发现隐藏算法的漏洞可以帮助开发检测方法来应对此类威胁。然而，该框架主要用于建模隐蔽时间通道，而不是隐蔽存储通道。

与之前的框架相比，Fraczek和Szczypiorski提出了一个框架，该框架能够利用网络协议作为载体创建不同的网络隐写方法。作者指出，他们的框架可以用来建立完全不可检测的隐写术方法，这是指任何无限的计算能力都无法检测这些方法[56]。希望作者开发这个框架，以支持安全和有用的用途。然而，值得注意的是，上述框架正在开发不可检测的隐蔽通道技术，这使得隐蔽通道对抗的开发方式变得复杂。

Seo等人表明由于更快的通信和更复杂的处理系统的可用性，高带宽公开信道的数量可能会增长[57]。另一方面，作者指出，没有一种解决方案能够检测出所有类型的潜在隐蔽通道，而利用所有可用技术训练入侵检测以检测多种类型的隐蔽通道是可能的。然而，这种解决方案需要资源，并且会导致更多的计算开销，这些开销对系统性能有很大的影响。相反，Seo等人。建议开发一个预防系统（即流量正常化），以减少潜在的隐蔽通道。针对这一建议，本文的下一部分将对近期网络隐蔽信道的缓解和消除工作进行综述。

*B、 网络隐蔽信道的抑制与消除*

随着计算机网络在日常活动中的出现，使人们生活的各个方面都受益匪浅，网络隐蔽通道已经成为对信息保密性和完整性的巨大威胁。尽管在发现、消除、减轻和减少这类威胁方面进行了许多成功的研究。然而，完全消除是很难实现的，或者它会影响公开信道通信的容量，从而影响系统的性能和可用性。因此，限制隐蔽信道容量是缓解隐蔽信道威胁的有效途径。它不是完全消除隐蔽通道的方法，但可以干扰隐蔽通道以实现其全部任务[58]。然而，在不影响系统可用性和性能的情况下减少隐蔽信道容量是一个真正的挑战。这是一个可能的容量减少的问题，它可以有效地降低隐蔽通道的威胁，对系统性能和可用性的影响可以接受。例如，值得注意的是，通过将所有分组长度设置为最大长度或减小分组可能具有的长度，可以实现分组长度隐蔽信道的完全消除。然而，这两种方式都削弱了合法的通信信道（公开信道）[29]。

A.Epishkina和K.Kogos指出，即使采用数据加密，也可以构造包长隐蔽信道。包长隐蔽信道是不可检测的、复杂的、无噪声的。此外，作者声称不存在限制此类隐蔽信道带宽的技术[59]。因此，A.Epishkina和K.Kogos分析了包大小隐蔽信道的带宽，并提出了限制其容量的对策工具。他们提出的方法是基于引入随机流量填充来减少信道容量[23]。然而，在应用他们的技术之前，需要对任何已研究的隐蔽信道进行估计。该技术的一些参数主要基于隐通道容量估计。感兴趣的读者可以在[60-62]中看到更多关于包长度隐蔽信道的信息。

一些隐蔽通道是通过存储和定时隐蔽通道技术的结合来建立的。这种组合的隐蔽通道可以获得高容量，而且很难被发现。这是因为存储信道技术可以提供高容量，而定时信道技术使信道可检测性复杂化。[6364]中的后分组隐蔽信道就是此类隐蔽信道的一个例子。其中，秘密数据包以一定的延迟发送。因此，合法的接收者丢弃这些数据包，因为它们是按照数据流的顺序接收的，而隐蔽的接收者处理它们并提取隐蔽的消息。试图对抗这种秘密渠道，Rezaei等人提出了一种跟踪接收包序列号的检测方法[65]。它们缓冲这些序列号以检测延迟的数据包，然后丢弃它们。Rezaei等人声称他们提出的方法在保持语音质量的同时有效地防止了这种隐蔽通道，因为他们的实验是应用在语音数据上的。然而，在视频数据流的情况下，它们的方法可能会影响系统的可用性。因此，在数据流较大的情况下，需要验证上述方法的可用性。

网络协议安全（IPsec）是一个提供安全通信的协议套件。它有助于在因特网上秘密地交换机密信息。不幸的是，这个协议容易受到秘密通信的攻击。它们是IPSec秘密信道的多种解决方案。然而，这些解决方案直接影响到系统的可用性[66]。这种影响促使Kundu引入了一种IPSec隐蔽信道威胁的缓解方法。Kundu详细分析了他的方法的安全性和可用性。他表明，与现有方法相比，他的方法提供了更好的可用性[66]。

Dakhane和Deshmukh开发了一个主动的检查者来阻止或消除TCP序列号存储隐蔽通道[3]。他们指出，TCP序列号是具有高隐蔽信道容量的载体。他们成功地降低了隐蔽信道带宽，根据他们的要求规范了正在进行的和传出的通信量。然而，应用该模型可能引起的通信开销并没有给出或估计以反映模型的可用性。

基于交换协议的隐蔽信道最初出现在文献[67]中，使得隐蔽信道能够将其存在从协议切换到另一个协议。最初，这种交换技术是基于用户命令的，而最近它被开发成一种隐蔽通道，可以自动从协议切换到另一个协议。最近的研究表明，对于此类复杂的隐蔽通道场景，缺乏应对措施。实际上，交换技术正在放大这种隐蔽通道背后的风险，因为它们很难被发现或减轻。为了开发对抗这种威胁的对策工具，Wendzel和Keller开发了一种基于协议交换技术（基于协议交换的隐蔽通道）的隐蔽通道带宽限制方法。他们的工作基于使用主动典狱长引入恒定延迟，从而降低隐蔽信道容量[68]。后来，这个典狱长被加强，引入了常数和随机延迟[69]。此外，作者还增强了他们的对策工具，以确保引入的延迟对网络正常流量没有影响。然而，它们的方法不适用于大型网络。

在网络虚拟化环境下，任何虚拟节点都会受到隐蔽通道攻击。换句话说，两个虚拟节点可以以违反系统策略的方式进行秘密通信。Wang等人。指出缓解网络虚拟化隐蔽通道威胁仍是一大挑战。因此，Wang等人。提出了一种降低隐蔽信道风险的安全虚拟网络嵌入方案[70]。他们的方案成功地降低了虚拟网络隐蔽通道攻击的风险。他们将他们的方案与[71，72]中的两个现有模型进行了比较。结果表明，该方案提高了40%的安全性。然而，为了获得使用网络虚拟化技术的最大好处，在这个领域还需要更多的安全性增强。

*C、 近期趋势*

随着秘密信道技术的迅速发展，一些研究建议最近通过在秘密消息中包含微协议引入了重大改进。微协议促进了一些通信增强，以确保可靠的通信、动态路由和一些其他功能，为秘密消息提供可信的通信。这种类型的隐蔽通道通常被称为隐蔽通道-内部控制协议。在隐蔽消息中使用微协议的特性可以保护隐蔽通道不被发现，从而增加了网络安全问题的复杂性。Wendzel和Keller强调了缺乏对抗这种隐蔽通道的对策[73]，此外，Kaur等人指出现有的对抗隐蔽通道的方法不足以应对隐蔽通道的内部控制协议[74]。

Kaur等人提供了有关微协议攻击的全面详细信息，包括但不限于对这些攻击的分析、分类和分类。因此，他们提出了一种新的攻击方法来对抗两种基于微协议的工具：Ping隧道工具和智能隐蔽通道工具。验证了这种方法的可行性[75]。然而，在已知微协议报头的结构或预测微协议的情况下，应用该方法。此外，Kaur等人。提出了一种增强微协议结构防御攻击的方法。他们提出了这种方法来保护为良好目的而实现的微协议。正如作者所说，他们未来的工作将集中于设计一种盲对策，在微协议结构或存在未知的情况下有效地工作[75]。

随着物联网的发展，物联网设备越来越流行。据报道，到2020年，满足互联网需求的设备（物）数量预计将达到500亿至1000亿台[76]。丹尼等人。表明其中相当多的设备可能是手表、眼镜、传感器等可穿戴设备。此外，估计到2019年，四分之一的智能手机用户将使用可穿戴设备[77]。这就增加了保护此类通信的重要性。真的，未来将放大临时安全部队面临的挑战。丹尼等人。提出了一种基于Android的可穿戴设备存储隐蔽通道。他们评估了他们的隐蔽通道性能，并确保其可行性和功能性。

另一方面，随着云计算的快速发展，许多企业都在利用其服务。巴特尔斯等人表明到2020年，公共云市场预计将达到1910亿美元[78]。众所周知，虚拟化技术在提高云资源利用率方面发挥着重要作用。然而，虚拟化技术非常容易受到两个虚拟机（vm）之间发起的隐蔽通信攻击。这种攻击通常被称为跨虚拟机隐蔽通道[79]。近年来，这种秘密通信因其可能带来的重大威胁而引起了众多研究者的关注。塔希尔等人。提出了一种跨虚拟网络（cross-VN）在逻辑上分离的虚拟网络之间隐藏信息泄漏通道。他们深入讨论并估计了他们的隐蔽信道带宽。此外，作者还提出了一种机制，通过减少在网络共享资源上花费的时间来减轻这种类型的隐蔽通道，并使攻击者在试图绘制网络地图时变得困难[80]。

Qian等人提出了隐蔽行为通道的定义，其中，秘密消息可以通过操作顺序传输。因此，他们开发了一种基于网络序列命令的新型网络隐蔽信道，该信道可以从存储隐蔽信道和定时隐蔽信道中获得一些特性[81]。结果表明，新的隐蔽信道与隐蔽定时信道相比，具有更好的鲁棒性和更高的比特率，对检测方法的抵抗能力也优于隐蔽存储信道。

Mileva和Panajotov指出，最近的发展方向集中在开发基于互联网服务的新型隐蔽渠道，如点对点（P2P）服务（即Skype）、云交换、社交网络（即Facebook）、新的网络协议、IP电话等[82]。

尽管开发和设计利用网络协议的不同类型的隐蔽信道的工作正在普及，但仍有一些协议尚未被用来交换隐蔽消息[83]。尤其是最近发展起来的新协议。

1. **结果**

人们清楚地注意到，大多数隐蔽信道检测方法都是通过检测正常和异常流量之间的差异来指出一种隐蔽行为。然而，最近的研究提出了一种引入隐蔽通信量的方法，这种方法通常接近于正常的通信量；这给检测此类信道带来了真正的挑战。事实上，建立一个以正常的交通通道为特征的隐蔽交通是不合逻辑的，总是有一定的变化。对于稍有偏离但未被注意到的业务信道，检测方法似乎失败了。因此，挑战在于引入对任何变化水平都敏感的检测技术。作者认为，使用机器学习方法将大大提高隐蔽信道检测技术的能力。

加密作为一种传统的安全措施，正在推动不同类型网络隐蔽通道的设计。此外，网络技术的快速发展为隐蔽通道的实现提供了丰富的环境。因此，安全专业人员正面临一个真正的持续威胁。

由于隐蔽信道类型和技术的多样性，人们注意到每一种解决方案都集中在单一类型的网络隐蔽信道上，而没有考虑到共同的行为来开发一个共同的框架来应对这种威胁。为了解决多类型隐蔽通道的问题，对隐蔽通道进行分类有一些新的趋势，本文对此作了明确的综述。然而，随着秘密技术的迅速兴起，这一可喜的方向仍需要更多的努力和贡献。

本文认为，目前对隐性信道的研究大多集中在隐性信道的理论研究上，而对隐性渠道的实践研究较少，缺乏真实的实际场景展示。对隐蔽信道的实际实现的深入了解可以帮助我们预防或减缓其发展和持续的威胁。作者支持在隐通道实现上使用真实类的方法，如[66]所示。这样的工作有助于填补实践与理论之间的空白。

物联网（IoT）、云计算和数据中心的发展为实现不同类型的网络隐蔽通道提供了丰富的环境，提高了开发新的隐蔽通道技术的动机，从而可能导致严重的安全漏洞。因此，未来的网络安全挑战将更加复杂和复杂。此外，虚拟化技术被认为是云计算资源利用的中坚力量，极易受到隐蔽通道攻击。

与其开发用于积极用途的隐蔽通道，不如让那些朝着这个方向工作的人将他们的贡献引向发现导致制作隐蔽通道的漏洞。这对于克服系统设计或其他防御阶段中存在的潜在隐蔽通道的弱点和漏洞尤其有益。

发展组合隐蔽信道的趋势是：利用定时和存储隐蔽信道技术形成混合隐蔽信道，这对复杂的隐蔽信道检测具有重要意义。组合隐蔽信道可以继承定时信道的不可检测特性和存储信道的高带宽特性。因此，这种趋势会放大风险，并可能导致严重的安全漏洞。

大量研究表明，通过重置默认值，可以完全消除利用TCP/IP报头字段的隐蔽信道。但是，这种规范化技术不适用于采用随机值的字段，例如初始序列号字段（ISN）和标识符字段（ID）。因此，探测这种隐蔽通道仍然是一个挑战。

最后，我们调查了一些可能丰富、激励和鼓励基于网络的隐蔽渠道的开发和设计的因素，这些因素反过来又加剧了这些渠道带来的威胁和危险：

* 计算机算机网络技术的飞速发展
* 主要基于网络平台的物联网（IoT）的演进
* 云计算、数据中心、虚拟化技术等的快速普及
* 交换技术，使隐蔽信道能够将其存在从一个协议切换到另一个协议
* 在一个给定的协议中使用不同的字段来携带秘密消息
* 内部控制协议技术，其中一个微协议可以包含在一个秘密消息中。微协议有助于实现可靠的通信、动态路由和其他一些为秘密消息提供可信通信的功能

因此，在本次调查的基础上，引入一个网络隐蔽通道三角形是值得注意的，它包含了三个要素，这三个要素对网络隐蔽通道技术的发展有着最直接的影响。三角形反映了网络隐蔽通道的重要性和可能带来的安全挑战。这个三角形的三个元素是：

1.网络技术的飞速发展。

2.转换技术。

3.微协议。

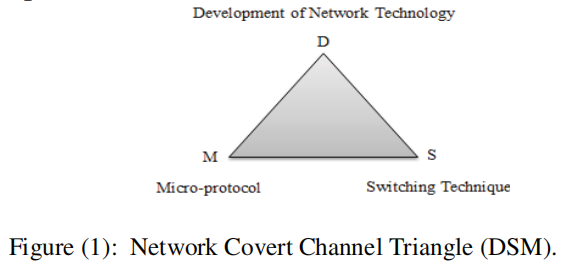
我们将这三个要素简称为DSM，其中：

D:指计算机网络技术的快速发展，包括通信技术、物联网、云计算、数据中心以及在开发计算机网络环境中扮演不同角色的所有其他技术方面。选择单词”开发”，是由于它的灵活性，涉及任何类型的开发现在或以后。调查显示，网络技术的快速发展对网络隐蔽通道的发展产生了巨大的影响。

S:指包括任何此类机制的交换技术：在给定协议内将隐蔽消息从一个文件切换到另一个文件、从一个协议切换到另一个协议或从一个网络切换到另一个-隐蔽消息的所有形式的交换。选择“交换”这个词是因为它具有灵活性，可以涉及到交换技术的任何未来发展。交换技术在保护隐蔽通道不被发现和增加任何建议的解决方案的开销方面具有巨大的影响。

M:指微协议。微协议可以嵌入到一个隐蔽的消息中，以提供和支持可靠的通信。选择“微控制器”一词是因为它的灵活性，包括任何通信功能，一个合法的协议可以提供安全的通信。微协议在保护秘密消息方面有着巨大的影响。此外，微协议可以固有任何网络协议的发展。这就丰富了隐蔽信道的能力和不可探测性。显然，微协议在为网络秘密通道提供可靠和安全的通信方面有着巨大的影响。

DSM试图描述网络隐蔽通道的危险性，从而描述安全专家面临的特殊挑战。



1. **今后的工作**

鼓励今后对网络隐蔽信道的研究，重点发展一种通用的安全模型。该模型基于这些类型信道的显著共同行为。所提出的安全模型得益于机器学习算法研究的进展，最近在不同的科学领域，特别是在信息安全领域，都取得了准确的结果。

**7. 引用**

[1] D. C. Latham, "Department of defense trusted computer system evaluation criteria," Department of Defense, 1986.

[2] B. Carrara and C. Adams, "A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels," in Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 115-126: ACM.

[3] D. M. Dakhane and P. R. Deshmukh, "Active warden for TCP sequence number base covert channel," in Pervasive Computing (ICPC), 2015 International Conference on, 2015, pp. 1-5.

[4] Y. A. H. Fadlalla, Approaches to resolving covert storage channels in multilevel secure systems. The University of New Brunswick (Canada), 1997.

[5] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-based survey and categorization of network covert channel techniques," ACM Computing Surveys (CSUR), vol. 47, no. 3, p. 50, 2015.

[6] S. Craver, "On public-key steganography in the presence of an active warden," in Information Hiding, 1998, pp. 355-368: Springer.

[7] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," Communications Surveys & Tutorials, IEEE, vol. 9, no. 3, pp. 44-57, 2007.

[8] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," IEEE Communications Magazine, vol. 52, no. 5, pp. 225-229, 2014.

[9] M. Wojciech, W. Steffen, Z. Sebastian, H. Amir, and S. Krzysztof, "Network Steganography," in Information Hiding in Communication Networks:Fundamentals, Mechanisms, Applications, and Countermeasures: Wiley-IEEE Press, 2016, p. 296.

[10] D. V. Forte, C. Maruti, M. R. Vetturi, and M. Zambelli, "SecSyslog: An approach to secure logging based on covert channels," in Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on, 2005, pp. 248-263: IEEE.

[11] Y. Qian, H. Song, F. Wang, and Z. Wang, "Network Covert Channel Encoding by Packet Length: Design and Detection," Journal of Computational Information Systems, vol. 7, no. 5, pp. 1463-1471, 2011.

[12] M. A. Elsadig and Y. A. Fadlalla, "VANETs Security Issues and Challenges: A Survey," Indian Journal of Science and Technology, vol. 9, no. 28, 2016.

[13] A. Singh and K. Manchanda, "Establishment of bit selective mode storage covert channel in VANETS," in 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2015, pp. 1-4.

[14] D. Dhobale, V. Ghorpade, B. Patil, and S. B. Patil, "Steganography by hiding data in TCP/IP headers," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010, vol. 4, pp. V4-61-V4-65: IEEE.random projections and neural networks. In Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on, pages 3422–3426. IEEE, 2013.

[15] L. Spitzner, "Know Your Enemy: Sebek2 A kernel based data capture tool," ed, 2003.

[16] R. DeGraaf, J. Aycock, and M. Jacobson Jr, "Improved port knocking with strong authentication," in Computer Security Applications Conference, 21st Annual, 2005, pp. 10 pp.-462: IEEE.

[17] W. Mazurczyk and Z. Kotulski, "New security and control protocol for VoIP based on steganography and digital watermarking," arXiv preprint cs/0602042, 2006.

[18] H. Qu, Q. Cheng, and E. Yaprak, "Using Covert Channel to Resist DoS attacks in WLAN," in ICWN, 2005, pp. 38-44.

[19] M. H. Almeshekah, M. J. Atallah, and E. H. Spafford, "Layering authentication channels to provide covert communication," in Proceedings of the 14th Annual Information Security Symposium, 2013, p. 9: CERIAS-Purdue University.

[20] Y. Sun, X. Guan, and T. Liu, "A new method for authentication based on covert channel," in IFIP International Conference on Network and Parallel Computing, 2011, pp. 160-165: Springer.

[21] T. S. Fatayer and K. A. A. Timraz, "MLSCPC: Multi-level security using covert channel to achieve privacy through cloud computing," in 2015 World Symposium on Computer Networks and Information Security (WSCNIS), 2015, pp. 1-6.

[22] S. Hammouda, L. Maalej, and Z. Trabelsi, "Towards Optimized TCP/IP Covert Channels Detection, IDS and Firewall Integration," in 2008 New Technologies, Mobility and Security, 2008, pp. 1-5.

[23] A. Epishkina and K. Kogos, "A random traffic padding to limit packet size covert channels," in Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on, 2015, pp. 1107-1111: IEEE.

[24] T. G. Handel and M. T. Sandford II, "Hiding data in the OSI network model," in Information Hiding, 1996, pp. 23-38: Springer.

[25] S. Zander, G. Armitage, and P. Branch, "Covert channels in the IP time to live field," in Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC), 2006.

[26] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP," in Proc. Workshop on Multimedia Security at ACM Multimedia, 2002, vol. 2.

[27] B. W. Lampson, "A note on the confinement problem," Communications of the ACM, vol. 16, no. 10, pp. 613-615, 1973.

[28] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," First Monday, vol. 2, no. 5, 1997.

[29] D. J. Dye, "Bandwidth and detection of packet length covert channels," Monterey, California. Naval Postgraduate School, 2011.

[30] L. Barroso and M. Santos, "A Review on Covert Techniques."

[31] M. A. Elsadig and Y. A. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques," in Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016, 2016..

[32] N. Schear, C. Kintana, Q. Zhang, and A. Vahdat, "Glavlit: Preventing exfiltration at wire speed," IRVINE IS BURNING, p. 133, 2006.

[33] Q. Yuwen, S. Huaju, S. Chao, W. Xi, and L. Linjie, "Network covert channel detection with cluster based on hierarchy and density," Procedia Engineering, vol. 29, pp. 4175-4180, 2012.

[34] J. Zhai, G. Liu, and Y. Dai, "Detection of TCP covert channel based on Markov model," Telecommunication Systems, vol. 54, no. 3, pp. 333-343, 2013.

[35] H. Zhao and Y. Q. Shi, "A phase-space reconstruction approach to detect covert channels in TCP/IP protocols," in Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, 2010, pp. 1-6: IEEE.

[36] T. Sohn, J. Seo, and J. Moon, "A study on the covert channel detection of TCP/IP header using support vector machine," in ICICS, 2003, pp.313-324: Springer.

[37] E. Tumoian and M. Anikeev, "Network based detection of passive covert channels in TCP/IP," in Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on, 2005, pp. 802-809: IEEE.

[38] S. J. Murdoch and S. Lewis, "Embedding covert channels into TCP/IP," in Information hiding, 2005, pp. 247-261: Springer.

[39] N. D. Rohankar, A. Deorankar, and D. P. Chatur, "A Review of Literature on Design and Detection of Network Covert Channel," International Journal of Engineering Science and Innovative Technology (IJESIT) Volume, vol. 1, 2012.

[40] P. Dong, H. Qian, Z. Lu, and S. Lan, "A Network Covert Channel Based on Packet Classification," IJ Network Security, vol. 14, no. 2, pp. 109-116, 2012. 2017 9th IEEE-GCC Conference and Exhibition (GCCCE)

[41] A. S. Nair, A. Sur, and S. Nandi, "Detection of Packet Length Based Network Steganography," in 2010 International Conference on Multimedia Information Networking and Security, 2010, pp. 574-578.

[42] Q.-z. YAO and P. ZHANG, "Coverting channel based on packet length," Computer engineering, vol. 34, no. 3, pp. 183-185, 2008.

[43] L. Zhang, G. Liu, and Y. Dai, "Network packet length covert channel based on empirical distribution function," Journal of Networks, vol. 9, no. 6, pp. 1440-1446, 2014.

[44] L. Ji, W. Jiang, B. Dai, and X. Niu, "A novel covert channel based on length of messages," in 2009 International Symposium on Information Engineering and Electronic Commerce, 2009, pp. 551-554: IEEE.

[45] L. Ji, H. Liang, Y. Song, and X. Niu, "A normal-traffic network covert channel," in Computational Intelligence and Security, 2009. CIS'09. International Conference on, 2009, vol. 1, pp. 499-503: IEEE.

[46] M. Hussain and M. Hussain, "A high bandwidth covert channel in network protocol," in Information and Communication Technologies (ICICT), 2011 International Conference on, 2011, pp. 1-6: IEEE.

[47] O. I. Abdullaziz, V. T. Goh, H. C. Ling, and K. Wong, "Network packet payload parity based steganography," in 2013 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET), 2013, pp. 56-59.

[48] A. Sur, A. S. Nair, A. Kumar, A. Jain, and S. Nandi, "Steganalysis of network packet length based data hiding," Circuits, Systems, and Signal Processing, vol. 32, no. 3, pp. 1239-1256, 2013.

[49] X. Lu, Y. Wang, L. Huang, W. Yang, and Y. Shen, "A Secure and Robust Covert Channel Based on Secret Sharing Scheme," in AsiaPacific Web Conference, 2016, pp. 276-288: Springer.

[50] W. Frączek, W. Mazurczyk, and K. Szczypiorski, "Hiding information in a Stream Control Transmission Protocol," Computer Communications, vol. 35, no. 2, pp. 159-169, 2012.

[51] M. Wojciech, W. Steffen, Z. Sebastian, H. Amir, and S. Krzysztof, "Network Steganography Countermeasures," in Information Hiding in Communication Networks:Fundamentals, Mechanisms, Applications, and Countermeasures: Wiley-IEEE Press, 2016, p. 296.

[52] Y. Shen, L. Huang, X. Lu, and W. Yang, "A novel comprehensive steganalysis of transmission control protocol/Internet protocol covert channels based on protocol behaviors and support vector machine," Security and Communication Networks, vol. 8, no. 7, pp. 1279-1290,

2015.

[53] S. Z. Goher, B. Javed, and N. A. Saqib, "Covert channel detection: A survey based analysis," in High Capacity Optical Networks and Emerging/Enabling Technologies, 2012, pp. 057-065.

[54] F. Rezaei, M. Hempel, and H. Sharif, "A novel automated framework for modeling and evaluating covert channel algorithms," Security and Communication Networks, vol. 8, no. 4, pp. 649-660, 2015.

[55] F. Rezaei, M. Hempel, P. L. Shrestha, and H. Sharif, "Evaluation and Verification of Automated Covert Channel Modeling Using a Real Network Platform," in 2014 IEEE Military Communications Conference, 2014, pp. 12-17.

[56] W. Fraczek and K. Szczypiorski, "Steg Blocks: Ensuring Perfect Undetectability of Network Steganography," in 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 436-441.

[57] J. O. Seo, S. Manoharan, and A. Mahanti, "A Discussion and Review of Network Steganography," in 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2016, pp. 384-391.

[58] M. McFail, "Covert storage channels: A brief overview," in PACISE Conference, Bloomsburg, PA, 2005.

[59] A. Epishkina and K. Kogos, "Covert Channels Parameters Evaluation Using the Information Theory Statements," in IT Convergence and Security (ICITCS), 2015 5th International Conference on, 2015, pp. 1-5.

[60] A. Epishkina and K. Kogos, "Packet Length Covert Channel Capacity Estimation," in 2016 6th International Conference on IT Convergence and Security (ICITCS), 2016, pp. 1-4.

[61] A. Epishkina and K. Kogos, "A Traffic Padding to Limit Packet Size Covert Channels," in Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, 2015, pp. 519-525.

[62] M. A. Elsadig and Y. A. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques," International Journal of Advances in Computer Networks and Its Security, vol. 6, no. 3, pp. 11-17, 2016.

[63] W. Mazurczyk and J. Lubacz, "LACK—a VoIP steganographic method," Telecommunication Systems, vol. 45, no. 2-3, pp. 153-163, 2010.

[64] W. Mazurczyk, "Lost audio packets steganography: the first practical evaluation," Security and Communication Networks, vol. 5, no. 12, pp. 1394-1403, 2012.

[65] F. Rezaei, M. Hempel, D. Peng, and H. Sharif, "Disrupting and Preventing Late-Packet Covert Communication Using Sequence Number Tracking," in MILCOM 2013 - 2013 IEEE Military

Communications Conference, 2013, pp. 599-604.

[66] A. Kundu, "Mitigation of Storage Covert Channels in IPSec for QoS Aware Applications," Procedia Computer Science, vol. 54, pp. 102-107, 2015.

[67] P. Magazine, "7 (51) September 01, 1997, article 06 of 17 [LOKI2 (the implementation)]," ed.

[68] S. Wendzel and J. Keller, "Design and implementation of an active warden addressing protocol switching covert channels," in Proc. 7th International Conference on Internet Monitoring and Protection (ICIMP 2012), Stuttgart, 2012.

[69] S. Wendzel and J. Keller, "Preventing protocol switching covert channels," International Journal on Advances in Security, vol. 5, 2012.

[70] W. Zhiming, W. Jiangxing, G. Zehua, C. Guozhen, and H. Hongchao, "Secure virtual network embedding to mitigate the risk of covert channel attacks," in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 144-145.

[71] S. Liu, Z. Cai, H. Xu, and M. Xu, "Towards security-aware virtual network embedding," Computer Networks, vol. 91, pp. 151-163, 2015.

[72] L. Gong, Y. Wen, Z. Zhu, and T. Lee, "Toward profit-seeking virtual network embedding algorithm via global resource capacity," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014, pp. 1-9: IEEE.

[73] S. Wendzel and J. Keller, "Hidden and under control," annals of telecommunications-annales des télécommunications, vol. 69, no. 7-8, pp. 417-430, 2014.

[74] J. Kaur, S. Wendzel, and M. Meier, "Countermeasures for Covert Channel-Internal Control Protocols," in Availability, Reliability and Security (ARES), 2015 10th International Conference on, 2015, pp. 422-428.

[75] J. Kaur, S. Wendzel, O. Eissa, J. Tonejc, and M. Meier, "Covert channel­internal control protocols: attacks and defense," Security and Communication Networks, 2016.

[76] P. F. Drucker, "Internet of Things," 2015.

[77] K. Denney, A. S. Uluagac, K. Akkaya, and S. Bhansali, "A novel storage covert channel on wearable devices using status bar notifications," in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 845-848.

[78] A. Bartels, J. Rymer, J. Staten, K. Khalid, and J. Clark, "The Public Cloud Market Is Now In Hypergrowth: Sizing the Public Cloud Market, 2014 To 2020," Forrester, April, vol. 24, p. 2014, 2014.

[79] W. Qi, J. Wang, H. Hovhannisyan, K. Lu, and J. Zhu, "A Generic Mitigation Framework against Cross-VM Covert Channels," in 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016, pp. 1-10.

[80] R. Tahir et al., "Sneak-Peek: High speed covert channels in data center networks," in IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, 2016, pp. 1-9.

[81] Y. Qian, T. Sun, J. Li, C. Fan, and H. Song, "Design and analysis of the covert channel implemented by behaviors of network users," Security and Communication Networks, vol. 9, no. 14, pp. 2359-2370, 2016.

[82] A. Mileva and B. Panajotov, "Covert channels in TCP/IP protocol stackextended version," Open Computer Science, vol. 4, no. 2, pp. 45-66, 2014.

[83] R. Rios, J. A. Onieva, and J. Lopez, "Covert communications through network configuration messages," Computers & Security, vol. 39, pp. 34-46, 2013.