基于隐蔽通信的访问控制增强技术综述

张　宏，郭云伟
（北京理工大学　计算机学院，北京　100081）

摘　要：网络访问控制模型对于安全防范和保护具有重要意义。现有的网络访问控制模型大多是通过加密实现的，具有隐蔽性和可控性，容易被发现和攻击。基于隐写标签的隐蔽通信技术主要检测网络数据包是否包含隐写头部标签，并根据访问控制规则确定数据包的流向，有效控制主体对客体的访问。此外，详细介绍了几种方法下的访问控制规则，并描述了针对各种类型的隐蔽通道的相应检测方法。最后分析了区块链隐蔽通信构建技术及其发展趋势，旨在为相关研究提供一定参考价值。

关键词：访问控制；隐蔽通信；区块链；信息隐藏
中图分类号：TN925；TP18　　**文献标识码**：A　　**DOI**：10.19358/j.issn.2097-1788.2023.05.001
引用格式：张宏，郭云伟. 基于隐蔽通信的访问控制增强技术综述［J］. 网络安全与数据治理，2023，42(5)：1-9.

A survey on covert communication-based access control enhancement technology

Zhang Hong，Guo Yunwei
（School of Computing Science，Beijing Institute of Technology，Beijing 100081，China）

Abstract：The network access control model is important for security prevention and protection. Most of the existing network access control models are implemented through encryption，which has defects in concealment and controllability，and is easy to detect and attack. The covert communication technology based on steganographic labels mainly detects whether network packets contain stegantic headers，and determines the flow direction of packets according to access control rules，to effectively control the subject's access to objects. In addition，this paper introduces the access control rules under several access control methods in detail，and describes the corresponding detection methods for various types of covert channels. Finally，this paper analyzes the development trend of blockchain covert communication construction technology and its detection methods，aiming to provide some significant value for related research.

Key words：access control；covert communication；blockchain；information hiding

0　引言

近年来，随着计算机计算能力的大幅提升和技术架构的进步，针对传统安全协议和密码算法的攻击能力越来越强，数据传输的安全性和网络通信的隐私性面临着重大挑战[1]。现有主要的安全手段是通过密码学方法对秘密信息进行加密，使非授权用户在限定时间内无法破译，借以保护隐私信息，其安全性通常取决于算法的复杂度和密钥的长度。但是，随着现代计算机计算能力的快速提升，为保持所需的安全强度，单纯增加密钥长度等普通加密算法会严重影响使用效率，显得过于被动。因此，网络隐蔽通信技术成为传统加密通信的有力补充手段[2]。隐蔽通信技术是一种信息隐藏技术。根据信息隐藏技术的不同应用目的，可分为四类：隐写术[3]、匿名通信[4]、数字水印[5]、隐蔽通道[6]。近年来，构建隐蔽通信通道及相应的分析检测技术发展尤为迅速。

区块链技术自出现以来发展迅速，已经涉及生活的方方面面，具有“区块链＋领域”的特点[7]，人们逐渐将区块链视为一种可编程的分布式信用基础设施[8]。随着区块链相关技术的研究和项目施行，数据隐私和安全问题越来越受到重视。研究人员通常将区块链的隐私分为身份隐私和交易隐私。文献［9］将区块链的隐私保护机制分为三种类型：网络层、交易层和应用层。近年来，越来越多的研究人员专注于密码学相关技术，如隐蔽信道、零知识证明、同态加密、安全多方计算、承诺方案、环签名和差分隐私等技术。加密和信息隐藏技术旨在区块链开放平台中保护用户隐私和通信安全[11-16]。2018 年

后，基于区块链平台的隐蔽通信研究已经开始。业界普遍认为，Partala 提出的 BLOCCE 是第一个基于区块链的可证明安全的隐蔽通信通道[17]。区块链本身的优良特性可以解决隐蔽通信领域的许多问题，包括匿名性、不可信性和隐蔽性。

隐蔽通信技术研究领域还处于起步阶段，仍有许多问题亟待解决，包括增加隐蔽容量、提高通信效率、降低成本确保隐蔽性等[18-19]。随着区块链研究的深入和应用的落地，对区块链上的数据安全和通信安全的需求将会增加，通过区块链平台建立隐蔽通道将是一个高效的解决方案。

与此同时，隐蔽信道的分析检测和攻击方法的相关研究也同步进行。传统的解决方案在面对非法的秘密通信处境时往往处于被动，因此需要针对不同的隐蔽通道类型提供不同的解决方案。近年来，机器学习技术的发展也为隐蔽通信的检测和攻击提供了具体的手段。随着基于区块链的隐蔽通信研究的逐步深入，针对区块链上隐蔽通信的检测方法的研究也迫在眉睫，以保证系统的安全性和稳定性。

本文简要介绍了隐蔽通信技术的相关基本概念和技术分类，将现有的基于区块链隐蔽通信通道的技术分为四类：基于块结构、基于外部载体、基于业务操作时间、基于系统机制。按照提出的隐蔽通道的分类方法依次介绍了检测方法和攻击方法，最后展望了区块链隐蔽通信通道构建技术和检测方法的发展方向和应用前景，为今后的技术研究提供有益启示和借鉴。

1　隐蔽通信模型概述

1.1　隐蔽通信渠道的分类

（1）存储型隐蔽通道

接收方通过修改双方共有的资源来隐藏秘密消息接收方找到资源的位置，并使用双方同意的方案来提取秘密消息[20]。资源称为消息载体，载体可以是文本、图像、视频、音频等形式。由于图像、视频和音频包含更多的冗余信息，因此隐藏容量更显重要。近年来，基于文本的敏感信息隐藏[21]研究较少。基于文本的信息隐藏算法通常可以分为三类：基于文本格式、基于文本内容和基于文本图像[22]。无论选择哪种类型的载体文件，基本思路都是利用其冗余空间来嵌入敏感信息而不被感知。该方法具有隐蔽性强、隐蔽性好、鲁棒性弱等特点。

（2）时间型隐蔽通道

发送方通过调整资源的时间特性，结合预先协商的编码方法来隐藏秘密信息。接收端观察相关资源的时间属性，并对其进行解码，得到秘密信息[23]。然而，这种解决方案对网络环境有很高的要求。如果网络环境质量不稳定或攻击者主动添加噪声和延迟，信道传输速率和准确性都会大打折扣。该方案具有低隐蔽容量和高隐蔽性。

（3）行为型隐蔽信道

发送方通过更改资源的行为、状态和其他属性对秘密信息进行编码和隐藏。接收方监视系统网络中每一个动作的特性，在找到约定的编码序列后开始接收[24]。由于这些资源行为属性是通信协议或网络中的典型行为，因此信道的构建和传输过程具有很强的隐蔽性[25]。

1.2　信息隐藏嵌入算法

信息隐藏嵌入算法包括替换、变换和扩频算法[26-30]。

（1）置换算法

置换算法是一种在空间域中操作的算法。该算法通过选择合适的载体和合适的嵌入区域，可以有效地嵌入需要隐藏的秘密信息。该算法一般包括最低位替换、载波区奇偶校验位替换和伪随机替换。从算法实现的角度来看，该算法是最容易实现的信息隐藏嵌入算法。

（2）变换算法

变换算法是在变换域中操作的算法。算法主要包括离散傅里叶变换（DFT）、离散余弦变换（DCT）、离散小波变换（DWT）和离散哈达玛变换（DHT）。该算法一般用于以图像为载体的信息隐藏。其中，离散傅里叶变换主要是将图像划分为几个频带，然后选择合适的部分来嵌入需要隐藏的秘密信息。离散余弦变换（DCT）是将图像在水平和垂直方向上分成若干块，分别对每个块进行离散余弦变换，使其变换矩阵只包含余弦分量。信息隐藏是根据每个 DCT 后的块的相对大小来进行的。DWT 是对图像进行多尺度、空间和频率分解。输入信号被分解为一个低分辨率的参考信号和一系列细节信号。在一个尺度上，参考信号和细节信号包含的所有信息，以完全恢复信号在以前的尺度。

（3）扩频算法

扩频算法采用比传输信息数据速率高出许多倍的伪随机码，对携带信息数据的基带信号进行频谱扩展，形成宽带低功率谱密度信号来隐藏信息。常用的扩频算法有直接序列扩频和跳频扩频。扩频算法的优点是检测信息不需要原始信号。也就是说，在检测过程中可以进行盲检测。即使信号在传输过程中受到加性噪声和乘性噪声的攻击，也能在接收端检测出隐藏的信息。它的缺点是载体信息必须与秘密信息同步。一旦受到异步攻击，在接收端提取隐藏数据就比较复杂，提取过程相对复杂。与信息隐藏嵌入算法进行比较（如表 1 所示）发现，置换算法比变换算法和扩频算法更易于实现。由于图像、

视频等传统载体的信息隐藏常采用变换算法和扩频算法，因此置换算法适合于协议作为载体的信息隐藏。

表 1　三种信息隐藏嵌入算法对比

Information Hiding Embedding Algorithm	Ease of implementation	Robustness
Replacement Algorithm	easy	poor
Change Algorithm	difficult	well
Spread Spectrum Algorithm	difficult	well

1.3　区块链网络隐蔽通道

1.3.1　交易地址类型

此类型隐蔽通道使用区块链中的交易地址作为载体功能，在通信过程中，根据其他的公私密钥对生成不同的交易地址作为秘密信息的载体编码或传输。文献［31］建议 BLOCCE 区块链网络隐蔽通道，文献［32］在 BLOCCE 和文献的基础上进行了改进。文献［33］使用相同的想法使用 V-BLOCCE 方法的地址生成软件 Vanitygen。BLOCCE 系列直接将秘密信息显示在地址的实际位中。与直接将私有信息映射到事务地址的 BLOCCE 系列不同，文献［34］使用特殊的地址生成算法对信息进行编码，将需要嵌入的二进制秘密信息与预共享密钥融合，生成新的公钥，根据公钥生成交易地址作为传输秘密信息的载体。接收方只需要根据交易地址判断公钥与输出的关系，判断其是否包含私有信息并进行解码。将前一事务的输出作为下一事务的输入，无需遍历所有事务即可筛选出特定地址，提高了效率。该方法虽然每个地址只能嵌入 1 比特信息，但将秘密信息与交易地址直接结合，提高了隐蔽性。文献［35］根据交易时间的先后顺序生成交易索引矩阵，对编码秘密信息的交易量进行排序和解码。该方法利用金额对私有信息进行编码，增加了单笔交易可嵌入的信息容量，减少了交易次数，提高了传输效率。而交易地址索引矩阵提供了一种筛选方法，不需要遍历所有事务，筛选效率更高。但是，这种方法重复使用一个交易双方都知道的地址集进行交易，并且交易地址关联分析方法可以追溯到交易双方，破坏了通道的隐蔽性。

此外，与上述基于固定地址的筛选机制相比，交易地址设置结合动态标签生成特定交易地址，更好地平衡了筛选效率和隐蔽性。文献［36］使用不断变化的块高度作为一个积极的标签。它使用预共享密钥生成一个新的私钥，该私钥使用基于哈希的消息身份验证代码（HMAC），并生成一个特殊的交易。交易地址确保只有持有预共享密钥的通信方可以提取信息。文献［37］基于实际交易统计 OPRETURN 字段上的交易数据，结合域生成算法生成具有动态标签的唯一地址。文献［38］然后使用前一个块的块号和 Nonce 值来创建活动标记。

1.3.2　签名算法类型

此类型的隐蔽通道使用区块链中的数字签名算法作为载体特征。在区块链中，每一笔交易都将由交易双方进行数字签名，以确保数据未被篡改，确保交易双方的身份真实可靠。在改进的特殊签名算法中，只有接收方可以使用私钥获取发送方的私钥，提取秘密信息。另一种是类似于交易地址的构造过程，利用签名算法本身作为秘密信息（如数字签名中的有效位）的存储载体进行传输。

文献［39］首次提出了一种构造签名算法类型隐蔽信道的模型。文献［40］给出了一种具体的实现方法，即利用窃取算法修改区块链中原有的签名算法来构建通道，并利用区块链官方客户端的开源代码设计了专用的数据发送客户端和专用的数据接收客户端来进行信息传输。发送端修改包含秘密信息的交易中的签名算法，接收端用窃取算法进行检测和屏蔽。交易包含机密信息和摘录信息。只有节点知道窃取算法的密钥信息可以提取私钥，解码秘密信息。这种方法生成每个事务所需的时间仅比普通事务长 36 ms，差别不大。文献［41］通过修改比特币交易的椭圆曲线数字签名算法（ECDSA），在僵尸网络场景中构建了一个隐蔽通道。文献［42］和文献［43］结合环签名技术，利用环签名技术的特点，在提高匿名性的同时构建隐蔽信道。

1.3.3　智能合约类型

此类隐蔽通道以区块链的智能合约为载体特征。参数的多样性、数据的冗余性、代码的可编程性，使其成为构建隐蔽信道的优秀载体。发送方将秘密信息编码到智能合约的预设触发条件和预设响应规则中，接收方根据不同的响应对不同的秘密信息进行解码。

文献［43］采用智能合约作为传感器网关，结合图像隐写技术实现隐蔽通信。将包含分区号、访问时间和镜像地址的说明书嵌入到智能合同交易的时间戳中，接收方根据预先共享的信息从合约中提取。其中，分区数是组播传送的接收者数量，访问时间是隐写图像的时效性，图像 URL 是隐写图像的位置。该方法以智能合约为载体，结合图像隐写技术，具有较高的信道容量。说明书中的访问时间，防止秘密信息被永久存储在区块链中，提高了通道的隐蔽性。文献［32］利用投票合约中的不同期权和投标契约中的不同投标编号映射秘密信息序列，然后调用契约传递信息。在投票契约中，增加了多项选择和冗余选择，既增加了信息编码的复杂性，又提

高了信息传递的效率。在竞价合同中，通过设置单个节点的有效竞价范围，提高了筛选效率，并允许提出包含多个有效竞价的集合，减少了交易次数，提高了传输效率。

1.3.4 P2P 广播机制

此类隐蔽通道以区块链的 P2P 广播机制为载体特征，是区块链节点间通过泛洪模式迭代转发过滤的区块链数据交易信息系统下的网络隐蔽通道。一方面，通过空间特性，利用 P2P 广播机制的转发过程，修改数据中的字段或利用冗余字段添加内容对秘密信息进行编码来构造隐蔽通道的方法。另一方面，通过时间特性，利用交易转发的时间间隔和转发数据的时间延迟对秘密信息进行编码，构造隐蔽信道的方法。

在利用空间特征的方法中，文献［44］基于比特币交易广播机制，首先将节点 A 的加密秘密信息编码到 Coinbase 字段中，使用其哈希值作为索引，并插入 INPUT 消息和 GET 数据消息共享的信息。列表向量用于通知其他节点该节点拥有对象或请求数据节点 B 接收到 inv 消息后，根据索引在节点事务消息中搜索相同的事务哈希值。如果存在，找到交易的 coinbase 字段进行信息提取和解码，然后将过滤后的 get 数据消息返回给节点 A；如果不存在，则将包含索引的 get 数据消息返回给节点 A，说明通信尚未完成。但是，将秘密信息编码到利用率较低、每 10 min 生成一次的字段中，影响了信道的传输效率和隐蔽性。

文献［45］建议使用 Ethereum Whisper 协议建立一个隐蔽信道模型。在此基础上，文献［46］和文献［47］给出了一个基于 Whisper 协议的隐蔽信道模型。该方法有很多优点：Whisper 协议信件的信封中包含最新的有效时间和生存时间，到期后不会被存储，提高了信道的隐蔽性，采用类似于比特币挖矿机制寻找 Nonce 值的方法设置门限，只有当发送消息的节点的阈值超过特定阈值时，才能在以太坊网络中继续转发，也可以将不符合持续发送要求的节点列入黑名单，避免第三方干扰；使用专门编码的主题字段过滤不相关的内容，提高筛选效率。除了以太坊中的 Whisper 协议，文献［48］利用比特币中的 Gossip 协议，通过使用基于比特币的客户端 Tithonus 来构建一个隐蔽通道。文献［49］利用广播机制中的时间特性，构造了一种基于多节点时间戳共谋的区块链网络隐蔽通道[50]，将秘密信息映射到不同区块链业务操作的时间间隔，形成具有唯一标识序列的集合后发送。信息接收端使用预设的方法对唯一标识节点进行识别，提取秘密信息并进行解码。文献［51］结合具体应用场景，利用区块链业务的时间间隔是否超过阈值对授权信息进行编码，并利用这项技术保证智能电网中用户授权的有效性。这两种利用 P2P 广播机制的时间特性对秘密信息进行编码的方法在信道隐蔽性和鲁棒性方面都优于传统的基于时间的网络隐蔽性，因为区块链网络的时间戳功能受网络波动的影响较小。

2 访问控制模型的研究现状

2.1 基于智能合约的访问控制

文献［52］在前人工作的基础上提出了一种访问控制参考模型，提出并实现了一种新的访问控制方案 FairAccess。基于访问凭证，该方案引入了四种交易类型，包括授予、获取、代理和撤销凭证。然而，基于区块链的交易机制也使得这种解决方案无法满足需要实时性能的应用场景。以比特币的工作负载共识机制为例，一笔交易确认大约需要 10 min。文献［53］提出了一种基于区块链和 CapBAC 模型的访问控制方案 Blend-CAC。该方案提出了一个支持多级证书的代理模型，并探讨了代理授权和撤销机制。同时，提出了一种基于智能合约的凭证生存周期管理策略，实现了访问控制凭证的生成和撤销功能。该方案的多级代理路径是树形的，其访问证书以委托人为单位表示。文献［54］提出了一个访问控制框架，包括访问控制合约（ACC）、决策合约（JC）和注册合约（RC）。每一个访问控制合约为一个主体 - 客体对，提供一个访问控制接口函数，它可以实现基于预定义的访问策略的静态访问验证和通过检测主体的行为来实现动态访问验证。JC 通过分析 ACC 的异常行为报告生成惩罚，辅助 ACC 的动态访问权限验证。注册合约用于注册访问控制和异常行为惩罚功能及其智能合约信息，以及这些功能的生存周期（注册、更新和撤销）功能。但是，该解决方案不具备访问代理功能，不适合需要高灵活性的场景。文献［55］是一种改进的解决方案。与文献［53］不同的是，该方案以访问操作为单位以图的形式表示代理路径，实现了一种更细粒度、更灵活的证书代理机制。

2.2 结合属性和角色的访问控制模型

2010 年，美国国家标准与技术研究所的 Kuhn 和美国科学应用国际公司的 Coyne 提出整合基于角色的访问控制和基于属性的访问控制的最优特性[56]，提供一个分布式和快速变化的环境。应用系统提供有效的访问控制。方案通过枚举定义了三种可能的使用角色和属性的方法，分别是动态角色、以属性为中心和以角色为中心。动态角色的方法是属性决定应该激活用户的哪些角色；以属性为中心的方法是，角色不再与权限相关联，但角色名称被用作属性的成员；以角色为中心的方法是，角色决

定用户拥有的最大权限集，属性用于限制权限。文献［56］中详细比较了基于角色的访问控制和基于属性的访问控制。Coyne 等人认为 RBAC 已经得到了广泛的应用，在管理和安全方面具有优势，但不能适应以实时环境状态作为访问控制参数的场景；ABAC 更新颖，易于实现，能够适应以实时环境状态作为访问控制参数的场景，但是很难审计给定权限可以访问哪些用户或者给定用户可以访问哪些权限。因此，结合两者的优点，可以提供一个灵活的、可扩展、可审计和可理解的访问控制模型。

2.2.1 以属性为中心的访问控制模型

以属性为中心的访问控制将角色名视为众多属性中的一个属性。与传统 RBAC 相反，角色不再是权限的集合，而是一个名为“role”的属性。在文献［57］中，提出了一种使用 RBAC 管理用户属性的框架，并对 ARBAC97 模型中的用户角色分配模型 URA 进行了推广，得到了 GURA 模型，该模型将角色作为一类用户属性来实行用户属性管理。主要方法是为每一个管理角色分配它所管理的用户属性范围，然后将这些管理角色分配给每一个管理用户，从而达到属性管理的目的。在文献［58］中将身份、安全级别、敏感性、角色等用户和主客体特征都视为属性，提出了基于属性的访问控制模型，建立 ABACα，并从策略的角度对 ABACα 进行了形式化验证。但它只支持核心 RBAC 模型，不支持 RBAC 模型的扩展模型。后来的文献［59］中，在 ABACα 模型的基础上，提出了 ABACβ 模型，该模型能够覆盖大部分扩展的 RBAC。在考虑角色层次和动态职责分离的基础上，将角色看作用户和主体的一个属性，用属性值的偏序关系表示角色层次，用会话中是否同时激活角色的策略表示动态职责分离。文献总结了 RBAC 扩展所需的功能，最后介绍了五个扩展功能来代表 RBAC 模型及其扩展模型与 ABACβ。为了解决如何为云存储服务构建一个与 RBAC 兼容的基于属性的访问控制的问题，文献［60］提供了一个用户友好、易于管理和安全的 ABAC 机制，通过比较 RBAC 和 ABAC 的异同将角色映射为多个属性的集合，将角色之间的层次关系映射为属性表达式之间的偏序关系，将用户角色分配映射为规则，从而实现从 RBAC 到 ABAC 的迁移。

2.2.2 以角色为中心的访问控制模型

以角色为中心的访问控制模型的目的是解决 RBAC 模型不能很好地支持细粒度授权和 ABAC 模型中权限审计困难的问题。扩展的 RBAC 模型往往采用角色层次化的方法，通过不断细分角色来解决细粒度的授权问题，这会带来“角色爆炸”的问题，增加了模型的管理成本和复杂性。ABAC 模型能很好地支持细粒度授权，但其权限审计难以保证其安全性。角色中心方法以 RBAC 为基本框架，通过引入属性实现细粒度授权。Kim 等人首先提出了以角色为中心的访问控制模型（Rabac）[26]，将 RBAC 扩展为用户属性和对象属性，并将一个称为权限过滤策略（PFP）的组件添加到会议上的 RBAC2004 标准模型。该方法很好地解决了角色爆炸的问题，从而促进了用户的角色分配，同时保留了角色和权限之间的静态关系，从而保留了 RBAC 授权操作、权限审计、策略管理的优点。但是，该方法没有引入环境属性，因此不能应用于系统中经常变化的属性，如位置和时间。卡西姆等人提出了一种属性增强的基于角色的访问控制模型（AERBAC）[61]，该模型综合考虑了用户属性、对象居性和环境属性。AERBAC 中的权限由对象属性表达式和操作方法组成。权限不再分配给单个对象，而是分配给具有相同属性的一组对象。同时，由用户属性表达式和环境构成的约束与属性表达式与权限直接相关。当用户请求访问时，用户请求将被作为输入。checkAccess 函数将处理每个请求并返回判断结果。为了更好地实现访问目的，模型将访问分为两种访问形式：基于身份的访问和基于属性的访问[62]，并分别对两种访问形式进行了说明。模型仍然采用基于角色的访问控制作为主要框架，因此继承了基于角色的访问控制的优点，同时由于引入了属性作为约束，可以实现细粒度的访问控制，而不会出现角色爆炸。

2.3 基于规则和策略的访问控制模型

E. Bertino 等人在 RBAC 模型的基础上提出了一种基于规则的授权模型。该模型提出了一种能同时表达静态约束和动态约束的约束描述语言，并给出了约束规则的一致性检查算法。朱玲等人还提出了一种基于约束的访问控制模型（CBAC），它采用显式授权和隐式授权相结合的安全机制，引入形式化语言来准确描述 CBAC 模型的安全策略，并制定统一的语法规范来描述用户属性约束和时间属性约束。

2.4 基于网络隐蔽通信的访问控制模型

网络访问控制模型是网络安全防范和保护的重要手段。现有的网络访问控制模型大多是通过加密实现的，在隐藏性和可控性方面存在缺陷，容易被发现和攻击。针对这一缺陷，文献［63］提出了一种新的访问控制模型——基于网络隐蔽通信的访问控制（NCC-AC）模型，该模型采用隐写技术实现访问控制，主要由隐写标签嵌入单元和隐写标签检测单元组成。隐写标签的设计主要包括隐写标签的内容设计和长度设计，以及隐写标签数字载体的选择。为了防止重放攻击，隐写标记中包含了时间戳。为了增强隐写标签的鲁棒性，对隐写标签进行

置乱后再嵌入。隐写标签嵌入单元主要对网络数据包进行截获和解析，并为目标对象嵌入隐写标签。隐写标签检测单元主要检测网络数据包中是否包含隐写标签，并根据访问控制规则判断数据包的流向，从而有效控制主体对客体的访问。

NCC-AC 模型的总体框架如图 1 所示。NCC-AC 模型主要由四部分组成：主题集、隐写标签嵌入（SLE）单元、隐写标签检测（SLD）单元和对象集。这四个部分共同作用，将信息隐藏技术和访问控制技术结合起来，形成一个完整的基于网络隐蔽通信的访问控制模型。主题集由 n 个主题组成，其中 n 是大于 0 的自然数。对象集由 m 个对象组成，其中 m 也是大于 0 的自然数。隐写标签嵌入单元的主要功能是为隐写标签选择一个合适的数字载体，然后将带有隐写标签的数据包重新发送到网络。隐写标签检测单元的主要功能是检测网络数据包中是否包含隐写标签。如果没有，丢弃数据包；如果有，提取隐写标签。根据隐写标签中的安全级别和访问控制规则确定网络数据包的目的地，从而有效控制主体对对象的访问。

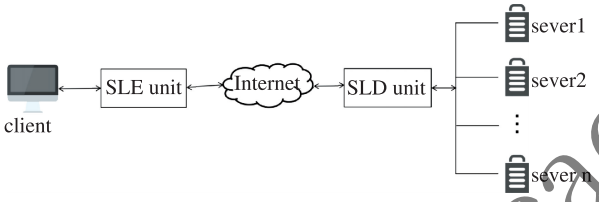


图 1　NCC-AC model framework

3　未来发展趋势及应用场景

3.1　区块链隐蔽通信建设

目前，基于区块链的隐蔽通道构建还处于探索阶段。本文对目前提出的具有代表性的区块链隐蔽通道进行了分析，并提出了四种分类。在相应的隐蔽通信领域，基于文本的存储隐蔽通道的开发起步较早，技术也相对成熟，可用于基于区块链的结构。隐蔽通道开发提供了技术支持，促进了该方向的初步应用探索，但其隐蔽容量低的缺陷可能难以克服。对于基于外部载体的隐蔽信道，链上和链外数据相对独立。虽然运营商摆脱了隐藏容量的限制，但使用图像、音频、视频等的实时性较差。一个低延迟的隐蔽信道的问题可能是值得探讨的。基于业务操作时间的隐蔽通道受区块链网络环境的限制太大，但区块交易本身的时间戳结构也为这类通道的研究带来了可能性。基于系统机制构建隐蔽通道的方案相对复杂，需要与具体区块链架构中的应用层、共识层、网络层等技术机制相结合。此类型可以看作是上述三种隐蔽通道的混合体，综合各种渠道的优势，很难对其进行有效防范。目前，对这类渠道的探索还不多，但其价值和潜力不容忽视。

3.2　区块链隐蔽通信的应用前景

接下来，从三个方面简要介绍区块链隐蔽通信渠道的应用前景。

（1）推动区块链应用在现实场景中的落地。

由于区块链本身的公开性和透明性，在实际场景的应用中必须考虑通信方式、用户隐私和安全等关键问题。基于区块链开辟隐藏通信路径的方案为解决这些实际问题提供了一种特殊的途径。区块链应用中的大多数安全通信方式往往集中在如何提高解密算法和通信协议的安全性上，而区块链与隐蔽通信通道的结合使得即使在区块链的开放平台上也可以传输数据和信息，而其他用户无法直接“知晓”。区块链隐蔽通信的思想将对区块链的实际应用产生积极影响。

（2）促进网络空间安全和隐蔽通信的发展。

近年来，随着城市信息化建设步伐的加快以及新一代信息技术的快速发展，网络空间安全被置于国家战略的重要位置，通信安全与隐私问题也受到越来越多的关注。区块链隐秘通信系统的设计理念在网络空间安全建设中发挥了积极作用。一方面，常用的隐蔽信息通信渠道可能依赖第三方服务（如公共社交媒体），通信信道的安全性和保密性将极大地影响传统的隐蔽通信方案，而分布式区块链网络作为通信介质不需要利用任何可识别的第三方来进行通信，大大降低了可用性攻击的安全风险；另一方面，对密钥管理、访问控制、隐私保护、信息隐藏等网络空间安全研究方向具有一定的参考和利用价值，可以为我国网络空间安全环境的建立作出贡献。

（3）为军事、情报等对通信安全要求极高的特殊场景提供安全保障。

在跨域作战中，提高作战效率、降低战争成本是关键，使用智能网络技术的需求必然会增加。同时，现代战争中对“制信息权”和“制智权”的争夺将成为决定战争走向的决定性因素。区块链技术已经在其中显示出其潜力。

4　结论

近年来，随着区块链技术的深入探索和普及，利用区块链技术构建隐蔽通信通道的探索也开始兴起，其应用潜力正引起更多研究者的关注。本文首先简要介绍了隐蔽通信技术的发展及其一般分类，详细梳理了近年来在区块链系统中构建隐蔽通信通道的技术研究现状，并对相关文献进行了整理和分析。其次，本文对访问控制

技术进行了分类和分析，并对每种访问控制技术的发展过程和优缺点也进行了说明。最后，对区块链隐蔽通信通道构建技术和检测方法的未来研究方向进行了展望，尝试整理出较为全面清晰的区块链隐蔽通信方向概述，为相关领域的研究者提供参考。

参考文献

[1] BORDERS K, PRAKASH A. Web tap: detecting covert web traffic [C]// Proceedings of the Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004: 110 – 120.

[2] LI Y, DING L, WU J, et al. Survey on key issues in networks covert channel [J]. Journal of Software, 2019 (30): 2470 – 2490.

[3] JOHNSON NF, JAJODIA S. Exploring steganography: seeing the unseen [J]. Computer, 1998 (31): 26 – 34.

[4] JOINSON A N. Self-disclosure in computer-mediated communication: the role of self-awareness and visual anonymity [J]. European Journal of Social Psychology, 2001 (31): 177 – 192.

[5] PETITCOLAS F A, ANDERSON R J. Evaluation of copyright marking systems [C]// Proceedings of the IEEE International Conference on Multimedia Computing and Systems. IEEE, 1999 (1): 574 – 579.

[6] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [J]. Decentralized Business Review, 2008: 21260.

[7] YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. Acta Autom Sinica, 2016, 42 (4): 481 – 494.

[8] Zhu Leihuang, Gao Feng. Survey on privacy preserving techniques for blockchain technology [J]. Journal of Computer Research and Development, 2017 (54): 2170 – 2186.

[9] SIMMONS G J. The prisoners' problem and the subliminal channel [C]// Advances in Cryptology: Proceedings of Crypto 83, 1984: 51 – 67.

[10] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof-systems [J]. Journal of Symbolic Logic, 56 (3): 1092.

[11] RIVEST R L, ADLEMAN L, DERTOUZOS M L, et al. On data banks and privacy homomorphisms [J]. Foundations of Secure Computation, 1978 (4): 169 – 180.

[12] YAO A C. Protocols for secure computations [C]//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). IEEE, 1982: 160 – 164.

[13] BRASSARD G, CHAUM D, CRÉPEAU C. Minimum disclosure proofs of knowledge [J]. Journal of Computer and System Sciences, 1988 (37): 156 – 189.

[14] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]// Proceedings of the Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, 2001: 552 – 565.

[15] DWORK C, ROTH A. The algorithmic foundations of differential privacy [J]. Foundations and Trends in Theoretical Computer Science, 2014 (9): 211 – 407.

[16] MILLEN J K. Covert channel capacity [C]// 1987 IEEE Symposium on Security and Privacy. IEEE, 1987: 60.

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

[18] LIU M D, CHEN Z N, SHI YJ. Research progress of blockchain in data security [J]. Chinese Journal of Computers, 2021, 44 (1): 1 – 27.

[19] CHEN J F. Review of Image Steganalysis Based on Deep Learning [J]. Journal of Software 2020 (32): 551 – 578.

[20] QI W, DING W, WANG X, et al. Construction and mitigation of user-behavior-based covert channels on smartphones [J]. IEEE Transactions on Mobile Computing, 2017 (17): 44 – 57.

[21] MOHAMED E E, MNAOUER A B, BARKA E. PSCAN: a port scanning network covert channel [C]// 2016 IEEE 41st Conference on Local Computer Networks (LCN). IEEE, 2016: 631 – 634.

[22] GURI M, MONITZ M, MIRSKI Y, et al. Bitwhisper: covert signaling channel between air-gapped computers using thermal manipulations [C]// 2015 IEEE 28th Computer Security Foundations Symposium. IEEE, 2015: 276 – 289.

[23] KANG X, HUANG J, SHI Y Q, et al. DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003 (13): 776 – 786.

[24] MALVAR H S, FLORÊNCIO D A. Improved spread spectrum: a new modulation technique for robust watermarking [J]. IEEE Transactions on Signal Processing, 2003 (51): 898 – 905.

[25] FEI C, KUNDUR D, KWONG R H. Analysis and design of watermarking algorithms for improved resistance to compression [J]. IEEE Transactions on Image Processing, 2004 (13): 126 – 144.

[26] JIN X, KRISHNAN R, SANDHU R. A unified attribute-based access control model covering DAC, MAC and RBAC [C]// Data and Applications Security and Privacy XXVI: 26th Annual IFIP WG 11. 3 Conference, 2012: 41 – 55.

[27] JIN X. Attribute-based access control models and implementation in cloud infrastructure as a service [J]. Dissertations & Theses-Gradworks, 2014.

[28] ZHU Y, HUANG D, HU C J, et al. From RBAC to ABAC: constructing flexible data access control for cloud storage services [J]. IEEE Transactions on Services Computing, 2014 (8): 601 – 616.

[29] WEN S J. Design of access control model based on network convert communication [D]. Zhenjiang: Jiangsu University of Science and Technology, 2015.

[30] WANG F Y. Military blockchain: from asymmetric warfare to symmetric peace [J]. Journal of Command and Control, 2018 (4): 175 - 182.

[31] SONG S, PENG W. BLOCCE +: an improved blockchain-based covert communication approach [J]. Journal of Chongqing University of Technology (Natural Science), 2020 (34): 238 - 244.

[32] ZHANG L, ZHANG Z, WANGW, et al. A covert communication method using special bitcoin addresses generated by vanitygen [J]. Computers, Materials & Continua, 2020 (65): 495 - 510.

[33] BARTOLETTI M, POMPIANU L. An analysis ofBitcoin OP_ RETURN metadata [C]//International Conference on Financial Cryptography and Data Security, 2017: 218 - 230.

[34] LUO X, ZHANG P, ZHANG M, et al. A novel covert communication method based on bitcoin transaction [J]. IEEE Transactions on Industrial Informatics, 2021 (18): 2830 - 2839.

[35] SI C X, LI R, GAO F, et al. Covert data transmission mechanism based on dynamic label in blockchain [J]. Xi' an Dianzi Keji Daxue Xuebao, 2020 (47): 94 - 102.

[36] TIAN J, GOU G, LIU C, et al. DLchain: a covert channel over blockchain based on dynamic labels [C]// Information and Communications Security: 21st International Conference, 2019: 814 - 830.

[37] SIDIQ M F, WIBOWO F M, WIBOWO M, et al. Secret and trustable communication channel over blockchain public ledger [C]//2021 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT). IEEE, 2021: 371 - 376.

[38] FIONOV A. Exploring covert channels in bitcoin transactions [C]// 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). IEEE, 2019: 59 - 64.

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

[40] FRKAT D, ANNESSI R, ZSEBY T. Chainchannels: private botnet communication over public blockchains [C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1244 - 1252.

[41] GUO Z, SHI L, XU M, et al. MRCC: a practical covert channel over Monero with provable security [J]. IEEE Access, 2021 (9): 31816 - 31825.

[42] LAN Y, ZHANG F, TIAN H. Using monero to realize covert communication [J]. Journal of Xidian University, 2020 (47): 19 - 27.

[43] BASUKI A I, ROSIYADI D. Joint transaction-image steganography for high capacity covert communication [C]//2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA). IEEE, 2019: 41 - 46.

[44] ABDULAZIZ M, ÇULHA D, YAZICI A. A decentralized application for secure messaging in a trustless environment [C]// 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT). IEEE, 2018.

[45] ZHANG L, ZHANG Z, JIN Z, et al. An approach of covert communication based on the Ethereum whisper protocol in blockchain [J]. International Journal of Intelligent Systems, 2021 (36): 962 - 996.

[46] ZHANG Z, ZHANG L, RASHEED W, et al. The research on covert communication model based on blockchain: a case study of Ethereum' s whisper protocol [C]// Proceedings of the Frontiers in Cyber Security: Third International Conference, 2020: 215 - 230.

[47] RECABARREN R, CARBUNAR B. Tithonus: a bitcoin based censorship resilient system [J]. arXiv preprint arXiv: 1810. 00279, 2018.

[48] LI Y, DING L, WU J, et al. Research on a new network covert channel model in blockchain environment [J]. Journal on Communications, 2019 (40): 67 - 79.

[49] ZHANG Y, WANG J, HE X, et al. Blockchain-based access control mechanism in electronic evidence [C]//Proceedings of the Blockchain Technology and Application: Third CCF China Blockchain Conference, 2020: 17 - 33.

[50] GAI K, WU Y, ZHU L, et al. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks [J]. IEEE Internet of Things Journal, 2019 (6): 7992 - 8004.

[51] ZHANG Y, GAI K, XIAO J, et al. Blockchain-empowered efficient data sharing in Internet of Things settings [J]. IEEE Journal on Selected Areas in Communications, 2022 (40): 3422 - 3436.

[52] MILLER M L, DOËRR G J, COX I J. Applying informed coding and embedding to design a robust high-capacity watermark [J]. IEEE Transactions on Image Processing, 2004 (13): 792 - 807.

[53] WU M, LIU B. Data hiding in image and video. I. Fundamental issues and solutions [J]. IEEE Transactions on Image Pro-

cessing, 2003 (6): 12.

[54] OUADDAH A, ELKALAM A A, OUAHMAN A A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT [C]//Proceedings of the Europe and MENA Cooperation Advances in Information and Communication Technologies, 2017: 523 - 533.

[55] XU R, CHEN Y, BLASCH E, et al. Blendcac: a smart contract enabled decentralized capability-based access control mechanism for the IoT [J]. Computers, 2018 (7): 39.

[56] ZHANG Y, KASAHARA S, SHEN Y, et al. Smart contract-based access control for the Internet of Things [J]. IEEE Internet of Things Journal, 2018 (6): 1594 - 1605.

[57] NAKAMURA Y, ZHANG Y, SASABE M, et al. Exploiting smart contracts for capability-based access control in the Internet of Things [J]. Sensors, 2020 (20): 1793.

[58] KUHN D R, COYNE E J, WEIL T R, et al. Adding attributes to role-based access control [J]. Computer, 2010 (43): 79 - 81.

[59] COYNE E, WEIL T R. ABAC and RBAC: scalable, flexible, and auditable access management [J]. IT Professional, 2013 (15): 14 - 16.

[60] JIN X, KRISHNAN R, SANDHU R. A role-based administration model for attributes [C]// Proceedings of the First International Workshop on Secure and Resilient Architectures and Systems, 2012: 7 - 12.

[61] GAI K, WU Y, ZHU L, et al. Privacy-preserving energy trading using consortium blockchain in smart grid [J]. IEEE Transactions on Industrial Informatics, 2019 (15): 3548 - 3558.

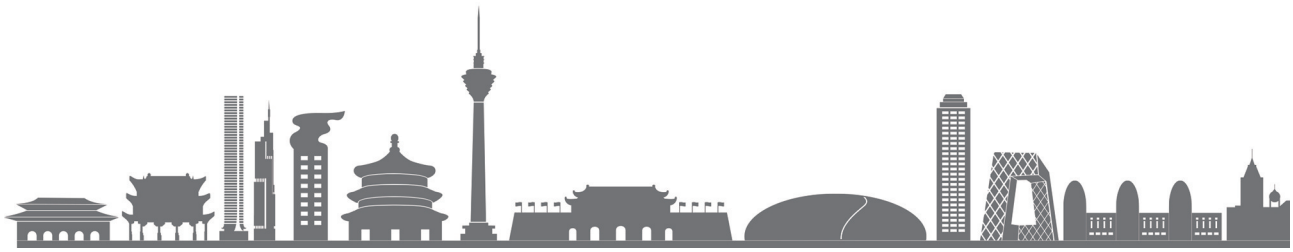
[62] QIU M, CAO D, SU H, et al. Data transfer minimization for financial derivative pricing using Monte Carlo simulation with GPU in 5G [J]. International Journal of Communication Systems, 2016 (29): 2364 - 2374.

(收稿日期: 2023 - 04 - 26)

作者简介:

张宏 (1999 -), 女, 硕士研究生, 主要研究方向: 区块链安全、隐私保护。

郭云伟 (1998 -), 男, 硕士研究生, 主要研究方向: 区块链安全、访问控制。



版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部