基于交易构造和转发机制的区块链网络隐蔽通信方法

熊礼治[1,2]，朱蓉[1]，付章杰[1,2]

（1. 南京信息工程大学计算机学院、软件学院、网络空间安全学院，江苏 南京 210044；
2. 数字取证教育部工程研究中心，江苏 南京 210044）

摘 要：针对现有存储型区块链网络隐蔽通信方案存在含密交易多副本、永久存储的问题，以及现有时间型方案隐藏容量低的问题，提出了一种基于交易构造和转发机制的区块链网络隐蔽通信方法。首先发送方借助交易构造机制创建无效交易，并将秘密信息嵌入其中，再利用交易转发机制向邻居节点发送无效交易，形成隐蔽通信信道模型，使含密交易在节点间传播且不存于区块链账本中，达到信息隐蔽安全传输的目的。实验结果表明，传输容量高于现有方案，单次通信时间减少至 2.5 s。

关键词：隐蔽通信；区块链网络；比特币交易构造；比特币交易转发；无效交易

中图分类号：TP309

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022161

Covert communication method of blockchain network based on transaction construction and forwarding mechanism

XIONG Lizhi[1,2], ZHU Rong[1], FU Zhangjie[1,2]

1. School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China
2. Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing 210044, China

Abstract: Aiming at the problems of multiple copies and permanent storage of the transactions containing secret information in the existing storage-based covert communication schemes in blockchain network, as well as the issue of low hidden capacity of the existing time-based schemes, a covert communication method of blockchain network based on transaction construction and forwarding mechanism was proposed. First, an invalid transaction was created by the sender with the help of the transaction construction mechanism, and the secret information was embedded in it, and then the transaction forwarding mechanism was used to send the invalid transaction to the neighbor nodes to form a covert communication channel model, enabling that the transactions containing secret information were spread between nodes and did not exist in the blockchain ledger, so as to achieve the purpose of information concealment and safe transmission. Experimental results show that the transmission capacity of the proposed method is higher than that of the existing schemes, and the single communication time is reduced to 2.5 s.

Keywords: covert communication, blockchain network, bitcoin transaction construction, bitcoin transaction forwarding, invalid transaction

0 引言

在当今信息爆炸的时代，用户通信的隐私和信息的安全传输越来越被重视。传统的加密通信方式是直接将明文转换成密文来实现通信。但是，密文容易引起攻击方的注意，使攻击方试图破解或者破坏密文信息，阻碍通信传输。因此，隐蔽通信提供了一种能让秘密信息的通信过程不被察觉的解决方案。

隐蔽通信模型最早源于 Simmons[1]提出的囚徒模型，将其扩展到计算机网络通信[2]中，如图 1 所示，可以抽象为 Alice 与 Bob 通过接入网络的计算机进行交流，Alice 需要选择一个看似平常的消息

收稿日期：2022−04−01；**修回日期：**2022−08−03

基金项目：国家重点研发计划基金资助项目（No.2021YFB00900）

Foundation Item: The National Key Research and Development Program of China (No.2021YFB00900)

M，将秘密信息 m 使用密钥加密后嵌入载体 M 中，并且不改变 M 原有的特性，使攻击方 Wendy 无法获悉通信双方的身份，并且就算截取到载体 M 也无法获得秘密信息。

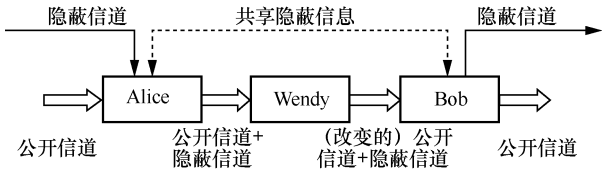

图 1　网络通信中的囚徒模型

现有网络系统中的存储型隐蔽信道主要运用网络通信协议的冗余部分，例如在网络协议、网络数据包头部的保留字段嵌入秘密信息；时间型隐蔽信道不改变网络数据包的信息内容，它运用约定的协议数据单元中网络流量的时间特征（例如，数据包到达的顺序或者规定时间内数据包到达的数量等），来传递秘密信息。

随着科学技术的迅速发展，传统的网络隐蔽信道面临若干挑战。1) 存储型隐蔽信道的可靠性和隐蔽性依赖于网络数据包的传输，容易被支持向量机方法[3]检测，被基于内容的方法识别[4]，被通信归一化等基于内容修改的新技术消除[5-6]。2) 时间型隐蔽信道受网络环境影响很大，容易被数据延迟、数据包丢失、噪声等问题干扰。3) 传统的网络隐蔽信道中，通信双方都采用静态且单一的路径实现直接通信，其匿名性很难保证。

2009 年，比特币[7]一词首次被提出，从中引申出了区块链的概念，区块链是一个由对等（P2P, peer to peer）节点共同参与的数据共享，不可篡改且不可伪造的分布式数据库系统，不存在中心节点，由一串利用密码学方式生成的数据区块组成，每个区块中包含交易、时间戳、上一区块的哈希、困难目标等信息，从创世区块开始通过哈希指针连接到当前区块，数据结构类似于链表。比特币网络中的所有节点都包含这些区块，整个网络被视为包含交易记录的分布式账本。账本中的交易通过比特币用户的公钥地址完成，每个用户可拥有多个公钥地址，且地址与实际身份无关。因此，比特币区块链具备数据同步、安全可信、匿名性强、去中心化的特点，是构建隐蔽信道的天然载体。

然而，正是因为区块链具有数据可追溯、永久存证[8]的特性，在区块链中构建隐蔽信道存在一些问题。1) 新产生的交易和区块需要在全网节点间进行广播，网络中的所有节点都能查看交易和区块内容；2) 交易和区块被验证上链，意味着隐蔽通信的“证据”被永久记录在区块链账本中，所有用户都可以通过相关的应用程序编程接口（API, application programming interface）无限次地获取该“证据”，这对隐蔽通信的隐藏算法要求相当高。

针对区块链网络隐蔽通信技术存在的问题，本文设计了一种基于交易构造和转发机制的区块链网络隐蔽通信方法。在本文方法中，隐蔽通信双方首先利用比特币底层节点的连接机制成为邻居节点；然后发送方借助比特币交易的构造机制创建无效交易，并将秘密信息嵌入其中；最后发送方利用比特币交易的广播机制向接收方发送含有秘密信息的无效交易。由于比特币交易转发机制的泛洪广播特性，每次隐蔽通信中，发送方发出的包含秘密信息的无效交易只在其邻居节点之间传播。除隐蔽通信接收方之外的节点在交易验证不通过后会立刻抛弃该交易，因此，无效交易不会永久存储在区块链账本中，隐蔽通信的“证据”在通信结束后立即消失。本文方法不仅解决了现有区块链网络中隐蔽通信技术存在的问题，并且在一定程度上扩大了隐藏容量，提高了通信效率。

本文贡献点可以总结如下。1) 本文方法中传递秘密信息使用的交易不会广播给区块链网络中的所有节点，并且此交易不会永久存储在区块链的账本中，隐蔽通信不会留下“证据”。2) 利用比特币的交易构造机制来构造无效交易，只需要保证数据格式和长度与正常交易相同，所有可修改字段都能用于嵌入秘密信息，扩大了隐蔽通信信道的隐藏容量。3) 接收方作为发送方的邻居节点，在发送方广播交易的第一轮能立刻收到无效交易，不需要等待交易广播给所有节点，隐蔽通信的通信效率得到了提升。

1　研究现状

当前的比特币区块链网络隐蔽通信方案可以分为存储型和时间型 2 种。现有的存储型隐蔽通信方案中，包含秘密信息的交易在全网范围的节点间广播，且最终会被永久存储在区块链的账本中，任何人可随时查看，因此在构建存储型隐蔽通信信道时，需要特别考虑其隐蔽性和不可感知性，难以兼顾隐藏容量高、通信效率快和隐蔽性强 3 种性质。

Partala[9]通过牺牲隐蔽通信信道的隐藏容量和

通信效率达到强隐蔽性，首次提出使用比特币地址的最低有效位（LSB, least significant bit）嵌入秘密信息，在每个区块中按顺序存放一笔包含秘密信息的交易，从而初步完成了隐蔽通信，为相关研究提供了方向。不过该方案在一个区块生成的时间间隔内仅传递了 1 bit 的秘密信息，信道的隐藏容量低，同时，Cao 等[10]在区块链中提出了一种基于哈希链的隐蔽数据嵌入方案，保证了嵌入数据的隐蔽性和安全性，但是每条交易也只能传递 1 bit 的秘密信息，此类方案在效率和成本上均不尽人意[11]。

DLchain[12]和 ChainChannel[13]使用秘密信息代替签名算法中的私钥和随机数，保证了一定的嵌入容量和信道的隐蔽性，但是接收方在筛选和提取秘密信息时计算量较大，降低了信道的效率。

Gao 等[14]、Plohmann 等[15]、吕婧淑等[16]使用比特币交易中的默认存储字段 OP_RETURN 和 coinbase 嵌入秘密信息，只要保证数据格式和字段长度正常，就能达到高隐蔽性和较高隐藏容量，但默认存储字段比较特殊，很容易引起攻击方的注意，导致隐蔽信道被干扰。Zhang 等[17]利用 vanitygen 生成特殊比特币地址，地址中嵌入 base58 编码的信息，并将特殊地址的索引记录在 OP_RETURN 中，从而提高了信息嵌入效率以及默认存储字段的隐蔽性。

上述关于区块链网络中存储型隐蔽通信的方案中，包含秘密信息的交易都在区块链账本中永久存储，并且任何人都可以申请查看相关交易。随着技术的发展和研究的深入，攻击方有足够的时间收集数据进行分析，使以这种方案传输的秘密信息有泄露的风险。

现有的时间型隐蔽通信方案中，李彦锋等[18]提出基于业务操作时间间隔的区块链网络隐蔽信道，利用区块链中的交易发送间隔的不同作为调制方式来传递秘密信息，其网络流量波动较大，与发送正常交易时的网络流量不同，隐蔽性很低。吕婧淑等[16]提出的地址广播信道通过比特币交易中某些参数的排列方式与编码方式进行映射来传递秘密信息，隐蔽性极高，但是其容量和效率完全依赖于地址的个数，可用性和可扩展性不高。

另外，以太坊的研究主要集中在它的安全通信协议——whisper 协议上，whisper 协议中特殊的数据包格式和广播机制可以保证通信接收方的匿名性。Abdulaziz 等[19]利用 whisper 协议构造了去中心化的应用程序，秘密信息可以在其中安全匿名地传输。Lee 等[20]在此基础上提出了一种新的通信应用程序，秘密信息通过 whisper 协议进行传输，解决了传统隐蔽通信中的数据伪造和隐私侵犯等问题。Zhang 等[21]使用 whisper 协议中的 payload 存储秘密信息，生成的索引填充在 padding 字段，从而在已有方案的基础上增加了隐蔽通信的隐蔽性。

2 预备知识

比特币以去中心化为基础，信息由网络中的各个节点共同记录和维护。一旦网络中的某个节点花费算力找到满足比特币共识机制的随机值，就能获得新区块的记账权，选择本地交易池中的交易打包进新区块，通过比特币特有的广播机制向网络中的其他节点广播。本文提出的区块链网络隐蔽通信方法涉及比特币节点连接机制、比特币广播机制，以及比特币交易，相关介绍如下。

2.1 比特币节点连接机制

比特币网络的一个新节点为了能够获取网络中的信息，必须主动和网络中已存在的节点进行连接。连接方式有以下 2 种。

1) 使用种子节点。新节点首先连接比特币网络所提供的域名系统种子（DNS, domain name system seed）节点，向其请求所有比特币活跃节点的 IP 地址列表，新节点挑选活跃的比特币节点进行连接。

2) 使用-connect 选项。新节点在加入网络之前，在配置文件中使用-connect 选项指定已知的若干个活跃的比特币节点作为自己的邻居节点。

新节点 A 确定好连接的对等节点 B 后，会向目标节点 B 发送 version 消息，目标节点 B 每次收到 version 后必须回复 verack 消息表示收到。若目标节点 B 同意被连接，会主动向新节点 A 发送自己的 version 消息，新节点 A 向目标节点 B 回复 verack 消息，即新节点 A 和目标节点 B 通过图 2 所示的“握手”通信建立连接。

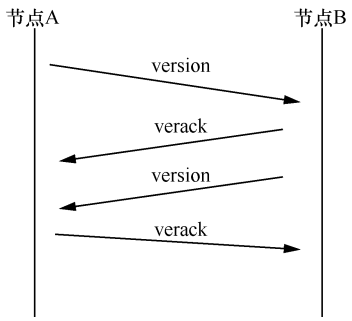

图 2 节点“握手”通信过程

连接完成后，节点 A 向节点 B 发出包含自己 IP 的 addr 消息并要求节点 B 向其邻居节点进行转发，使网络中的更多节点知道新节点 A 的加入，并且发出一个 getaddr 消息，要求节点 B 返回已知的活跃节点以便于寻找更多的节点进行连接，如图 3 所示。

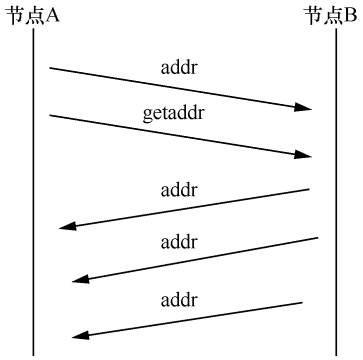

图 3　地址请求过程

已经连接网络的节点会定期发送 addr 信息给邻居节点来维持连接，若某一节点超过 90 min 没有与网络中的其他节点进行通信，则默认此节点断开网络，连接此节点的其他节点会立刻寻找新的活跃节点进行连接。

2.2　比特币广播机制

区块链网络中的所有新交易和区块在创建后都必须向网络中其他节点进行广播，在获得足够多节点的确认之后，新增的交易和区块才能被写入区块链账本中。但是比特币的每日交易量大约有 60 万，若随意进行交易广播会造成网络的拥堵和崩溃，为了使传播和确认效率最大化，比特币网络使用 Gossip 协议[22]来在各个节点之间同步交易以及区块的信息。Gossip 协议被设计用来在分布式数据库的多个节点之间同步和复制数据，让数据到达网络中的各个节点，达成“最终一致性”。

在比特币网络中，Gossip 协议可认为是包含以下 3 个过程的一个简短循环，直到网络中的每个节点同步了相同的信息，如图 4 所示。1) 从新交易或区块的信息源开始，选择一个广播周期，向其连接的邻居节点发送 inv 消息，其中包括新交易或新区块的哈希值；2) 在每个节点接收消息后，先遍历本地存储的交易或区块的哈希值，若本地存在，则忽略；若不存在，则发送 getdata 消息请求此哈希值的全部数据，以验证交易或区块的合法性；3) 验证合法后，在下一周期里，向其他的邻居节点发送相同的 inv 消息。

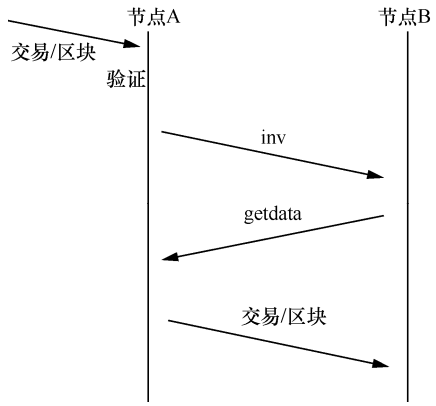

图 4　比特币广播过程

2.3　比特币交易

区块链交易在 2 个“地址”之间进行可靠的、具有公信力的数据传递。简单而言，就是原比特币的拥有者授权把比特币转账给他人，而新拥有者也可以继续授权，转账给该区块链网络中的其他人，这个转账的过程就是交易。这里说的“地址”是由用户的公钥通过椭圆加密算法计算得到的，对外公开，用于发送或接收交易。每个用户可拥有多个公钥地址，私钥由用户本人保存，用于对交易进行签名。

根据比特币源码中的 checktransaction 函数可知，一条有效的比特币交易需要满足以下所有条件，若有其中任意一条不满足，则为无效交易。

1) 所有字段的语法和数据格式正确。

2) 锁定时间在规定范围内。

3) 交易大小不低于 100 B。

4) 解锁脚本能正确解锁前置交易。

5) 每一个输入的前置交易不能在节点本地的交易池中。

6) 每一个输入必须要有其前置交易存在，并且未被花费。

7) 输入的总值大于输出的总值。

8) 交易费用不能小于当前网络的最小值。

比特币的交易数据格式如表 1 所示，包括版本号、输入输出数量、输入输出数组和锁定时间。

表 1　　比特币的交易数据格式

字段尺寸/byte	描述	说明
4	version	交易协议版本号
1+	tx_in_count	输入交易的数量
41+	tx_in	一个或多个输入交易组成的数组
1+	tx_out_count	输出交易的数量
8+	tx_out	一个或多个输出交易组成的数组
4	lock_time	交易锁定时间

交易输入列表的数据格式如表 2 所示，包括前向交易的哈希值和索引、解锁脚本及其长度和交易序列号。

表 2 交易输入列表的数据格式

字段尺寸/B	描述	说明	是否可自定义
32	TX hash	前向交易的哈希值	是
4	output index	前向交易的索引	是
1～9	unlocking-script size	解锁脚本的长度	是
可变长度	unlocking-script	解锁脚本	是
4	sequence	交易序列号	否

交易输出列表的数据格式如表 3 所示，包括每笔交易的比特币数量、锁定脚本及其长度。

表 3 交易输出列表的数据格式

字段尺寸/B	描述	说明	是否可自定义
8	amount	交易的比特币数量	是
1～9	locking-script size	锁定脚本的长度	是
可变长度	locking-script	锁定脚本	是

3 隐蔽通信方法设计

本节首先定义一个基于交易构造和转发机制的区块链网络隐蔽通信模型，然后以此模型为基础，以比特币的交易字段为隐蔽通信载体，利用比特币的交易转发机制在比特币底层的 P2P 网络上构建一个基于交易构造和转发机制的区块链网络隐蔽通信信道。在比特币区块链网络中，同时拥有路由、交易转发和交易验证的节点只有全节点，因此，模型中出现的节点默认为比特币全节点。

3.1 隐蔽通信模型

基于交易构造和转发机制的区块链网络隐蔽通信模型包含信息发送方、信息接收方、秘密信息、交易传播。对秘密信息的操作包括信息处理、嵌入、提取和恢复，交易传播包括有效交易的广播和上链以及无效交易的广播和抛弃。整体隐蔽通信模型分为伪装阶段和传输阶段两部分。

伪装阶段的隐蔽通信模型如图 5 所示。

1) 隐蔽通信的发送方和接收方通过节点连接机制加入比特币网络，进行正常的路由通信。假设发送方 P_s 有 x 个一级邻居节点，节点关系表示为 P_{s-x}，如式(1)所示。

$$P_{s-x}=\{<P_s,P_1>,<P_s,P_2>,\cdots,<P_s,P_r>,\cdots,<P_s,P_x>\},x\neq s \tag{1}$$

其中，P_r 表示接收方。

假设其一级邻居节点的邻居节点也有 x 个，则发送方 P_s 的二级邻居节点关系表示为 P_{s-x-x}，如式(2)所示。

$$\begin{aligned}P_{s-x-x}=\{&<P_s,P_1<P_1,P_{11}>,<P_1,P_{12}>,\cdots,<P_1,\\&P_{1x}>>,\cdots,<P_s,P_r<P_r,P_{r1}>,\cdots,<P_r,P_{rx}>>,\cdots,\\&<P_s,P_x<P_x,P_{x1}>,\cdots,<P_x,P_{xx}>>\},x\neq s\end{aligned} \tag{2}$$

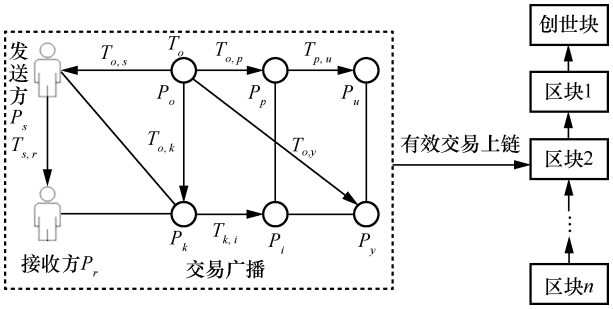

图 5 伪装阶段的隐蔽通信模型

2) 通信双方节点进行正常交易的广播和验证，维护网络稳定。比特币网络使用 Gossip 协议，信息由起始节点发送给一级邻居节点，再由一级邻居节点发送给二级邻居节点，迭代转发，直到所有的节点都收到信息。假设网络中节点 P_o 向邻居节点 P_s 发送交易 TX 表示为 $T_{o,s}$，如式(3)所示。

$$T_{o,s}=P_o\overset{\mathrm{TX}}{\rightarrow}P_s \tag{3}$$

节点 P_s 对收到的交易进行验证，将符合验证规则的交易继续转发给 P_o 的二级邻居节点（即 P_s 的一级邻居节点），那么节点 P_o 发送一条有效交易 TX 在网络中的传播可以表示为 T_o，如式(4)所示。

$$\begin{aligned}T_o=(&T_{o,1},T_{o,2},\cdots,T_{o,s},\cdots,T_{o,x},T_{1,11},\cdots,\\&T_{2,21},\cdots,T_{s,s1},\cdots,T_{s,sr},\cdots,T_{s,sx},\cdots)\end{aligned} \tag{4}$$

3) 有效交易上链。网络中的节点验证交易 TX 有效后，将其放入本地的交易池。矿工得到新区块的记账权后，选择本地交易池中的交易打包进新区块，将新区块添加到已经形成链式存储的区块之后。

传输阶段的隐蔽通信模型如图 6 所示。

1) 发送方利用交易的构造机制构造无效交易。首先，发送方 P_s 利用某种加密方法 E 加密原始秘密信息 $M(m_1,m_2,\cdots,m_n)$，再通过某种编码方式 R 处理密文 M'，使它能更好地嵌入交易中，该过程分别

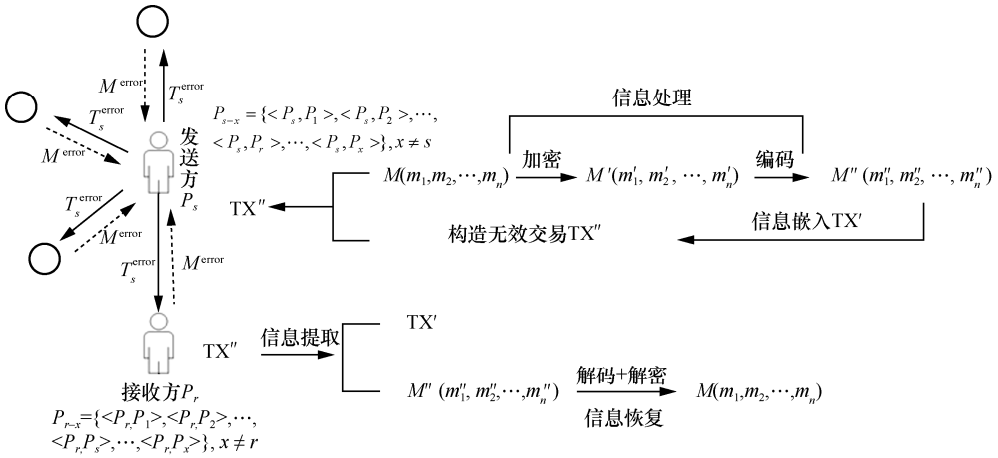

图 6　传输阶段的隐蔽通信模型

表示为 $M\xrightarrow{\text{E}}M'$ 和 $M'\xrightarrow{\text{R}}M''$，如式(5)和式(6)所示。

$$M\xrightarrow{\text{E}}M'=(m_1,m_2,\cdots,m_n)\xrightarrow{\text{E}}(m_1',m_2',\cdots,m_n') \tag{5}$$

$$M'\xrightarrow{\text{R}}M''=(m_1',m_2',\cdots,m_n')\xrightarrow{\text{R}}(m_1'',m_2'',\cdots,m_n'') \tag{6}$$

编码完成后，通过某种方案 F 将 M'' 嵌入无效交易 TX′ 中，得到含密无效交易 TX″，过程表示为 $M'',\text{TX}'\xrightarrow{\text{F}}\text{TX}''$，如式(7)所示。

$$M'',\text{TX}'\xrightarrow{\text{F}}\text{TX}''=(m_1'',m_2'',\cdots,m_n'')\xrightarrow{\text{F}}\text{TX}'' \tag{7}$$

2) 发送方通过无效交易的转发验证机制，向接收方传输秘密信息。发送方 P_s 得到处理完毕的含密无效交易 TX″ 后，向包含接收方节点 P_r 在内的邻居节点发送此交易，表示为 T_s^{error}，如式(8)所示。

$$T_s^{\text{error}}=(T_{s,1},\cdots,T_{s,r},\cdots,T_{s,x}) \tag{8}$$

由于 TX″ 是不符合验证规则的无效交易，因此包括接收方 P_r 在内的邻居节点会抛弃该交易，并且返回抛弃信息给发送方 P_s，验证交易无效后返回的抛弃信息表示为 M^{error}，如式(9)所示。

$$M^{\text{error}}=\text{TX}''\rightarrow\text{Invalid} \tag{9}$$

3) 接收方提取信息。接收方 P_r 收到无效交易后先根据交易的公钥判断是否由发送方构造，若是，根据协商好的方案 F 对应的提取方案 F′ 对 TX″ 进行提取，得到编码后的密文 M''，通过编码规则 R 对应的解码规则 R′，以及加密方法 E 对应的解密方法 E′ 对密文 M'' 进行解码，得到最终的秘密信息 $M(m_1,m_2,\cdots,m_n)$，过程分别表示为 $\text{TX}''\xrightarrow{\text{F}'}M'',\text{TX}'$ 和 $M''\xrightarrow{\text{R}',\text{E}'}M$，如式(10)和式(11)所示。

$$\text{TX}''\xrightarrow{\text{F}'}M'',\text{TX}'=\text{TX}''\xrightarrow{\text{F}'}(m_1'',m_2'',\cdots,m_n'') \tag{10}$$

$$M''\xrightarrow{\text{R}',\text{E}'}M=(m_1'',m_2'',\cdots,m_n'')\xrightarrow{\text{R}',\text{E}'}(m_1,m_1,\cdots,m_n) \tag{11}$$

3.2　隐蔽通信信道构建

根据以上隐蔽通信模型，构建隐蔽通信信道的方式如下。

首先，伪装阶段是指隐蔽通信的接收方节点先加入比特币网络，进行正常的路由通信以及交易（区块）的转发。

在区块链中有 n 个区块的前提下，接收方节点加入网络后，一条有效交易被转发上链的过程如下。

步骤 1　Alice 创建一个向 Bob 转账的有效交易 TX_1。

步骤 2　Alice 将构造好的交易 TX_1 交给网络中任意一个节点进行广播。

步骤 3.1　信息源节点根据 2.3 节的规则验证 TX_1 是否为有效交易，若为有效交易，则将交易 TX_1 放入本地的交易池中，并且转发给其一级邻居节点，执行步骤 3.2；若为无效交易，则抛弃交易 TX_1，并且给用户 Alice 返回信息表示交易被抛弃。

步骤 3.2　一级邻居节点接收到新交易 TX_1 后，也会对其进行验证，若有效，则将交易 TX_1 放入本地的交易池中，并将交易发送给二级邻居节点（此时接收方节点伪装成正常节点隐藏在二级邻居节点中），执行步骤 3.3；若无效，则抛弃交易并且向发送此交易的前一级节点返回交易无效的信息。

步骤 3.3　二级邻居节点（包括接收方节点）执行步骤 3.2 的操作，向下一级节点发送有效交易或者抛弃无效交易。

步骤 3.4 每一级邻居节点重复步骤 3.2 的操作，直到网络中的所有节点都接收到交易 TX_1。

步骤 4 网络中的某个矿工节点根据工作量证明协议（POW, proof of work）获得第 n+1 个区块的记账权后，将本地交易池中包括 TX_1 交易在内的 m 个交易打包成第 n+1 个区块，区块数据结构如图 7 所示。

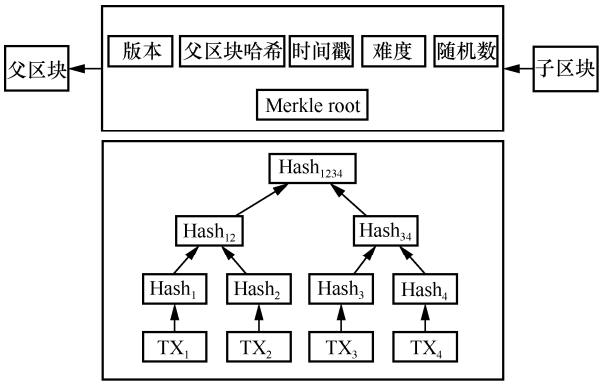

图 7 区块数据结构

步骤 5 矿工节点将打包好的区块广播到网络中。

步骤 6 网络中的其他节点对新生成的区块进行验证。

步骤 7 当新区块被全网大多数节点验证合法之后，其中包含的交易（包括 TX_1 交易）才被写入整个区块链账本。

发送方节点加入网络时，使用 2.1 节中的节点连接方法 2)，指定接收方节点作为自己的一级邻居节点，其他的邻居节点随机连接。发送方加入网络后和接收方节点类似，参与网络中的所有活动，维持网络稳定。至此，隐蔽通信的伪装阶段结束，如图 8 所示。

隐蔽通信的传输阶段由发送方节点创建包含秘密信息的无效交易 TX_2 开始，传输阶段分为信息嵌入阶段、交易广播阶段和信息提取阶段。

1) 信息嵌入阶段主要是根据 2.3 节中列举的条件来构造无效交易。为了简化发送方和接收方对信息的处理，选择将秘密信息编码后，作为交易相应字段的参数，直接嵌入发送方构造的无效交易中，如文献[14-15]。

发送方在构建无效交易时，可以将处理后的秘密信息嵌入比特币交易规定的所有可变字段，例如前置交易哈希、签名、接收方公钥等。但是，选择交易的所有可变字段进行秘密信息的嵌入会增加无效交易的特殊性。为了最大化隐蔽信道的不可感知性以及最大化单次通信的隐藏容量，本文把秘密信息嵌入用户可自定义字段中容量最大的解锁脚本（或锁定脚本）字段，如表 2 所示，且遵循其数据格式。

解锁脚本由数字签名、公钥和一些操作码组成，最后经过编码变成 hex 格式，这样可以确保只有持有私钥的用户才能将交易解锁，在构造多输入交易时，解锁脚本的长度会随着输入的个数线性增加。因此，交易包含的输入个数越多，可以用来进行数据嵌入的空间就越大。

当构造一个输入一个输出的有效交易时，转换为 hex 格式的解锁脚本大约占 100~120 B，如图 9 所示。

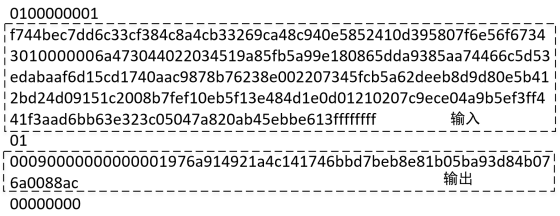

图 9 一个输入一个输出的有效交易

发送方先将秘密信息编码，然后在编码完的信息后加上 endflag 作为秘密信息结束的标志，未满

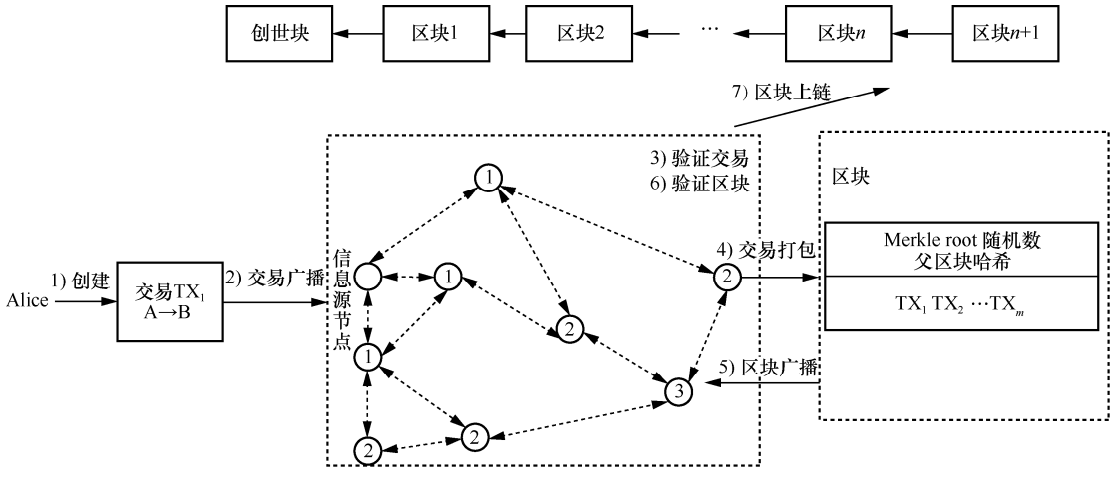

图 8 隐蔽通信的伪装阶段

足正常解锁脚本长度的部分使用冗余字段填补，保证字段长度为 100~120 B，如图 10 所示。

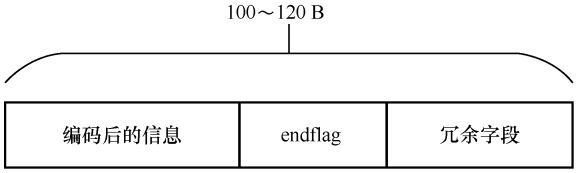

图 10　含密解锁脚本的生成

发送方将生成的解锁脚本使用接收方的公钥加密，嵌入无效交易中的解锁脚本字段，生成的无效交易如图 11 所示。

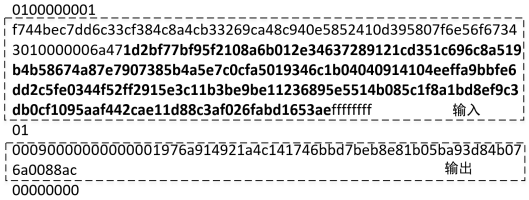

图 11　嵌入秘密数据后的无效交易

2) 交易广播阶段由发送方节点发起，向其一级邻居节点（包括接收方节点）发送构造的无效交易 TX_2，接收方收到交易 TX_2 后，对其进行验证，由于交易 TX_2 不满足有效交易的验证规则，因此其为一条无效交易。接收方再验证无效交易 TX_2 创建者的公钥，若公钥与发送方一致，则表示交易 TX_2 是一条包含秘密信息的无效交易，对它进行信息提取。其他一级邻居节点验证交易 TX_2 无效后将其抛弃，并且返回一条交易被拒绝的消息给发送方节点。

3) 信息提取阶段是指接收方节点收到发送方节点发送的含密无效交易后，用其私钥解密无效交易的解锁脚本，解密成功后，接收方根据 endflag 找到发送方编码后的秘密信息，使用通信双方约定的编码规则还原秘密信息。至此，隐蔽通信的传输阶段结束，如图 12 所示。

4　隐蔽通信信道分析

隐蔽信道的评价从 2 个方面进行：安全性和传输效率。安全性是指对于普通节点来说，包含秘密信息的无效交易是无法感知的，并且其特征在统计上不可区分，即在不影响网络通信和不被普通节点发觉的前提下进行秘密信息的传输。传输效率包括 2 个方面，一是信道单次通信的隐藏容量，二是信道单次通信所需的时间。本节将从安全性和传输效率 2 个方面分析本文提出的隐蔽通信信道。

4.1　安全性

4.1.1　抗检测性

在传统网络隐蔽通信中，通常从以下 2 个方面检测是否存在隐蔽信道。1) 分析网络流量。一些时间型隐蔽信道，通常以时间特性为调制方式，会在

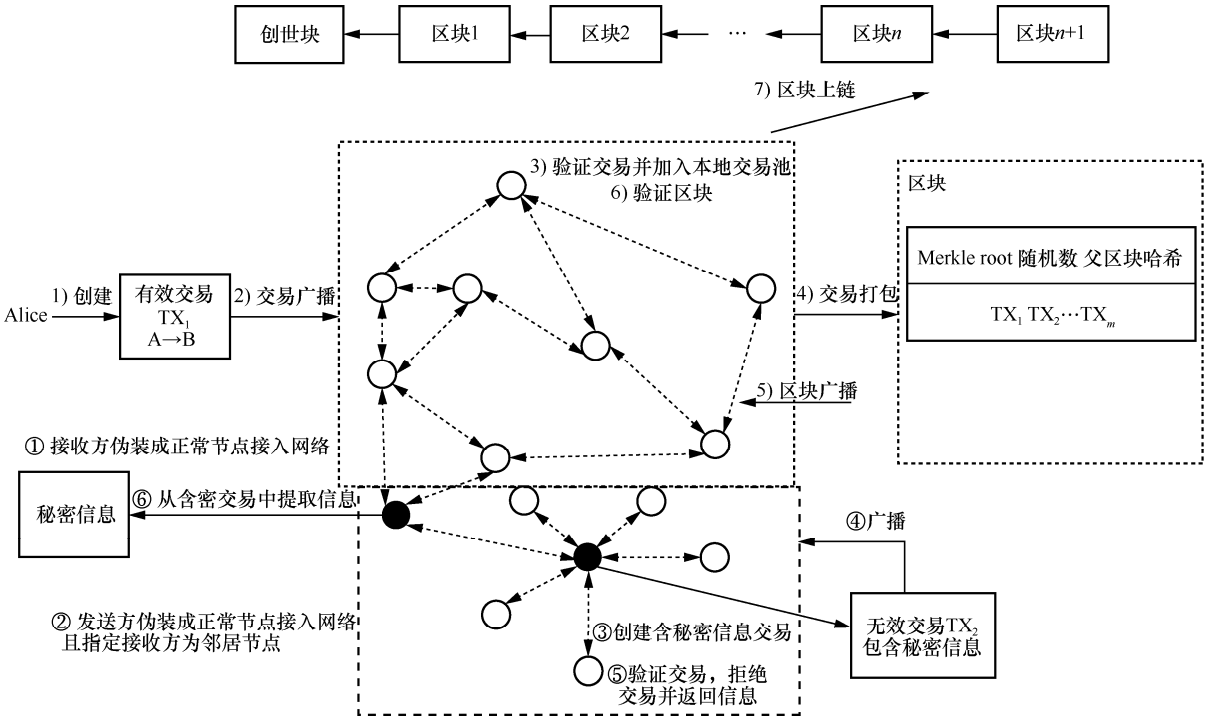

图 12　隐蔽通信的传输阶段

网络中造成短暂的流量异常，攻击方可以通过流量的波动情况检测出隐蔽信道。2) 分析数据包。一些存储型隐蔽信道，使用协议数据包的冗余字段嵌入秘密信息，攻击方可以根据数据包内容的规律性和相关性检测隐蔽信道。

在区块链网络中，由于嵌入数据时完全按照交易字段的数据格式，且交易内容经过已有规则层层加密，攻击方想要通过分析交易内容识别隐蔽信道比较困难，因此常用分析网络流量的方法检测隐蔽信道，即攻击方会持续监控网络中节点造成的流量波动。当发送方节点受到持续监控时，攻击方分析其发送交易的频率。假设比特币区块链的正常网络活动中，节点发送每条交易的正常时间间隔为 σ，5 min 内正常转发 ε 条交易，分别使用以下 3 种方案（方案 A、方案 B 和方案 C）在网络中发送秘密信息“001110110110”，造成的网络流量波动与正常情况的对比如图 13 所示。

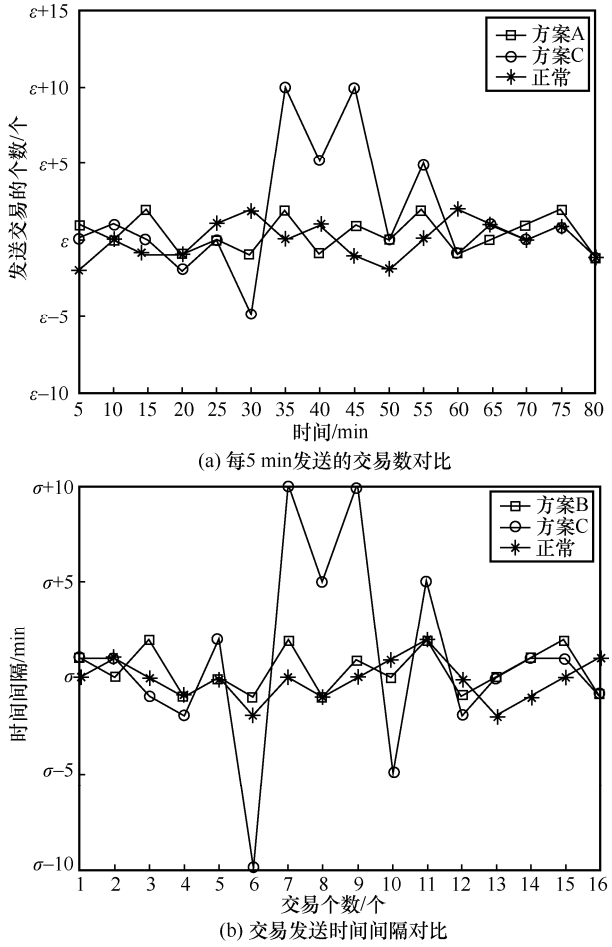

图 13 不同方案与正常网络流量对比

方案 A 发送方使用每 5 min 发送的交易个数“$\varepsilon-5,\varepsilon,\varepsilon+5,\varepsilon+10$”分别表示“00,01,10,11”，那么发送方在传递秘密信息时，每 5 min 的时间间隔内分别发送的交易个数为“$\varepsilon-5,\varepsilon+10,\varepsilon+5,\varepsilon+10,\varepsilon,\varepsilon+5$”。

方案 B 发送方使用发送交易的时间间隔“$\sigma-10,\sigma-5,\sigma+5,\sigma+10$”分别表示“00,01,10,11”，那么发送方在传递秘密信息时，发送交易的间隔为“$\sigma-10,\sigma+10,\sigma+5,\sigma+10,\sigma-5,\sigma+5$”。

方案 C 发送方使用本文方案将秘密信息嵌入无效交易中，在传递秘密信息时，仿照网络中正常的交易间隔 σ 发出含有秘密信息的无效交易。

从图 13(a)中可以发现，前 25 min 正常通信状态，每 5 min 的交易个数在 ε 上下波动；25~55 min 时，使用方案 A 时每 5 min 的交易个数显著增加，网络流量波动很大，直到 55 min 后通信结束，网络流量才趋于稳定。从图 13(b)中可以发现，在发送前 5 个交易时，方案 B 遵循正常交易发送的时间间隔，在 σ 上下波动；进入信息传递阶段，在发送第 6~第 11 个交易的时间内，发送交易的时间间隔与正常时间间隔区别较大，直到发送完第 11 个交易后通信结束，网络流量才趋于平缓。然而，使用本文方法的方案 C 在正常通信过程中夹杂着含密交易，整个过程不受时间性质的影响，与正常的交易频率相似，攻击方无法通过分析网络流量的方法检测到方案 C 使用的隐蔽信道。

4.1.2 不可感知性

为了确定网络中正常节点发送交易的时间间隔，通过调用比特币测试网络的开放接口 bitcoincore 接入 Bitcoin Testnet，设置探针节点监测邻居节点的活动状况。当监测 x 个邻居节点时，若它们在 h h 内向探针节点发送 y 条交易，那么网络中的节点每秒大约发送 N 条交易，如式(12)所示。

$$N=\frac{y}{3\,600xh} \tag{12}$$

实验设置探针节点对其 8 个邻居节点[23]进行监测，在 24 h 内收到了 275 440 条交易，因此可知，一个正常比特币网络节点每 2.5 s 转发一条交易。则隐蔽通信的发送方仿照正常发送交易的频率，每间隔 2.5 s 发送一条交易，将无效交易夹杂其中发送，不会造成网络流量的波动，对于其他节点来说是不可感知的。

另外，本文方案中的发送方节点和接收方节点是通过网络提供的协议正常加入比特币节点网络的，没有修改协议本身的内容，加入之后参与网络

正常活动，维护网络的稳定性。因此在伪装阶段，发送方节点和接收方节点都是无法感知的。在数据传输阶段，本文提出的隐蔽信道利用了无效交易作为秘密信息的载体，但是没有改变交易的数据格式和长度，因此不影响网络的正常通信。所以，对于普通节点来说，隐蔽信道是无法感知的。

由于比特币为公链性质的区块链，网络中的所有节点都能够随意加入和退出，它们对于交易和区块的广播没有第三方可以控制，因此会出现作恶节点——占用带宽以及发布不实消息、浪费计算资源的节点（广播无效交易也是其中之一）。然而，得益于交易转发机制的泛洪广播特性，作恶节点每一次的恶行只会影响其邻居节点，为了网络中节点的稳定，比特币网络设计了对邻居节点的惩罚机制，伪代码如算法 1 所示。

算法 1　邻居节点的惩罚算法

输入　节点编号 nodeID、设置的惩罚值 score、设置的惩罚阈值 threshold

输出　节点 A 是否与节点 B 连接

```
1) while(节点 A 受到作恶节点 B 影响) do
2)    if (节点 B 分数大于节点 A 的惩罚阈值)
3)    将节点 B 的分数减去节点 A 设置的惩罚值;
4)       if((节点 B 分数大于节点 A 的惩罚阈值)
5)       return;
6)       else
7)       断开与此节点连接 86 400 s;
8)       end if
9)    else
10)   断开与节点 B 连接 86 400 s;
11)   end if
12) end while
```

由算法 1 可以发现，当作恶节点发送一条恶意消息后，其邻居节点不一定会立即断开。只有当作恶节点的分数减少到阈值以下后，邻居节点会断开与它的连接，默认断开 24 h，之后断开的邻居节点可以重新连接。此时，作恶节点不会断开整个比特币网络，它会选择其他节点进行连接。

假设节点将惩罚阈值设为 T，惩罚值设为 S，那么它可以收到邻居节点发送的无效交易 M 条，如式(13)所示。

$$M=\frac{100-T}{S} \tag{13}$$

因此，隐蔽通信双方连接后，接收方在本地配置文件中将惩罚阈值调整为 $T<100-MS$，即可保持与发送方的稳定连接。

区块链网络中攻击方对于网络流量和交易的监测是通过部署探针节点完成的，假设整个网络中有 α 个节点，攻击方拥有 β 个节点，若想监测发送方发送的无效交易，攻击方必须作为发送方的邻居节点，因为无效交易会在第一轮转发后被抛弃。假设发送方有 γ 个邻居节点，那么攻击方作为发送方邻居节点的概率为 P_1，如式(14)所示，其中 C 表示组合数。以此类推，在第 i 轮中，攻击方有节点作为发送方邻居节点的概率为 P_i。

$$P_1=1-\frac{\mathrm{C}_{\alpha-\beta}^{\gamma}}{\mathrm{C}_{\alpha}^{\gamma}} \tag{14}$$

隐蔽通信中，若发送方有邻居节点断开连接，则替换新的邻居节点。当进行 V 轮通信时，攻击方节点在 V 轮中一直作为发送方邻居节点的概率为 P_V，如式(15)所示。P_V 随着通信轮次的增加而逐步减小，因此隐蔽信道对于攻击方节点来说是不可感知的。

$$P_V=P_1\prod_{i=2}^{V}P_i \tag{15}$$

4.2　传输效率

隐蔽通信的共同目标是高效、隐蔽、安全地在用户之间秘密地传递秘密信息。本节从以下几个方面将本文提出的隐蔽通信方法与现有区块链环境下的隐蔽通信方法进行比较，如表 4 所示。

表 4　隐蔽通信方法对比

方法	隐藏容量/bpt	单次通信时间	是否上链
BLOCCE	1	10 min	是
DLchain	256	12.5 s	是
ChainChannels	256	12.5 s	是
KBCC	320	12.5 s	是
BDTX	552	10 min	是
本文方法	≥1 376	2.5 s	否

4.2.1　隐藏容量

由于隐蔽通信每轮只通过一条交易完成，因此隐藏容量定义为每条交易可以嵌入的秘密信息比特数（bpt）。

BLOCCE[9]使用交易接收方比特币地址的最低

有效位嵌入秘密信息，每条交易的接收地址只有一个，因此一条交易只能传输 1 bit 的信息。DLchain[12]通过生成签名时使用的椭圆曲线算法隐藏秘密信息，用秘密信息代替签名时的私钥，由于私钥固定是 256 bit，则实现了 256 bpt 的隐藏容量。ChainChannels[13]与 DLchain 类似，用秘密信息代替签名时使用的随机数，由于随机数固定为 256 bit，则它也只实现了 256 bpt 的隐藏容量。KBCC（kleptography-based covert channel）[14]使用交易的 OP_RETURN 字段嵌入信息，OP_RETURN 字段的最大容量为 40 B，若全部使用可实现 320 bpt 的隐藏容量。BDTX[16]使用交易的 coinbase 字段嵌入信息，coinbase 字段最大容量为 69 B，全部使用可以实现 552 bpt 的隐藏容量。

本文方案由于无效交易只在与发送方连接的邻居节点间传播，不被区块链账本永久保存，大部分其他节点无法获取，因此可以选择交易的多个字段进行秘密信息嵌入。

当构造一个输入一个输出的无效交易时，交易中的前置交易（TXHASH）字段的 32 B、解锁脚本字段 120 B、输出的目的地址字段 20 B 都是可变字段，可以用来嵌入秘密信息，若都投入使用，一条交易可以实现 172 B 即 1 376 bpt 的隐藏容量。另外在构造无效交易时，可以选择构造多输入多输出的交易。因此，本文提出的方案，隐藏容量至少为 1 376 bpt，是 BDTX 方案的两倍以上。

4.2.2 通信时间

单次通信时间即发送方传递一条密文，从发送方创建交易开始到接收方收到交易为止所需的时间。

比特币网络中为了区块稳定，减少分叉，通过调整难度系数 Difficulty 来平衡全网算力，保证新区块的平均出块时间为 10 min，计算式如式(16)所示，其中 Time_{2016} 为生成过去 2 016 个区块的时间。若网络中不产生新的有效交易，那么每 10 min 新生成的区块中只包含创块交易，即输出地址为矿工账户的区块奖励。

$$\mathrm{Difficulty}_{\mathrm{new}}=\mathrm{Difficulty}_{\mathrm{old}}\times\frac{\mathrm{Time}_{2016}(\mathrm{min})}{10(\mathrm{min})\times 2016} \tag{16}$$

BLOCCE[9]要求接收方等待发送方发送的交易被包含进新生成的区块后，才能从大量交易中筛选出含密交易，因此该方案的单次通信时间即新区块生成需要的时间。BDTX[16]使用交易的 coinbase 字段嵌入信息，但是只有创块交易含有这个字段，即发送方处理完秘密信息后需要等待新区块生成，才能随着创块交易发出秘密信息。因此，这 2 个方案的单次通信时间都为 10 min。

DLchain[12]、ChainChannels[13]和 KBCC[14]这 3 种方案都需要发送方发出交易后，接收方在网络中监听筛选特殊交易，当网络中的所有节点都收到发送方发出的交易后，才能确保接收方节点能够收到此交易。比特币网络使用的是 Gossip 协议，节点周期性地向 8 个邻居节点广播交易信息，当网络中共有 k 个节点时，一条有效交易广播给全网节点需要 $K=\log_8 k$ 个轮次。目前比特币网络中存在节点 36 186 个，一条交易广播给所有的节点需要接近 5.05 个轮次。由式(15)可知，交易的一轮广播需要 2.5 s，因此 DLchain[12]、ChainChannels[13]和 KBCC[14] 3 种方案的单次通信时间约为 12.5 s。

在本文方案中，接收方的身份是发送方的邻居节点，接收方可以在发送方广播交易的第一轮收到含密交易，因此单次通信时间为 2.5 s。

5 结束语

本文针对现有区块链网络下隐蔽信道存在的问题，提出了一种基于交易构造和转发机制的区块链网络隐蔽通信方法。利用比特币交易的构造机制，将秘密信息嵌入交易的可自定义字段，来构造无效交易。由于构造无效交易时不需要遵循复杂的交易规则，只需数据格式和长度满足条件。因此，可根据秘密信息的长度选择嵌入秘密信息的字段，隐藏容量是 BDTX 方案的两倍以上。利用交易转发机制，使无效交易只在发送方的邻居节点之间传播，并且不存储于区块链的账本中，不会留下隐蔽通信的“证据”，安全性高。此外，本文通过实验和理论分析论证了该方法的抗检测性和不可感知性，并且通过计算分析得到，所提方案的隐藏容量和通信效率皆优于现有方案。之后的研究重点是将提出的方法扩展到群隐蔽通信中，在保证含有秘密信息的交易不被保存的前提下，实现多个接收者共同接收秘密信息。

参考文献：

[1] SIMMONS G J. The prisoners' problem and the subliminal channel[C]//Advances in Cryptology. Berlin: Springer, 1984: 51-67.

[2] 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 ZH, et al. Survey on key issues in networks covert channel[J]. Journal of Software, 2019, 30(8): 2470-2490.

[3] SOHN T, SEO J , MOON J. A study on the covert channel detection of TCP/IP header using support vector machine[C]//International Conference on Information and Communications Security. Berlin: Springer, 2003: 313-324.

[4] FISK G, FISK M, PAPADOPOULOS C, et al. Eliminating steganography in Internet traffic with active wardens[C]//International Workshop on Information Hiding. Berlin: Springer, 2002: 18-35.

[5] HANDLEY M, PAXSON V, KREIBICH C. Network intrusion detection: evasion, traffic normalization, and end-to-end protocol semantics[C]//Proceedings of the 10th conference on USENIX Security Symposium. Berkeley: USENIX Association, 2001: 9.

[6] LEWANDOWSKI G, LUCENA N B, CHAPIN S J. Analyzing network-aware active wardens in IPv6[C]//International Workshop on Information Hiding. Berlin: Springer, 2006: 58-77.

[7] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Decentralized Business Review, 2008.

[8] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.
ZHU L H, GAO F, SHEN M, et al. Survey on privacy preserving techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186.

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

[10] CAO H, YIN H, GAO F, et al. Chain-based covert data embedding schemes in blockchain[J]. IEEE Internet of Things Journal, 2020: doi.org/10.1109/JIOT.2020.3040389.

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

[12] 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.

[13] BRENNER M, CHRISTIN N, JOHNSON B, et al. Financial cryptography and data security[M]. Berlin: Springer, 2015.

[14] 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.

[15] PLOHMANN D, YAKDAN K, KLATT M, et al. A comprehensive measurement study of domain generating malware[C]//Proceedings of the 25th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2016: 263-278.

[16] 吕婧淑, 操晓春. 基于比特币系统的隐蔽通信技术[J]. 信息安全学报, 2021, 6(2): 143-152.
LYU J S, CAO X C. Covert communication technology based on bitcoin[J]. Journal of Cyber Security, 2021, 6(2): 143-152.

[17] ZHANG L J, ZHANG Z J, WANG W Z, et al. A covert communication method using special bitcoin addresses generated by vanitygen[J]. Computers, Materials & Continua, 2020, 65(1): 597-616.

[18] 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.

[19] ABDULAZIZ M, ÇULHA D, YAZICI A. A decentralized application for secure messaging in a trustless environment[C]//Proceedings of 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT). Piscataway: IEEE Press, 2018: 1-5.

[20] LEE B, LEE M Y, KO H S, et al. A secure mobile messenger based on Ethereum whisper[J]. The Journal of Korean Institute of Communications and Information Sciences, 2017, 42(7): 1477-1484.

[21] ZHANG L J, ZHANG Z J, JIN Z L, et al. An approach of covert communication based on the Ethereum whisper protocol in blockchain[J]. International Journal of Intelligent Systems, 2021, 36(2): 962-996.

[22] DEMERS A, GREENE D, HAUSER C, et al. Epidemic algorithms for replicated database maintenance[C]//Proceedings of the 6th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1987: 1-12.

[23] BONNEAU J, MILLER A, CLARK J, et al. SoK: research perspectives and challenges for bitcoin and cryptocurrencies[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 104-121.

[作者简介]

熊礼治（1988− ），男，湖北荆州人，博士，南京信息工程大学教授，主要研究方向为多媒体内容安全、数字取证与区块链安全等。

朱蓉（1998− ），女，江苏泰州人，南京信息工程大学硕士生，主要研究方向为区块链与数字取证等。

付章杰（1983− ），男，河南南阳人，博士，南京信息工程大学教授、博士生导师，主要研究方向为人工智能安全、区块链安全、数字取证等。