区块链环境下的新型网络隐蔽信道模型研究

李彦峰[1,2]，丁丽萍[1,3]，吴敬征[4]，崔强[5]，刘雪花[1,2]，关贝[6]

（1. 中国科学院软件研究所并行软件与计算科学实验室，北京 100190；2. 中国科学院大学计算机科学与技术学院，北京 100049；
3. 广州中国科学院软件应用技术研究所电子数据取证实验室，广东 广州 511458；4. 中国科学院软件研究所智能软件研究中心，北京 100190；
5. 中国科学院软件研究所互联网软件技术实验室，北京 100190；6. 中国科学院软件研究所协同创新中心，北京 100190）

摘 要：区块链是随着数字货币商品兴起的去中心化基础架构，具有安全可信、顽健性高等特点。首次提出区块链环境下的网络隐蔽信道模型，具有抗干扰性、抗篡改性、多线路通信性、接收方匿名性、线路无关性，可以克服现有网络环境下的隐蔽信道特性缺陷等弊端。首先提出了区块链网络隐蔽信道模型，用形式化方法建模并证明了抗干扰性和抗篡改性；其次构建了基于业务操作时间间隔的区块链网络隐蔽信道的场景；最后提出了包含抗检测性、顽健性、传输效率的区块链网络隐蔽信道评估向量，为基于区块链环境的新型网络隐蔽信道的实用化奠定了理论基础。

关键词：网络隐蔽信道；区块链；抗干扰性；抗篡改性；链式存储

中图分类号：TP309.2

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019111

Research on a new network covert channel model in blockchain environment

LI Yanfeng[1,2], DING Liping[1,3], WU Jingzheng[4], CUI Qiang[5], LIU Xuehua[1,2], GUAN Bei[6]

1. Laboratory of Parallel Software and Computational Science, Institute of Software Chinese Academy of Sciences, Beijing 100190, China
2. School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China
3. Digital Forensics Lab, Institute of Software Application Technology, Guangzhou & Chinese Academy of Sciences(GZIS), Guangzhou 511458, China
4. Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
5. Laboratory for Internet Software Technologies, Institute of Software Chinese Academy of Sciences, Beijing 100190, China
6. Collaborative Innovation Center, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

Abstract: Blockchain is a decentralized architecture emerging with cryptocurrencies, which is credible and robust. A network covert channel model in blockchain environment was proposed for the first time, which was anti-interference, anti-tamper modification, multi-line communication, receiver anonymity and line independence. The shortcomings of network covert channel in existing network environment could be tackled by the new type of network covert channel, such as characteristic defect. etc. Firstly, A network covert channel model in blockchain environment was presented by formal method, its anti-interference and anti-tamper modification was proved. Then, a blockchain network covert channel scenario using service operation interval time was presented. Finally, the undetectability, robustness and rate of the blockchain network covert channel evaluation vectors was proposed. A theoretical foundation was laid for the practicality of the new type of network covert channel in blockchain.

Key words: network covert channel, blockchain, anti-interference, anti-tamper modification, chained storage

---

收稿日期：2018−10−09；**修回日期**：2019−04−11

通信作者：丁丽萍，dingliping@gz.iscas.ac.cn

基金项目：国家重点研发计划基金资助项目（No.2016QY01W0200）；国家自然科学基金面上基金资助项目（No.61772507）；广州市科技计划基金资助项目（No.201802020015）

Foundation Items: The National Key Research and Development Program of China（ No.2016QY01W0200）, The National Natural Science Foundation of China (No.61772507), The Science and Technology Planning Project of Guangzhou Municipality (No.201802020015)

1 引言

区块链是随着数字货币商品兴起的去中心化基础架构，可以存储有先后关系的、能在系统内进行验证的数据，以密码学保证不可篡改和不可伪造。区块链使用共识机制使一个不可信网络变成可信的网络[1-3]，具有去中心化、时序性、集体维护等特性[3]。由于区块链具有安全可信、去中心化、健壮性等特点，其应用已延伸到数字货币商品、供应链管理、物联网、智能制造等多个领域[1-2]。

时间戳、对等网络和链式存储是区块链的 3 个重要技术。时间戳指区块链每次业务操作（如交易）发起时都会在该业务信息中加盖时间戳，使区块链具有时序性。对等网络指区块链网络中不存在任何中心化的特殊节点，每个节点以扁平式拓扑结构相互通信。链式存储指各个通信节点都会包含以时序连接的数据结构，能够提供区块链数据的溯源功能 [2-3]。

网络隐蔽信道定义为在网络环境下违反通信限制规则进行信息传输的隐蔽通信信道[1-4]，提供不能被监测到的隐蔽通信信道进行信息传输[4]，以网络信息载体（如网络协议、网络数据分组等）、载体特征（如协议字段、时间特征等）及特征模式（如值调制模式、时间间隔模式等）作为码元进行编码和优化隐蔽信息的传输。网络隐蔽信道分为存储型网络隐蔽信道和时间型网络隐蔽信道两大类。存储型网络隐蔽信道通过协议数据单元（PDU，protocol data units ）传递隐藏信息，如数据分组、数据帧、数据段的未使用或保留的协议头元素（如协议头字段）；时间型网络隐蔽信道通过协议数据单元或协议指令的间隔时间或数据分组的顺序编码传递隐藏信息[5]。

现有的网络隐蔽信道存在以下弊端。

1) 2 类网络隐蔽信道存在各自的特性缺陷。存储型网络隐蔽信道易被基于内容的检测方法进行针对性检测[6]；时间型网络隐蔽信道的信道容量小，发送者和接受者往往需要同步，并且很容易受网络条件变化（如延迟、分组丢失、噪音）的影响[5]。

2) 存在针对性限制 2 类网络隐蔽信道的技术。大部分存储型网络隐蔽信道可被通信归一化[7-8]等基于通信内容修改的技术消除；时间型网络隐蔽信道易受网络干扰 [9]、网络泵[10-11]等基于修改网络数据时间属性的方法干扰。

3) 缺少顽健性保障手段。现有存储型网络隐蔽信道依赖于所使用的载体协议的特性，一些具有可靠性保障的协议可以提供可靠性保障（如传输控制协议），大部分存储型网络隐蔽信道都不具备可靠性保障[5]；现有的时间型网络隐蔽信道本身受网络环境影响较大，往往采用纠错码的方式提高顽健性，降低了通信效率[12-14]。

4) 静态单一线路的传输方式。绝大多数网络隐蔽信道采用通信双方直接通信的方式，通信线路静态单一，易被针对性和检测、干扰和阻断。现有的动态路由技术虽然能够实现传输线路的变化，但传输过程依然是单一线路，并且缺乏顽健性保障[15-16]。

区块链的诸多特性契合网络隐蔽信道需求，并且可以克服网络隐蔽信道现有弊端，实现高顽健性的隐蔽通信。本文首次提出区块链环境下的网络隐蔽信道（简称为区块链网络隐蔽信道）模型，可以达到以下效果。

1) 抗干扰性。利用区块链的时间戳技术，使区块链网络环境下的时间型网络隐蔽信道具有抗干扰性，不受网络环境影响，不受基于修改网络数据时间属性的技术影响。

2) 抗篡改性。利用区块链的链式存储技术，使区块链网络环境下的存储型网络隐蔽信道具有抗篡改性，不受基于通信内容修改的技术影响。

3) 多线路通信性。利用区块链对等网络通信技术，使区块链网络环境下的隐蔽信息实现分布式多线路传输，弥补了传统网络环境下静态单一线路传输方式易被针对性地检测、干扰、阻断的缺陷。

4) 接收方匿名性。由于通信双方通过区块链对等网络进行间接通信，所有网络节点都是隐蔽信息的潜在接收方，因此无法准确辨别信息的接收方，使其具有匿名性。

5) 线路无关性。所有通信信息通过分布式存储的方式保存于各个节点，因此时间型区块链网络隐蔽信道下通信双方不需要进行同步并为此付出额外成本。

本文贡献如下。

1) 首次提出了区块链环境下的网络隐蔽信道模型，可以有效克服现有网络隐蔽信道的弊端，实现高顽健性网络隐蔽信道通信。

2) 对区块链环境下的网络隐蔽信道进行形式化建模，并对其抗干扰性和抗篡改性进行证明。

3) 构建了基于业务操作时间间隔的时间型区块链网络隐蔽信道场景。

4) 提出了区块链网络隐蔽信道的抗检测性、顽健性和传输效率这 3 个评估向量。

2　相关工作

2.1　区块链技术

区块链是一种按时间顺序将数据区块组成类似链表的数据结构，以密码学保证不可篡改和不可伪造的分布式去中心化账本，可以存储有先后关系的、能在系统内进行验证的数据，使用共识机制使一个不可信网络变成可信的网络[1-2]，具有去中心化、时序性、集体维护等特性。去中心化指区块链数据的记录、验证、存储、传输等过程基于分布式系统结构建立各个节点间信任关系，而不是传统的中心结构。时序性指区块链采用带有时间戳的链式区块结构存储数据，这增加了时间维度，具有可追溯性和可验证性。集体维护指区块链采用特定的激励机制保证系统中所有节点都可以参与数据区块的验证过程，通过共识算法来选择特定的节点将新区块添加到区块链[3]。由于区块链安全可信、去中心化、顽健性等特点，其应用已延伸到物联网、智能制造、数字资产交易等多个领域[2]。

区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。其中，数据层实现区块链中数据存储的机制，包含区块链数据存储的数据结构、加密机制、完整性保护机制；网络层实现区块链中各个区块的通信机制，包括数据传播机制、分布式组网机制和数据验证机制；共识层实现去中心化系统的各节点数据高效地达成共识，封装了网络节点的各类共识算法；激励层实现区块链中共识节点间任务众包过程的激励机制，主要包括激励的发行机制和分配机制；合约层实现商业逻辑和算法，是区块链可编程特性的基础，封装了各类脚本、算法和智能合约；应用层封装了区块链的具体应用场景，如可编程数字货币商品、食品溯源等。区块链技术的基础架构模型如图 1 所示[3]。

时间戳、对等网络和链式存储是区块链的 3 个重要技术。时间戳指每次业务操作发起时都会在该业务信息中加入时间戳，以确定业务发起时间；在数据区块创建时也会在当前数据区块头中加盖时间戳，用以确定数据区块创建的时间，使区块链具有时序性。对等网络指区块链网络中不存在任何中心化的特殊节点，每个节点以扁平式拓扑结构相互通信，每个节点均会承担数据通信、网络路由、验证区块等工作，并使用广播机制传输信息，发送数据的节点将信息广播到相连接的节点，验证通过后会再进行广播，信息快速被全网节点接收[17-18]。链式存储指各个通信节点都会包含以时序连接的数据结构，这个数据结构被称为区块链，各个区块依次相接，形成从创世区块到当前区块的一条主链，每个区块包含一个完整的数据信息，以递归计算散列值的 Merkle 树的形式组织在一起，从而记录了区块链数据的完整历史，并且能够提供区块链数据的完整性溯源功能；所有节点通过对等网络同步区块信息，进行分布式存储。区块结构如图 2 所示[2-3]。

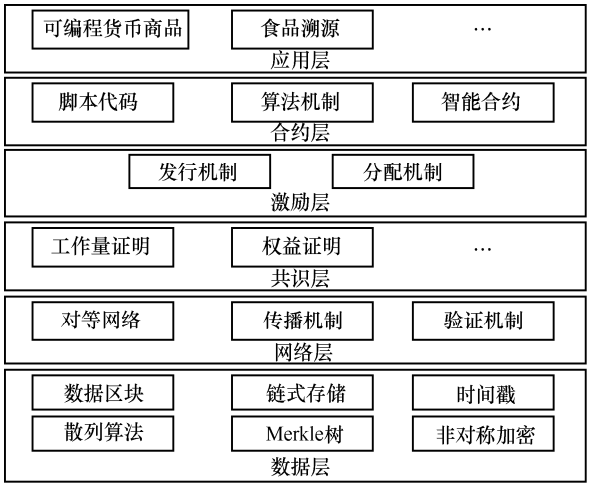


图 1　区块链技术基础架构模型

综上所述，区块链的时间戳、对等网络、链式存储技术为构建高顽健性的网络隐蔽信道提供了技术基础。

2.2　网络隐蔽信道

网络隐蔽信道是隐蔽信道的一个领域。隐蔽信道的概念最初由 Lampson 等[19]于 1973 年提出，定义为本意不是被设计用来传输信息的、破坏通信安全策略的通信信道，是在主机环境下造成越级的信息泄露的隐蔽信息传输通道[20-23]。随着网络技术的发展，隐蔽信道的研究扩展到了网络环境。文献[1-4]将网络隐蔽信道定义为在网络环境下违反通信限制规则进行隐蔽信息传输的通信信道。网络隐蔽信道的研究目标是提供不能被监测到的隐蔽通信通道进行信息传输[24]，寻找适合的网络信息载体（如网络协议、网络数据分组等）、载体特征（如协议字段、时间特征等）及特征模式（如值调制模式、时间间隔模式等）作为码元进行编码、优化以实现隐蔽信息传输。

文献[1-4]依据传统隐蔽信道的分类方法将网络隐蔽信道分为存储型网络隐蔽信道和时间型网络隐蔽信道两大类。文献[5]认为存储型网络隐蔽信道通过协议数据单元（PDU，protocol data unit）传递隐藏信息，如数据分组、数据帧、数据段的未使用或保留的协议头元素（如协议头字段）等；时间型网络隐蔽信道通过协议数据单元或协议指令的时间间隔或数据分组的顺序编码传递隐藏信息。文献[5]使用模式语言标记语言（PLML，pattern language markup language ）方法将 1987 年至 2013 年出现的 109 个隐蔽信道构建技术分为 11 个不同的模式，分别为调制大小模式[25-27]、序列模式[26]、增加冗余模式[28]、协议数据单元错误/丢失模式[29]、随机值模式[30]、值调制模式[31]、保留元素模式[32]、时间间隔模式[25]、速率模式[33]、协议数据单元顺序模式[34]和重传模式[34]。

上述 2 类网络隐蔽信道有着各自的缺陷。文献[5,35]认为存储型网络信道虽然利用载体信道的可靠性传输（如传输控制协议），并且容量较大，但是易被基于内容的检测方法检测[6]；而时间型网络隐蔽信道虽然较难检测，但是很容易受网络条件变化（如延迟、分组丢失、噪音）的影响，信道容量小，而且往往需要发送者和接受者同步。

2 类网络隐蔽信道都存在针对性的限制技术。存储型网络隐蔽信道可被通信归一化[7-8]等基于通信内容修改的技术消除。通信归一化技术会对网络层、通信层、应用层的协议内容进行修改，对以协议数据单元头字段构造的存储型网络隐蔽信道造成影响。时间型网络隐蔽信道可被基于修改网络数据时间属性的方法干扰，文献[36]认为，当隐蔽信道的噪声足够大，使信噪比很低，导致信道容量小于一定程度时，信息的准确度会低至无法容忍的地步，即使出现网络隐蔽信道也无法造成威胁，因此可以通过在信道中添加延时的方式，造成时间型网络隐蔽信道的解码错误；文献[9]提出了网络干扰的方法，利用随机延迟网络数据分组的方式限制网络时间型隐蔽信道的容量；文献[10-11]提出了网络泵技术，可以使网络数据分组的间隔时间随机化或均匀分布，从而限制时间型网络隐蔽信道。

现有网络隐蔽信道缺少顽健性保障手段。存储型网络隐蔽信道依赖所使用的载体协议的特性，一些具有可靠性保障的协议可以提供一定可靠性保障（如传输控制协议）[30,37-38]，但大部分存储型网络隐蔽信道都不具备可靠性保障；现有的时间型网络隐蔽信道本身受网络环境影响较大，往往采用纠错码的方式提高顽健性[34,36-37]，但这会增加额外的冗余信息，降低通信效率。

除此之外，大部分的网络隐蔽信道是通信双方基于静态单一路径进行通信的，通信双方直接暴露于网络之上，易被针对性地阻断、干扰及检测。现有的动态路由技术可以使网络隐蔽信道使用非固定通信路径进行通信，进而提高数据传输的抗检测性[15]。文献[16]利用随机游走算法随机选择下一跳的通信节点，进而构建了完全随机的隐蔽传输网络拓扑，无法监控和预测隐蔽信道传输的路径，从而提高了隐蔽信道的抗检测性。文献[15]实现了一种基于优化链接状态路由（OLSR，optimized link-state routing ）的动态路由协议，引入隐蔽性质量（QoC，quality of covertness ）与通信质量（QoS，quality of service ）构成通信节点间通信的 2 个度量指标，形

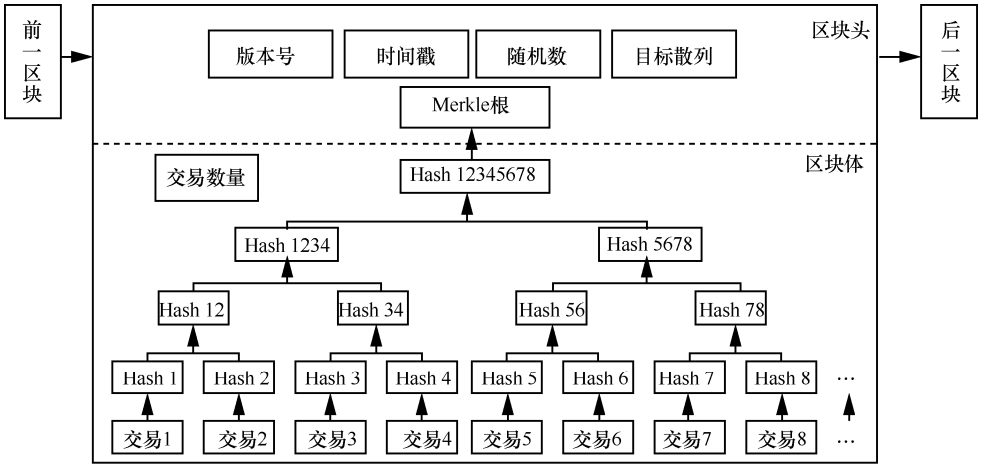


图 2 区块结构

成网络隐蔽信道的节点表和网络拓扑表，每次传输时寻找 QoC 和 QoS 最优的节点进行通信。然而这 2 种方法虽然使用的是非固定通信路径传输数据，但通信过程依旧是单路径的，并且缺乏顽健性保障。

综上所述，现有网络环境下的网络隐蔽信道存在特性缺陷、针对性的限制技术、缺少顽健性保障手段和静态单一线路的传输方式这 4 个弊端。本文提出的区块链网络环境下的隐蔽信道可以在提供隐蔽通信的同时提供顽健性保障，克服了现有网络环境下网络隐蔽信道的弊端。

3　区块链网络隐蔽信道模型

3.1　模型定义

区块链网络隐蔽信道由信息发送方、信息接收方、原始信息、信息传输组成。信息发送方通过信息传输将信息发送至信息接收方。

定义 1　区块链隐蔽信道通信。一个区块链网络隐蔽信道可以被形式化表示为

$$< P_{\mathrm{s}}, P_{\mathrm{r}}, M, T_{\mathrm{s,r}} > \tag{1}$$

其中，P_{s} 是信息发送方，P_{r} 是信息接收方，M 是传递的原始信息，$T_{\mathrm{s,r}}$ 是信息传输。

假设区块链网络中共有 x 个节点，则 P_{s} 与 P_{r} 可分别表示为

$$P_{\mathrm{s}} = (p_1) \tag{2}$$

$$P_{\mathrm{r}} = (p_2 , p_3 , p_4, \cdots, p_t, \cdots, p_x) \quad (2 \leqslant t \leqslant x) \tag{3}$$

区块链网络隐蔽信道的目标是把原始信息 M 从信息发送方 P_{s} 传输到信息接收方 P_{r}。

信息发送方 P_{s} 通过信息传递 $T_{\mathrm{s,r}}$ 将 M 传递给 P_{r}，如式(4)所示。

$$T_{\mathrm{s,r}} = P_{\mathrm{s}} \overset{M}{\rightarrow} P_{\mathrm{r}} \tag{4}$$

区块链网络隐蔽信道对等网络通信过程可以表示为

$$T_{\mathrm{s,r}} = (T_{1,2}, T_{1,3}, \cdots, T_{1,t}, \cdots, T_{1,x}, T_{2,3}, T_{2,4}, \cdots, T_{2,t}, \cdots, T_{2,x}, \cdots) \tag{5}$$

定义 2　信息编码。利用某种编码规则（如编码表）$R(R_1, R_2, \cdots, R_n)$将原始信息 M 转换为信息编码 M'，使之可以被通信网络传输，如式(6)所示。

$$M \rightarrow M' = (m_1, m_2, m_3, \cdots, m_m) \rightarrow (m_1', m_2', m_3', \cdots, m_n') \tag{6}$$

定义 3　信息调制。利用区块链的某种属性作为调制符号，利用某种调制规则（如调制符号表）$S(S_1, S_2, \cdots, S_n)$将信息编码 M'调制为隐蔽信息 M''，使其通过区块链网络环境进行隐蔽传输，如式(7)所示。

$$M' \rightarrow M'' = (m_1', m_2', m_3', \cdots, m_n') \rightarrow (m_1'', m_2'', m_3'', \cdots, m_o'') \tag{7}$$

根据用于调制信息的区块链的属性特点可以将区块链网络隐蔽信道分为时间型网络隐蔽信道和存储型网络隐蔽信道 2 类。

$$M'' = \{ \{\mathrm{Time}\}, \{\mathrm{Storage}\} \} = \{ \{\mathrm{time}_{\mathrm{transaction}}, \Delta\mathrm{time}_{\mathrm{transaction}}, \cdots\}, \{\mathrm{timestamp}, \mathrm{address}, \mathrm{address}_{\mathrm{hash}}, \mathrm{BTC} \ \cdots\} \} \tag{8}$$

其中，{Time}是区块链可以用来进行隐蔽信息传输的时间属性集合，以比特币为例，可以包括交易时间、交易时间间隔等。{Storage}是区块链可以用来进行隐蔽信息传输的存储属性集合，以比特币为例，可以包括时间戳、被交易方的比特币地址、被交易方的比特币地址的散列值、参与交易的比特币数量等[39]。

定义 4　区块链隐蔽信道存储。每个通信节点在收到调制符号 M''后，会将保存 M''的区块加到主链中，与其他区块依时序进行链式存储。

$$M'' \rightarrow \mathrm{BlockChain} \tag{9}$$

定义 5　信息解调。信息接收方在获得由个区块链属性调制的符号集合 M''后，通过调制规则（如调制符号表）$S(S_1, S_2, \cdots, S_n)$将其解调为信息编码 M'，如式(10)所示。

$$M'' \rightarrow M' = (m_1'', m_2'' , m_3'', \cdots, m_n'') \rightarrow (m_1', m_2', m_3', \cdots, m_o') \tag{10}$$

定义 6　信息解码。信息接收方通过编码规则（如编码表）$R(R_1, R_2, \cdots, R_n)$将信息编码解码 M'为原始信息 M，如式(11)所示。

$$M' \rightarrow M = (m_1', m_2', m_3', \cdots , m_m') \rightarrow (m_1, m_2 , m_3, \cdots, m_n) \tag{11}$$

综上所述，区块链网络隐蔽信道模型如图 3 所示。

3.2　特性及证明

区块链网络隐蔽信道的特点是具有较高的顽健性，网络隐蔽信道背景下的顽健性包括抗干扰性、抗篡改性这 2 个方面。此外还具有多线路通信性、接收方匿名性、线路无关性的特性。

3.2.1　抗干扰性证明

传统时间型网络隐蔽信道易受网络条件的变化（如延迟、分组丢失、噪音）的影响，此外，通

过网络干扰[9]、网络泵[10-11,40]等基于修改网络数据分组时间属性的干扰技术也很容易对时间型网络隐蔽信道造成影响。

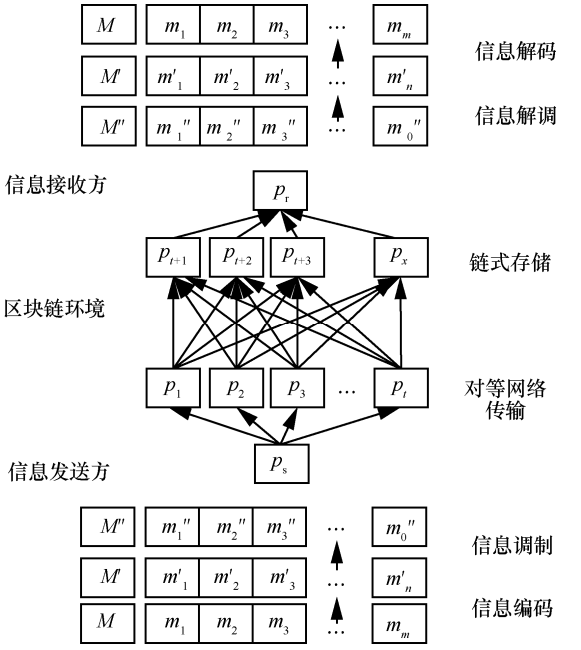


图 3 区块链网络隐蔽信道模型

以数据分组时间间隔型网络隐蔽信道为例，用 2 个数据分组之间的时间间隔 ΔT 作为信息调制符号 S，如式(12)所示。

$$S=\Delta T \tag{12}$$

则调制符号表为

$$S(S_1, S_2,\cdots, S_n)=\Delta T(\Delta T_1, \Delta T_2, \cdots, \Delta T_n) \tag{13}$$

$\mathrm{diff}_{n+1,n}$ 表示相邻的这 2 个编码的时间间隔的差值，如式(14)所示。

$$\mathrm{diff}_{n+1,n}=\Delta t_{n+1}-\Delta t_n \tag{14}$$

通信过程中，时间间隔抖动会导致通信误差，干扰通信过程。时间抖动导致的通信误差 $\Delta t_{\mathrm{error}}$ 包括本地时间抖动 $\Delta t_{\mathrm{local}}$ 和网络传输时间抖动 Δt_{net}，如式(15)所示。

$$\Delta t_{\mathrm{error}}=\Delta t_{\mathrm{local}}+\Delta t_{\mathrm{net}} \tag{15}$$

假设时间抖动的最大值为 $\Delta t_{\mathrm{disturb}}$，则实际通信过程中的隐蔽信息 M'''为

$$\begin{aligned}M'''=&(m_1''', m_2''', \cdots, m_n''')=(\Delta t_1', \Delta t_2', \cdots, t_n')=\\&(\Delta t_1+\Delta t_{\mathrm{disturb}}, \Delta t_2+\Delta t_{\mathrm{disturb}}, \cdots, \Delta t_n+\Delta t_{\mathrm{disturb}})=\\&(\Delta t_1+\Delta t_{\text{local-max}}+\Delta t_{\text{net-max}}, \Delta t_2+\Delta t_{\text{local-max}}+\\&\Delta t_{\text{net-max}}, \cdots, \Delta t_n+\Delta t_{\text{local-max}}+\Delta t_{\text{net-max}})\end{aligned} \tag{16}$$

如果 $\Delta t_{\mathrm{disturb}}$ 大于 $\mathrm{diff}_{n+1,n}$，那么就会发生误码，与下一个编码重叠。因此，在真实网络环境下时间型网络隐蔽信道的分组发送间隔时间最小为 $\Delta t_{\mathrm{disturb}}$，如式(17)所示。

$$\Delta t_{\mathrm{disturb}}<\mathrm{diff}_{n+1,n} \tag{17}$$

区块链网络环境下的时间型网络隐蔽信道中，业务信息包含时间戳，从而确保用来做隐蔽信息通信的时间属性可以通过时间戳进行校验和还原，从而不受网络传输过程中网络环境的影响。因此，区块链网络环境下通信误差 $\Delta t'_{\mathrm{error}}$ 中由网络传输时间抖动造成的误差 $\Delta t_{\mathrm{local}}$ 由于时间戳的存在而被消除，仅剩下本地时间抖动 Δt_{net}，如式(18)所示。

$$\Delta t'_{\mathrm{error}}=\Delta t_{\mathrm{local}} \tag{18}$$

实际通信过程为

$$\begin{aligned}&(m_1''', m_2''', \cdots, m_n''')=(\Delta t_1', \Delta t_2', \cdots, \Delta t_n')=\\&(\Delta t_1+\Delta t_{\text{local-max}}, \Delta t_2+\Delta t_{\text{local-max}}, \cdots, \Delta t_n+\Delta t_{\text{local-max}})\end{aligned} \tag{19}$$

由此可证，区块链隐蔽信道通信误差小于传统网络隐蔽信道通信误差。目前区块链技术（如比特币区块链）使用 Unix 时间戳，可以近似认为

$$\begin{aligned}&(m_1''', m_2''', \cdots, m_n''')=(\Delta t_1', \Delta t_2', \cdots, \Delta t_n')=\\&(\Delta t_1, \Delta t_2, \cdots, \Delta t_n)\end{aligned} \tag{20}$$

因此，区块链网络隐蔽信较传统网络隐蔽信道道具有更强的抗干扰性。

3.2.2 抗篡改性证明

大部分存储型网络隐蔽信道可被通信归一化方法[7-8]技术消除，即对通信内容进行篡改。在区块链网络隐蔽信道环境下，区块链网络中的所有节点基于统一的规则将收到的信息进行链式存储，篡改者只有计算出一条数据链的分支并获得其他节点的承认才能达到对数据篡改的目的。由于所有数据都是迭代存储的，篡改者需要补充篡改区块之后所有区块的工作量才能达到和合法存储数据链同样的长度[1-2,41]。

假设 p 为正常节点接收下一个数据并存储为区块的概率，q 为篡改者篡改下一条数据并存储为区块的概率，z 为篡改者数据链需要补充的数据区块的数量。则篡改者补充 z 个数据区块差距的概率为

$$q_z=\begin{cases}1, & p\leqslant q\\ \left(\dfrac{q}{p}\right)^z, & p>q\end{cases} \tag{21}$$

如果 $p>q$，那么攻击者成功篡改通信数据的概率随着数据区块数的增长呈指数级下降。

假设正常数据节点在正常时间内接收一条数据并存储为区块，篡改者的篡改进度是一个期望值为 $\lambda = z\frac{q}{p}$ 的泊松分布。篡改者篡改的成功率为

$$\sum_{k=0}^{\infty}\frac{\lambda^k \mathrm{e}^{-\lambda}}{k!}\begin{cases}\left(\dfrac{q}{p}\right)^{(z-k)}, & k \leqslant z\\ 1, & k > z\end{cases} \tag{22}$$

可化简为

$$1-\sum_{k=0}^{z}\frac{\lambda^k \mathrm{e}^{-\lambda}}{k!}\left(1-\frac{q}{p^{(z-k)}}\right) \tag{23}$$

根据式(23)计算可得，当 p=0.9 时，篡改者篡改 2 个区块头部的概率约为 0.05；如果保证篡改者篡改成功的概率小于 0.001，则当 p=0.9 时，z=5[1-2,41]。由此可证，区块链网络隐蔽信道具有较强的抗篡改性。

3.2.3 多线路通信性

由于区块链使用对等网络通信技术，使区块链网络环境下的隐蔽信息实现分布式多线路传输，弥补了传统网络环境下静态单一线路传输方式易被针对性地检测、干扰及阻断的弊端。

3.2.4 接收方匿名性

由于通信双方通过区块链对等网络进行间接通信，隐蔽信息发送方只需按照与信息接收方约定的规则进行隐蔽信息调制并将其发送至区块链网络即可，不需要与接收方进行任何直接通信，所有区块链网络中的通信节点都是隐蔽信息的潜在信息接收方，第三方甚至隐蔽信息发送者都无法准确辨别信息的接收方，使其具有匿名性。

3.2.5 线路无关性

所有通信信息通过分布式存储的方式保存于所有区块链网络节点，所有通信过程都会被完整保存，因此时间型区块链网络隐蔽信道下通信双方不需要进行同步并为此付出额外成本，只需要观察区块链数据中是否存在约定特征的数据即可。

4　区块链网络隐蔽信道场景构建

第 2.1 节给出了区块链网络隐蔽信道的模型构建过程，下面以该模型为基础，构建一个基于业务操作时间间隔的区块链网络隐蔽信道场景。

基于数据分组时间间隔的网络时间型隐蔽信道（IPCTC，inter-packet covert timing channel ）是一种传统时间型网络隐蔽信道技术，利用时间窗口内是否包含数据分组进行二进制编码，将时间分成连续相等但不相交的时间窗口，“1”表示在时间窗口内发送数据分组，“0”表示不发送数据分组[42]。在此基础上，出现了基于编码表的网络时间型隐蔽信道，发送方使用时间间隔作为调制符号，使用调制符号表使 n 个时间间隔与 n 元的信息编码表建立映射。发送方利用调制符号表，将编码后的原始信息使用时间间隔进行调制发送给接收方；接收方在收到发送方发来的数据分组后，查询事先约定的调制符号表，将数据分组的时间间隔还原为编码符号，再还原为原始信息[12,43]。编码方式可采用霍夫曼编码[44]、几何码[14]等。

在此思路基础上，构建基于交易时间间隔的区块链网络隐蔽信道。最早在区块链技术中引入“交易”一词的是比特币系统，指把若干比特币经过交易双方的签名运算，进行价值转移的数据结构。每一笔交易都经过比特币的对等网络进行分布式传输，由各节点接收并封装至区块中，通过链式存储的方式分布式存储在比特币网络[39]。在后来的区块链应用中，“交易”一词泛指基于区块链技术的业务操作导致的状态转变。本节以“交易”指代广义的基于区块链应用的业务操作，而非专指电子货币商品中的交易。基于区块链交易时间间隔的区块链网络隐蔽信道实现方法如图 4 所示。

在区块链网络环境下，建立以区块链交易时间间隔作为信息调制方式[43-44]实现的时间型区块链网络隐蔽信道传输场景如下。

1) 发送方和接收方事先达成共识。使用相同的 n 元信息编码表 $R(R_1,R_2,\cdots,R_n)$；使用相同的调制符号表 S，即 n 元交易时间间隔表 $\Delta T(\Delta T_1, \Delta T_2, \cdots, \Delta T_n)$，使其与 n 元信息编码表 $R(R_1, R_2, \cdots, R_n)$建立映射；使用相同的隐蔽信息传输起始符号 S_{start} 和隐蔽信息传输结束符号 S_{end}，例如以 5 个连续的二进制“0”的交易时间间隔调制符号作为隐蔽信息传输起始符号，以 5 个连续的二进制“1”的交易时间间隔调制符号作为隐蔽信息传输的结束符号。

2) 利用编码表 R 对原始信息进行信息编码，形成编码信息序列 $M'(m_1', m_2', m_3', \cdots, m_n')$。

3) 发送方利用调制符号表将编码后的信息调

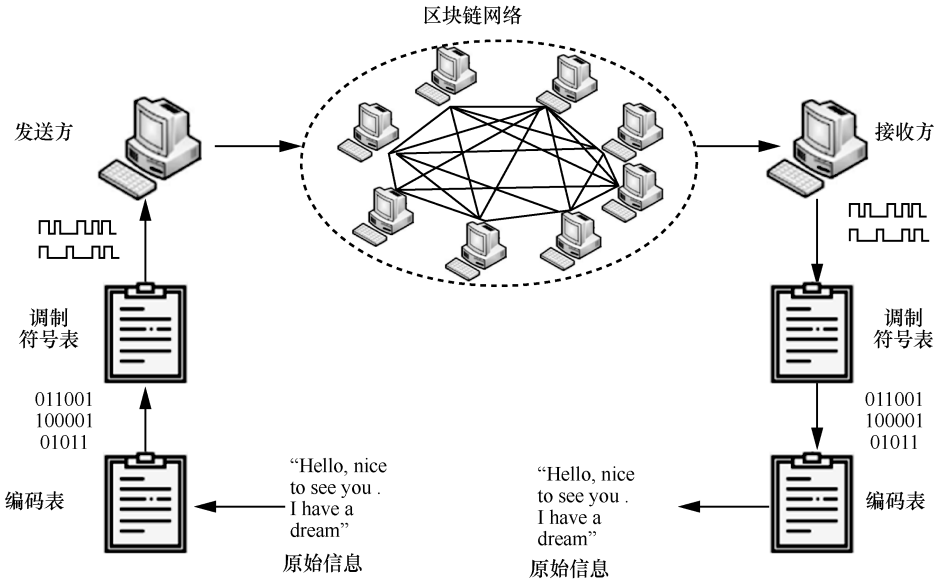


图 4　基于交易时间间隔的区块链网络隐蔽信道实现

制成时间间隔序列 $\Delta t(\Delta t_1,\Delta t_2,\Delta t_3,\cdots,\Delta t_n)$，生成隐蔽信息。

4) 发送方通过区块链网络发送隐蔽信息，从隐蔽信道起始符号 S_{start} 开始隐蔽通信，之后进入隐蔽信息发送阶段 S_{cycle} 发送时间间隔序列，到隐蔽信道结束符号 S_{end} 结束隐蔽通信。

5) 接收方获取所有隐蔽信道起始符号 S_{start} 至隐蔽信道结束符号 S_{end} 之间，即隐蔽信息发送阶段 S_{cycle} 的时间间隔序列 $\Delta t(\Delta t_1, \Delta t_2, \Delta t_3, \cdots, \Delta t_n)$，以交易时间戳为基准校对隐蔽信息序列，获取隐蔽信息；使用事先约定的符号调制表 $\Delta T(\Delta T_1, \Delta T_2, \cdots, \Delta T_n)$解调时间间隔序列获得编码信息序列 M' (m_1', m_2', m_3', $\cdots$, m_n')，再通过事先约定的编码表解码获得原始信息。

基于交易时间间隔的区块链网络隐蔽信道传输通信过程如图 5 所示。

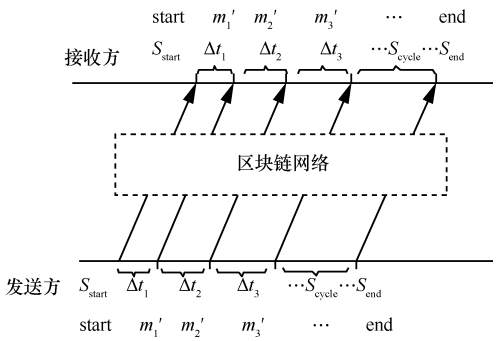


图 5　基于交易时间间隔的区块链网络隐蔽信道隐蔽信息传输过程

5　区块链网络隐蔽信道评估

当确定了潜在的隐蔽信道后，需要对隐蔽信道进行评估。文献[45]提出了对隐蔽信道的评估框架，可适用于存储型网络隐蔽信道和时间型网络隐蔽信道，使用信道容量、顽健性和隐蔽性这 3 种指标评估网络隐蔽信道。信道容量指隐蔽信道每个数据分组能够传输的数据量，顽健性指隐蔽信道对抗信道噪声和干扰的能力，隐蔽性指隐蔽信道传输与正常数据传输的差异程度。文献[14]使用抗检测性、顽健性和速率对网络隐蔽信道进行评估，其中，抗检测性指隐蔽通信不能与合法通信进行区分的能力，顽健性指对抗噪声的能力，速率指每个用来传递隐蔽信息的数据分组传递的隐蔽信息的比特数。

综合相关工作的研究，本文提出了区块链网络隐蔽信道的 3 个评估向量：抗检测性、顽健性和传输效率。其中，抗检测性指区块链网络隐蔽信道不被发现的能力，使用熵率作为评估指标；顽健性指区块链网络隐蔽信道正确传输信息的能力，使用误码率作为评估指标；传输效率指区块链网络隐蔽信道单位时间内数据传输的能力，使用单位时间内传输的信息量作为评估指标。

5.1　抗检测性评估

针对区块链网络隐蔽信道的抗检测性可以使用熵率（ER，entropy rate ）进行评估。熵率表示无穷

序列的不确定性，熵率越小规律性越强。熵率可以用来表示区块链某一属性变化的规律性[43,46-47]。熵率 ER 为

$$\mathrm{ER}=\min_{i=1,m}(\mathrm{CCE}(X_i\mid X_{i-1})) \tag{24}$$

熵率是无穷序列的条件熵，在实际情况中，采用有限采样的方式，使用修正条件熵（CCE，corrected conditional entropy）计算熵率[43]。其中，$H(X_m|X_{m-1})$表示经验概率密度条件熵，$p(X_m)$表示长度为 m 的序列只出现一次的比例，$H(X_1)$是序列长度为 1 时的熵。

$$\mathrm{CCE}(X_m|X_{m-1})=H(X_m\mid X_{m-1})+p(X_m)H(X_1) \tag{25}$$

当使用熵率评估抗检测性时，首先确定检测的对象（如交易时间间隔、被交易方数字签名等），使用大量正常通信确定该对象的阈值。当被检测对象的序列低于该阈值时，说明产生了区块链网络隐蔽信道。

5.2　顽健性评估

针对区块链网络隐蔽信道的顽健性可以使用误码率（BER，bit error rate ）对网络隐蔽信道的顽健性进行测量，误码率越低代表网络隐蔽信道的顽健性越高[36]。传输的错误码元数为 S_{error}，总码元数为 S_{all}，误码率 BER 为

$$\mathrm{BER}=\frac{S_{\mathrm{error}}}{S_{\mathrm{all}}} \tag{26}$$

另一种误码率的定义为将原始信息通过编码传输后再解码的最终信息比较得到的错误概率。其中，k 为解码后的信息长度；$m(i)$为第 i 位原始信息；m'为第 i 位传输后获得的信息；e 为 2 个信息的比较函数，2 个信息相同时 e=0，不相同则 e=1。BER 越低代表顽健性越高[14]，如式(27)所示。

$$\mathrm{BER}=\frac{\sum_{i=1}^{k}e(m(i),m'(i))}{k} \tag{27}$$

对区块链网络隐蔽信道顽健性的抗干扰性和抗篡改性证明见 3.2.1 节和 3.2.2 节。

5.3　传输效率评估

对区块链网络隐蔽信道传输效率可定义为最大可能的无错信息速率，单位为 bit/s，如式(28)所示。其中，N 表示 N 元编码在时间 t 内传输的信息量，C 越高代表网络隐蔽信道的传输效率越高[44]。

$$C=\frac{N(t)}{t} \tag{28}$$

假设以某种隐蔽信息载体构建区块链网络隐蔽信道，隐蔽信息载体包括时间型载体和存储型载体 2 类。以比特币为例，时间型载体可以包括交易时间、交易时间间隔等；存储型载体可以包括时间戳、被交易方的比特币地址、被交易方的比特币地址的散列值等。

信息调制方式为码元数量为 S 的信息调制符号表，p_i 为编码表第 i 个编码字符出现的概率，则每个调制符号的信息量 I_i 为

$$I_i=-\mathrm{lb}p_i \tag{29}$$

则调制符号表的信息量的数学期望，即调制符号表的信息熵 $H(S)$为

$$H(S)=-\sum_{i=1}^{S}p_iI_i\ =-\sum_{i=1}^{S}p_i\mathrm{lb}p_i \tag{30}$$

每个隐蔽信息载体可携带的调制符号数为 a，则每个隐蔽信息载体可携带的信息量的数学期望 I_C 为

$$I_C=\ aH(S)\ =-a\sum_{i=1}^{S}p_i\mathrm{lb}p_i \tag{31}$$

单位时间内传输隐蔽信息载体数量，即信息载体的传输速率为 v，则单位时间内传输的信息量，即区块链网络环境下的隐蔽信道传输效率 C 为

$$C=\ vI_C\ =\ -va\sum_{i=1}^{S}p_i\mathrm{lb}p_i \tag{32}$$

式(32)适用于所有类型的区块链网络隐蔽信道。综上所述，可得出以下结论。

1) 在区块链网络隐蔽信道构建方式（即隐蔽信息载体）相同，且编码策略相同的前提下，每个隐蔽信息载体可携带的总信息量 I_C 是相对固定的，不会随着调制符号表的码元数量 S 改变。

2) 在编码方式相同，区块链网络隐蔽信道构建方式相同，即每个隐蔽信息载体的信息量 I_C 相同的前提下，在允许范围内提高信息载体传输速率 v 可提高传输效率 C。一般来说，基于同一种区块链对象的存储型区块链网络隐蔽信道的隐蔽信息载体的传输效率高于时间型网络隐蔽信道，因为时间型区块链网络隐蔽信道的隐蔽信息载体采用改变正常通信时间属性的方式，往往延长隐蔽信息载体的通信时间，并且基于多个区块链对象实例的相对关系，会降低传输速率；而存储型区块链网络隐蔽信道是基于正常的通信时间进行传输的，并且往往只

基于一个区块链对象实例，因此信息载体传输速率较高。

3) 在编码方式相同，且信息载体传输速率 v 相同的前提下，采用隐蔽信息载体信息量 I_C 大的区块链网络隐蔽信道构建方式可提高通信效率 C。一般来说，存储型区块链网络隐蔽信道的隐蔽信息载体信息量大于时间型网络隐蔽信道，因为时间型区块链网络隐蔽信道载体受限于时间属性，只能采取串行传输的方式，一个隐蔽信息载体往往只能携带一个调制符号，因此隐蔽信息载体的信息量 I_C 较小；而存储型区块链网络隐蔽信道因隐蔽信息载体存储属性的不同，往往可以携带多个调制符号，因此隐蔽信息载体的信息量 I_C 较大。

4) 在区块链网络隐蔽信道构建方式（即隐蔽信息载体）相同，且传输速率 v 相同，调制符号表码元数量 S 相同的前提下，可采用不同的调制符号编码策略可提高信息量。如可使用霍夫曼编码对调制符号表的符号的平均编码长度进行压缩，提高调制符号表的信息熵 $H(S)$，从而提高每个隐蔽信息载体可携带的信息量的数学期望 I_C，进而提高通传输效率[44] 。

6 结束语

由于安全可信、去中心化、健壮性等特点，区块链应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域[1-2]，因此，区块链隐蔽信道的应用场景也会随着区块链应用延伸到各个领域中。未来的研究可以基于本文首次提出的区块链网络隐蔽信道模型，结合不同领域区块链具体的应用场景特性（如不同领域应用具体场景下的存储特性和时间特性），构建适用于不同应用场景环境下的区块链网络隐蔽信道。

区块链网络隐蔽信道因其抗干扰性、抗篡改性、多线路通信性、接收方匿名性、线路无关性等特性弥补了传统网络环境下隐蔽信道的弊端。

本文对现有的网络隐蔽信道的缺陷进行了总结，首次提出了区块链网络隐蔽信道模型，对区块链网络隐蔽信道进行了形式化建模，并证明了区块链网络隐蔽信道具有抗干扰性、抗篡改性，同时还具有多线路通信性、接收方匿名性和线路无关性的特性；构建了基于业务操作时间间隔的时间型区块链网络隐蔽信道场景；提出了区块链网络隐蔽信道的抗检测性、顽健性和传输效率这 3 个评估向量，为区块链网络隐蔽信道这一新的网络隐蔽信道类型的实用化奠定了基础。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008, 1(2012): 28.

[2] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.
SHEN X, PEI Q Q, LIU X F. Survey of block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(11): 11-20.

[3] 袁勇, 王飞跃. 区块链技术发展现状与展望[J].自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. ACTA Automatica Sinica, 2016, 42(4): 481-494.

[4] MILLEN J. 20 years of covert channel modeling and analysis[C]//The IEEE Symposium on Security and Privacy. IEEE, 1999: 113-114.

[5] WENDZEL S, ZANDER S, FECHNER B, et al. Pattern-based survey and categorization of network covert channel techniques[J]. ACM Computing Surveys, 2015, 47(3): 1-26.

[6] FISK G, FISK M, PAPADOPOULOS C, et al. Eliminating steganography in internet traffic with active wardens[C]//Revised Papers from the International Workshop on Information Hiding. 2002: 18-35.

[7] HANDLEY M, PAXSON V, KREIBICH C. Network intrusion detection: evasion, traffic normalization, and end-to-end protocol semantics[C]// Conference on Usenix Security Symposium. 2001: 9.

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

[9] GILES J, HAJEK B. An information-theoretic and game-theoretic study of timing channels[J]. Information Theory IEEE Transactions on, 2002, 48(9): 2455-2477.

[10] KANG M H, MOSKOWITZ I S. A pump for rapid, reliable, secure communication[C]//ACM Conference on Computer and Communications Security. ACM, 1993: 119-129.

[11] KANG M H, MOSKOWITZ I S, Chincheck S. The pump: a decade of covert fun[C]//Computer Security Applications Conference. 2006: 360.

[12] SELLKE S H, WANG C C, BAGCHI S, et al. TCP/IP timing channels: theory to implementation[C]//IEEE International Conference on Computer Communications. IEEE, 2007: 2204-2212.

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

[14] HOUMANSADR A, BORISOV N. CoCo: coding-based covert timing channels for network flows[C]//International Conference on Information Hiding. 2011: 314-328.

[15] BACKS P, WENDZEL S, KELLER J. Dynamic routing in covert channel overlays based on control protocols[C]//International Conference for Internet Technology and Secured Transactions. 2012: 32-39.

[16] SZCZYPIORSKI K, MAZURCZYK W, CABAJ K. TrustMAS: trusted communication platform for multi-agent systems[C]// OTM 2008 Confederated International Conferences, Coopis, Doa, Gada, Is, and Odbase. 2008: 1019-1035.

[17] 刘江, 霍如, 李诚成, 等. 基于命名数据网络的区块链信息传输机制[J]. 通信学报, 2018, 39(1):24-33.
LIU J, HUO R, LI C C, et al. Information transmition mechanism of Bloackchain technology based on named-data networking[J]. Journal on Commnications, 2018, 39(1):24-33.

[18] 傅晓彤, 陈思, 张宁. 基于代理的密码货币支付系统[J]. 通信学报, 2017, 38(7):199-206.
FU X T, CHEN S, ZHANG N. Proxy-cryptocurrency payment system[J]. Journal on Commnications, 2017, 38(7):199-206.

[19] LAMPSON B W. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613-615.

[20] 王永吉, 吴敬征, 曾海涛, 等. 隐蔽信道研究[J]. 软件学报, 2010, 21(9): 2262-2288.
WANG Y J, WU J Z, ZENG H T, et al .Covert channel research[J]. Journal of Software, 2010, 21(9): 2262-2288.

[21] 曾海涛, 王永吉, 祖伟, 等. 短消息指标新定义及在事务信道限制中的应用[J]. 软件学报, 2009 , 20 (4) :985-996.
ZENG H T, WANG Y J, ZU W, et al. New definition of small message criterion and its application in transaction covert channel mitigating[J]. Journal of Software, 2009,20(4):985−996.

[22] 王庆, 屠晨阳, 沈嘉荟. 侧信道攻击通用框架设计及应用[J]. 信息网络安全, 2017(5): 57-62.
WANG Q, TU C Y, SHEN J H. Design and application of general framework for side channel attack[J]. Netinfo Security, 2017(5): 57-62.

[23] 周昱, 于宗光. 硬件木马威胁与识别技术综述[J]. 信息网络安全, 2016(1): 11-17.
ZHOU Y, YU Z G. Threat analysis and detection techniques of hardware trojans[J]. Netinfo Security, 2016(1): 11-17.

[24] MILLEN J. 20 years of covert channel modeling and analysis[C]// IEEE Symposium on Security and Privacy. IEEE, 1999: 113-114.

[25] GIRLING C G. Covert channels in LAN's[J]. IEEE Transactions on Software Engineering, 1987, SE-13(2): 292-296.

[26] A D, S C. Exploitation of data streams authorized by a network access control system for arbitrary data transfers: tunneling and covert channels over the http protocol[R]. Technical Report, 2005.

[27] MAZURCZYK W, SMOLARCZYK M, SZCZYPIORSKI K. Retransmission steganography and its detection[J]. Soft Computing, 2011, 15(3): 505-515.

[28] TRABELSI Z, JAWHAR I. Covert file transfer protocol based on the ip record route option[J]. Journal of Information Assurance and Security, 2010(5): 64-73.

[29] SERVETTO S D, VETTERLI M. Communication using phantoms: covert channels in the Internet[C]// IEEE International Symposium on Information Theory. IEEE, 2001: 229.

[30] ROWLAND C H. Covert channels in the TCP/IP protocol suite[J]. First Monday, 1997, 2(2): 32-48.

[31] SEBASTIAN Z , GRENVILLE A , PHILIP B. Covert channels in the IP time to live field[C]//Telecommunication Networks and Application Conference. 2006: 298-302.

[32] JANKOWSKI B, MAZURCZYK W, SZCZYPIORSKI K. Information hiding using improper frame padding[C]//Telecommunications Network Strategy and Planning Symposium. 2010: 1 - 6.

[33] PETITCOLAS F A P, ANDERSON R J, KUHN M G. Information hiding-a survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062-1078.

[34] HERZBERG A, SHULMAN H. Limiting MitM to MitE covert-channels[C]//International Conference on Availability, Reliability and Security. 2013: 236-241.

[35] SWINNEN A, STRACKX R, PHILIPPAERTS P, et al. ProtoLeaks: a reliable and protocol-independent network covert channel[C]// International Conference on Information Systems Security. 2012: 119-133.

[36] 王鹏, 兰少华, 张晶, 等. 一种基于 TCP 时间戳选项的隐蔽信道方法[J]. 解放军理工大学学报（自然科学版）, 2015(2):120-125.
WANG P, LAN S H, ZHANG J, et al. A hidden channel method based on TCP timestamp option[J]. Journal of PLA University of Science and Technology(Natural Science Edition), 2015(2):120-125.

[37] HANDEL T G, SANDFORD M T. Hiding data in the OSI network model[C]//Information Hiding, First International Workshop.1996: 23-38.

[38] GIFFIN J, GREENSTADT R, LITWACK P, et al. Covert messaging through TCP timestamps[C]//International Conference on Privacy Enhancing Technologies. 2002: 194-208.

[39] 安德烈亚斯. 精通比特币[M]. 乔延宏, 译. 南京: 东南大学出版社, 2018.
ANDREAS M. Mastering bitcoin[M]. QIAO Y H, transl. Nanjing: Southeast University Press, 2018.

[40] WENDZEL S, KELLER J. Hidden and under control：a survey and outlook on covert channel-internal control protocols[J]. Annals of Telecommunications, 2014, 69: 417-430.

[41] 程书芝, 师文轩, 刘俪婷. 区块链技术综述[J]. 中国科技论文在线, 2016.
CHENG S Z, SHI W X, LIU L T. Survey on blockchain[J]. Sciencepaper Online, 2016.

[42] CABUK S, BRODLEY C E, SHIELDS C. IP covert timing channels: design and detection[C]//ACM Conference on Computer and Communications Security. ACM, 2004: 178-187.

[43] 吴敬征, 丁丽萍, 王永吉. 云计算环境下隐蔽信道关键问题研究[J]. 通信学报, 2011, 32(9A): 184-203.
WU J Z, DING L P, WANG Y J. Reaserch on key problem of covert channel in cloud computing[J]. Journal on Communications, 2011,

32(9A): 184-203.

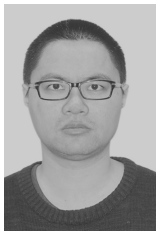
[44] WU J Z, WANG Y J, DING L P, et al. Improving performance of network covert timing channel through Huffman coding[J]. Mathematical & Computer Modelling, 2012, 55(1–2): 69-79.

[45] ZANDER S, ARMITAGE G. CCHEF-covert channels evaluation framework design and implementation[C]//Centre for Advanced Internet Architectures Technical Report, 2008: 1-10.

[46] GIANVECCHIO S, WANG H. Detecting covert timing channels: an entropy-based approach[C]//The 14th Conference on Computer and Communications Security. ACM. 2007: 307-316.

[47] 董庆宽.阈下信道技术研究[D].西安:西安电子科技大学,2003.
DONG Q K. Study on subliminal channels[D]. Xi'an: Xidian University, 2003.

[作者简介]



李彦峰（1984− ），男，山东济宁人，中国科学院软件研究所博士生，主要研究方向为网络隐蔽信道构建与分析。

丁丽萍（1965− ），女，山东青州人，博士，中国科学院软件研究所研究员、博士生导师，主要研究方向为数字取证、系统安全与可信计算。

吴敬征（1982− ），男，河北唐山人，博士，中国科学院软件研究所副研究员，主要研究方向为系统安全、漏洞挖掘、移动安全。

崔强（1985− ），男，辽宁抚顺人，中国科学院软件研究所博士生，主要研究方向为机器学习、推荐算法、众测。

刘雪花（1986− ），女，湖南涟源人，中国科学院软件研究所博士生，主要研究方向为数字取证、系统安全与可信计算。

关贝（1986− ），男，山西运城人，博士，中国科学院软件研究所助理研究员，主要研究方向为人工智能方法和大数据分析方法、网络安全分析技术、操作系统虚拟化技术和安全操作系统。