计算机科学
COMPUTER SCIENCE

基于Websocket协议的车联网隐蔽信道构建

赵辉, 彭建友, 秦玉林, 韩利利

引用本文

赵辉, 彭建友, 秦玉林, 韩利利. 基于Websocket协议的车联网隐蔽信道构建[J]. 计算机科学, 2024, 51(8): 364-370.

ZHAO Hui, PENG Jianyou, QIN Yulin, HAN Lili. Construction of Internet of Vehicles Covert Channel Based on Websocket Protocol [J]. Computer Science, 2024, 51(8): 364-370.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500037

基于 Websocket 协议的车联网隐蔽信道构建

赵 辉 彭建友 秦玉林 韩利利
重庆邮电大学通信与信息工程学院 重庆 400065
信号与信息处理重庆市重点实验室 重庆 400065

摘 要 针对传统车联网协议下的隐蔽信道构建方式单一、无法适用于复杂网络环境的问题,通过分析轻量级物联网应用层协议 Websocket 的数据帧格式和通信机制,提出了一种基于 Websocket 协议的车联网隐蔽信道构建方法。该方法利用信息分离聚合算法将待发送的隐蔽信息进行多维传输,以提升隐蔽信道的传输速率和抗暴露性。同时,考虑到车联网网络的动态拓扑特性,基于跳频技术自适应变换信息分离聚合方式和编码映射表。为了提高信道的隐蔽性,通过最小二乘算法模拟了正常网络流量的传输特性。仿真实验结果表明,所构建的隐蔽信道在面对较差的网络环境时,受到的网络波动影响较小,具有较好的鲁棒性;并且相较于单一维度传输的隐蔽信道,在隐蔽性和传输速率方面有一定的提升。

关键词:车联网;Websocket;信息分离聚合;跳频技术;最小二乘
中图分类号 TP309.2

Construction of Internet of Vehicles Covert Channel Based on Websocket Protocol

ZHAO Hui,PENG Jianyou,QIN Yulin and HAN Lili
1 School of Communication and Information Engineering,Chongqing University of Posts and Telecommunications,Chongqing 400065,China
2 Chongqing Key Laboratory of Signal and Information Processing,Chongqing 400065,China

Abstract Aiming at the problem that the construction method of covert channel under traditional Internet of Vehicles protocol is single and cannot be applied to complex network environment,a construction method of covert channel in Internet of Vehicles based on WebSocket protocol is proposed by analyzing the data frame format and communication mechanism of Websocket—a lightweight application layer protocol of Internet of Things. This method uses information separation and aggregation algorithm to transmit the covert information in multiple dimensions to enhance the transmission rate and anti-exposure of the covert channel. Besides,considering the dynamic topological characteristics of the Internet of Vehicles network,the information separation and aggregation mode and coding mapping table are transformed adaptively based on frequency hopping technology. Finally,in order to improve the concealment of the channel,the least square algorithm is used to simulate the transmission characteristics of normal network traffic. The results of simulation experiments show that the constructed covert channel is less affected by network fluctuations and has better robustness when facing poor network environment. And compared with the covert channel with single-dimension transmission,it has certain improvement in terms of concealment and transmission rate.

Keywords Internet of Vehicles,Websocket,Information separation and aggregation,Frequency hopping technology,Least square

1 引言

车联网是借助新一代通信技术,以交通道路上高速行驶的汽车作为网络节点的一种新型网络[1]。车联网的基础是安全可靠的信息传输。当前,车联网的主要研究工作是设计新型的网络通信协议来保障车联网信息传输的可靠性,并且提高网内信息传输的效率。但是随着车联网技术的不断发展,车联网信息安全问题已经成为车联网通信设计中不可规避的关键问题。

当前车联网中对信息安全的需求主要包括身份认证、保证数据的完整性、机密性和隐私性,其中绝大部分的敏感信息、机密数据都使用传统加密算法进行保护[2]。虽然使用密码学可以有效地防止信息被截获、窃取甚至篡改,进而能够一定程度上保护车辆驾驶人员的生命财产安全,但其在车联网中的信息安全方面也有着一定的局限性。一方面,加密算法会使密文信息变成乱码,对于车联网这种主要利用无线传输信息的开放网络而言,更容易引起攻击者或窃取者的额外关注。另一方面,高性能的加密算法往往复杂度高、耗时长,会

到稿日期:2023-05-08 返修日期:2023-08-30
基金项目:重庆市教委科技研究项目(KJZD-K202000602);四川省重点研发计划项目(2022YFG0022)
This work was supported by the Science and Technology Research Project of Chongqing Municipal Education Commission(KJZD-K202000602) and Key R&D Program of Sichuan Province(2022YFG0022).
通信作者:赵辉(zhaohui@cqupt.edu.cn)

消耗过多的网络资源和占用很大的网络带宽，不利于车辆的正常运转。隐蔽信道作为一种信息隐藏技术，不仅能实现信息的隐秘传输，降低外来攻击者发现并且破译出原始信息的机率，而且也能在不影响车辆正常运转的同时，结合一些常规的密码学算法，从而满足更高等级的安全需求。因此，将隐蔽信道应用在车联网中作为一种保密通信的途径，具有十分重要的意义。

网络隐蔽信道被定义为：一种可以违反系统的安全策略，可逃脱安全设备的检测，通过网络传播将秘密信息泄露出去的技术手段。其大体上分为存储型隐蔽信道和时间型隐蔽信道[3-4]。存储型隐蔽信道主要将网络协议中的可选字段以嵌入的方式进行信息的隐藏。例如，文献[5]基于 Internet 控制消息协议(ICMP)设计了一种基于时间戳的隐蔽信道，将私有消息隐藏在数据包报头和有效载荷之间的时间戳字段中。文献[6]和文献[7]发现在 IPv6 协议字段中构建存储隐蔽通道的可能性，构建了 10 种类型的 IPv6 隐蔽通道，其中包括流标签字段、IPv6 报头的流量类别字段、IPv6 扩展报头的保留字段和 ICMPv6 报头的代码字段。此外，针对一些上层协议，文献[8]和文献[9]提出了 HTTP 协议中可用于构建隐蔽信道的几种常用字段，如 Accept、Cookies 和 URL 字段。此类隐蔽信道往往能获得较大的信道容量，受网络条件的影响较小，但是隐蔽性较弱，易被检测和破坏。

时间型隐蔽信道则利用网络协议数据的时间属性来进行信息的隐藏。例如，Abbas 等[10]提出了一种基于重排序密度的隐蔽定时信道(RDCTC)，并引入了改进的 Turbo 码进行有效的编码，大大提升了信道的传输速率和隐蔽性。Harris 等[11]提出了一种新的物联网隐蔽定时信道，它对预先存在的网络信息(即端口或地址)中的数据进行编码。这种方法消除了对分组间延迟(IPD)进行数据编码的需要，并在 TCP/IP 和 ZigBee 两种物联网协议之间实现了 7 种不同的编码方法。Xu 等[12]为了在不可信的片上网络(NoC)中传输敏感数据，提出了一种基于分组间延迟(IPD)的隐蔽信道，采用 nBmT 块编码的方式平滑延迟分布，使得 IPD 信道更趋向于正常网络流量波动的信道。但此类隐蔽信道的信道容量往往较小，极易受网络环境(如抖动、延迟)的影响。

相对于传统有线和无线网络，目前很少有研究人员关注车联网中的隐蔽通信。Ying 等[13]针对车辆电子控制单元(ECU)的安全认证，提出了 3 种不同的 ECU 认证隐蔽信道，有效地抵御了外来的 CAN 总线攻击。Zhang 等[14]将车辆通信的网络区域划分为安全区域、危险区域和灰色缓冲区域，在对称假设和友好干扰的帮助下，安全区域内的所有车辆通信都是隐蔽的，这极大地提高了车辆的安全通信。Taheri 等[15]提出了一种基于发射机无线电范围内车辆流量的动态混合隐蔽信道，通过改变服务和控制分组的定时模式以及利用控制信道中周期性状态消息中的一些存储字段来发送隐蔽消息。但以上构建方式往往没有考虑车辆运行过程中网络环境的变化对隐蔽信道影响。

Websocket 协议是 HTML5 标准下的一种面向 TCP 连接的全双工通信协议，该协议打破了传统基于长轮询的通信方式，并为客户端与服务端之间构建了一条双向实时的传输通道[16]，其对于一些资源受限的不可靠网络，如网络流量消耗大、传输请求时间长的网络，具有良好的适应性，已成为当前应用最广泛的物联网通信协议之一。本文通过对 Websocket 协议进行分析，提出并实现了一种基于 Websocket 协议的隐蔽信道构建方法，为实现隐蔽信道向车联网的数据传输安全迁移提供了一定的理论支持和技术支撑。

2　Websocket 协议分析

2.1　Websocket 协议的数据帧格式

Websocket 协议诞生于 2008 年，2011 年成为国际标准，目前已经兼容所有浏览器，是一种新的异步通信协议。Websocket 基于 TCP 传输协议，并且复用 HTTP 的握手通道，是 HTML5 标准规定的一项浏览器同服务器间的通信协议，其支持持久连接，属于应用层协议[17]。

Websocket 数据帧格式如图 1 所示。在 Websocket 协议中，数据是通过帧序列来传输的。为了保障数据的安全，发送方要对数据进行掩码加密，如果接收方收到一个没有掩码的数据帧时，就会断开连接。

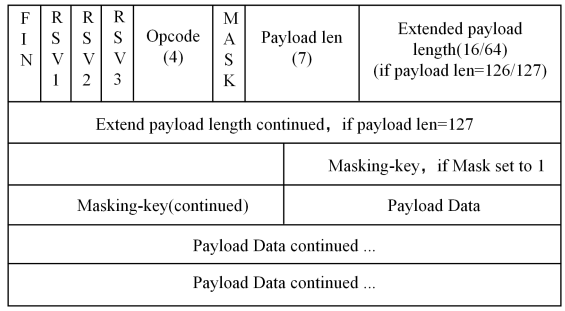

图 1　Websocket 数据帧格式

Fig. 1　Frame format of Websocket data

表 1 中，FIN 表示消息是否为最后一个数据帧；RSV1，RSV2，RSV3 为保留字段，一般为 0，除非对 Websocket 进行扩展；Opcode 表示传输数据帧的类型，一般情况下有 6 种类型；Mask 是一个标志字段，用来表示数据帧的数据是否进行掩码处理；Payload length(7 位＋16 位，或者 7 位＋64 位)定义了负载数据的长度；Masking-key 是可选字段，该区块用于存储掩码密钥；Payload data 表示扩展数据，一般为 0，除非已经协商了一个扩展。

2.2　Websocket 协议的通信机制

Ajax 轮询与 Websocket 的工作机制[18]如图 2 所示。图中左边部分是常见的基于 Ajax 轮询的通信方式。在特定的时间间隔内，客户端向服务端发出 HTTP 请求，如果服务端没有可以立即返回给客户端的数据，则不会立刻返回一个空结果，而是保持这个请求等待数据到来，之后将数据作为结果响应给客户端。由于每次通信都是基于请求-响应，这种通信机制往往会消耗过多的资源和带宽，增加不必要的请求时间。

图中右边部分是 Websocket 协议的通信机制。在特定的时间间隔内，客户端向服务端发出类似 HTTP 协议的请求，表明要将目前所用协议升级成 Websocket 协议，若服务端支持此类协议的升级条件，会向客户端发送一个 101 的状态响应码，若不支持，则会相应地返回其他含义的状态响应码，以

说明具体缘由。一旦连接建立后，通信双方可以在任意时刻通过 Websocket 数据帧向对方实时传递数据，大大节省了不必要的网络请求时间和带宽。

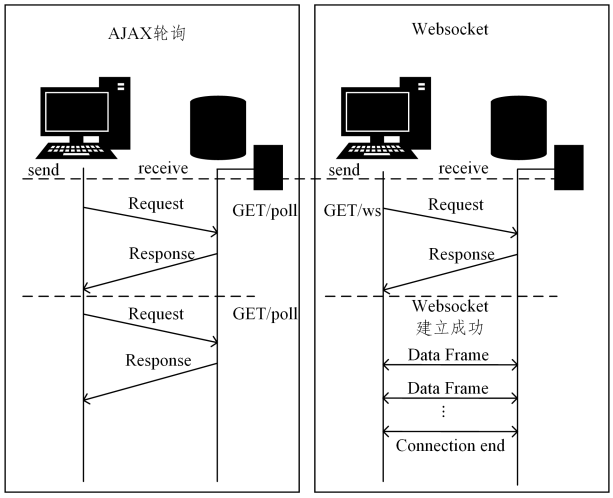

图 2 Ajax 轮询与 Websocket 的通信机制

Fig. 2 Ajax polling and Websocket communication mechanism

2.3 Websocket 隐蔽信道的可行性分析

Websocket 协议作为当前应用最广泛的物联网应用层协议之一，同样适用于车联网[19]。它可以在公开信道下传送大量信息，为秘密信息的传输提供充足的载体，使得防火墙等网络防护设施难以识别出隐蔽信道的存在。将其作为载体构建隐蔽信道的可行性原因有：

1）Websocket 使用了面向连接的 TCP 作为传输层协议，具有较好的消息可靠传输机制，可增强秘密信息传输的可靠性，降低秘密信息丢失的概率。

2）Websocket 具有较小的控制开销。在连接创建后，客户端与服务端之间交换数据时，用于协议控制的数据包头部相对较小，减少了无用数据传输。

3）Websocket 具备持久通信的能力。建立连接后，客户端与服务端完全对等，可以相互请求，减少了不必要的网络请求时间损耗和网络流量，提升了秘密信息的传输速率。

3 Websocket 隐蔽信道构建

3.1 Websocket 隐蔽信道模型

通信双方在传输隐蔽信息之前，会共享隐蔽信息的编解码方案。发送方对隐蔽信息进行编码，并根据编码结果选取对应载体，实现隐蔽消息的隐藏。接收方收到相应的数据包后进行解码，得到隐蔽消息。

本文依据 Websocket 协议的数据帧格式，选取了 Opcode 字段的几种传输数据类型，作为隐蔽信道的载体，相关类型如表 1 所列。将 0x89 数据类型作为隐蔽通信开始的标志，0x88 数据类型作为隐蔽通信结束的标志，其余 4 种数据类型作为隐蔽信息的映射。图 3 给出了隐蔽数据的传输模型，它在传统通信模型的基础上，分别在发送方和接收方添加信息分离模块和信息聚合模块，通过对隐蔽信息进行片分离，避免了因数据帧被外来攻击者截获而直接破译出隐蔽信息。发送方的编码模块和加密模块采用了十六进制编码算法和 sha1＋base64 的加密算法，可有效提升正常通信中隐蔽消息的数量和安全性。与此同时，考虑到车联网中网络环境的动态拓扑特性，通过传感装置将检测到的车流量、车位置和车速作为影响网络环境的性能指标，基于跳频技术自适应变化信息分离聚合算法和编码映射。最后，对整体隐蔽信道进行了优化处理，通过最小二乘优化算法模拟了真实的网络流量分布情况，以提高隐蔽信道的隐蔽性。

表 1 选用的数据类型及其含义

Table 1 Selected data types and their meanings

数据类型	含义
0x80	持续连续帧
0x81	文本帧
0x82	二进制帧
0x88	断开帧
0x89	Ping 帧
0x8A	Pong 帧

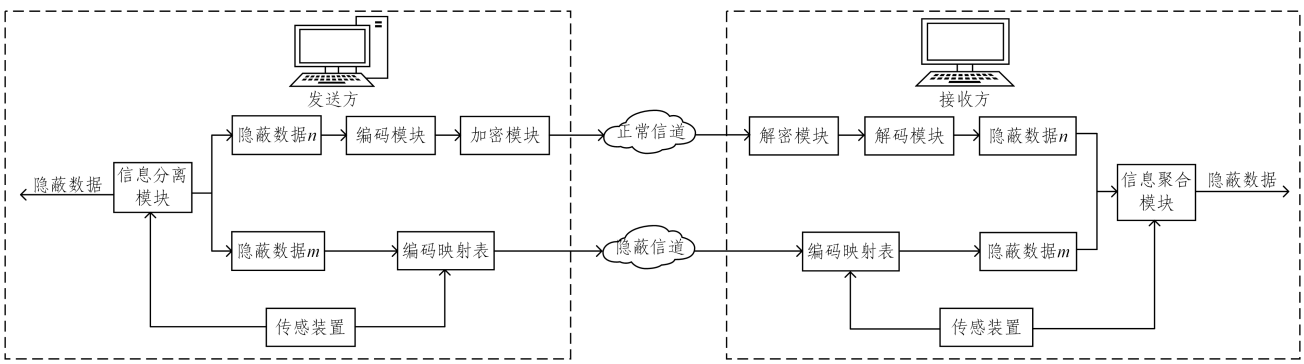

图 3 隐蔽数据的传输模型

Fig. 3 Transmission model of covert data

3.2 信息分离聚合算法

传统隐蔽信道的设计方式往往是单一的传输通道，这种方式的弊端为：首先，如果外来攻击者截取到数据包流，并且破解出了隐蔽信息的传输载体，则隐蔽信息会直接被解析出来，抗暴露性的能力较弱；其次，单一隐蔽信道的传输速率较低，导致携带隐蔽信息传输包的数量增多，也就增加了隐蔽信息被发现的可能性。

信息分离聚合算法旨在构建多维隐蔽信道，本文主要构建二维隐蔽通道，将正常数据通道看作一种伪隐蔽通道，其具体算法流程如下：

1）将待发送的隐蔽数据比特流 I 分解成个 n 大小相同的隐蔽信息分量：

$$S.separate(I)=[I_1,I_2,\cdots,I_n] \tag{1}$$

2）将 n 个大小相同的隐蔽信息分量 I_i 再次分解成 n 个单位大小的信息分量：

$$S.separate(I_i)=[J_1,J_2,\cdots,J_n] \tag{2}$$

3）使用组合方式从中选取 $n-m$ 个信息分量用于伪隐蔽信道的编码加密，m 个用于隐蔽信道的映射，则算法的组合类型 Q 有：

$$Q(I)=(C_n^{n-m})^n \tag{3}$$

4）将 $n-m$ 信息分量经由 C_i 进行传输，m 个信息分量经由 A_i 进行传输，则发送一次传输的隐蔽数据为：

$$I_i=C_isend(I_{n-m})+A_isend(I_m) \tag{4}$$

5）通过持续接收发送方发来的隐蔽信息分量 I_i，从而还原出完整的隐蔽数据：

$$R.separate([I_1,I_2,\cdots,I_n])=I \tag{5}$$

其中，S 是发送端，R 是接收端，C_i 是伪隐蔽信道组，A_i 是隐蔽信道组。为了保证还原出的隐蔽数据无误，每次信息分离和聚合的方式是同步且唯一的。

3.3　基于信息分离聚合算法的数据传输原理

在用 Websocket 协议构建隐蔽信道和伪隐蔽信道时，基于信息分离聚合算法将待发送的隐蔽数据比特流 I 分解成 n 个大小为 10 的信息分量，并再次将其分解成 10 个单位大小的信息分量。通过数学组合的方式从中选取 8 个作为伪隐蔽信道传输分量，经过十六进制数字编码算法，编码成 2 个数字字符，将其隐藏在伪隐蔽数据流中进行加密传输。选取 2 个作为隐蔽信道传输分量，通过隐蔽传输载体进行编码映射。接收方在经过 n 次同步的解密、解码、映射和聚合后，还原出原始的隐蔽数据，具体数据分离聚合过程如图 4 所示。此外，针对部分数据流大小小于 10 的情况，设置优先传输顺序隐蔽信道大于伪隐蔽信道，从而保证数据传输的完整性。

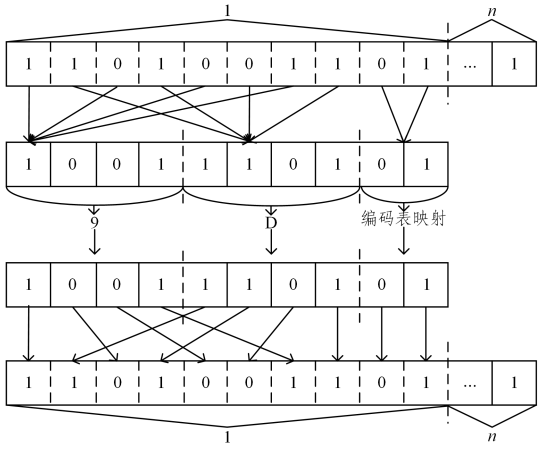

图 4　隐蔽数据的分离聚合流程

Fig. 4　Separation and aggregation process of covert data

3.4　基于跳频技术适应动态网络环境

在隐蔽信道应用于车联网的过程中，由于网络环境的动态拓扑特性，在网络环境相对良好的情况下，受到节点入侵的概率较小，反之亦然。单一的映射规则和分离算法在网络环境较差时有可能被攻击者解码破译。因此，适应车联网中网络环境的动态拓扑特性成为了隐蔽信道构建的关键问题之一。通常情况下，车辆网络环境的变化基于以下 3 个因素：

1）车辆的实时速度；

2）车辆的实时位置；

3）车辆的车流量情况。

其中，将车辆的实时位置作为影响网络环境变化的因素之一是基于以下两点考虑：

1）当车辆处于网络事故多发路段时，外界的遮挡物和其他的一些无线电设备的干扰，可能会对整体的车联网网络环境造成一定的影响，从而加大信息在传递过程中的危险性。

2）当车辆处于网络信号覆盖弱或者覆盖不到的区域时，整体网络的稳定性和通信质量会下降，从而增加了外来攻击者发现并且破译出隐蔽信息的可能性。

跳频技术是无线电保密通信的方式之一。为了防止基于无线电的保密通信过程被第三方窃听，通信双方会约定在通信过程中随时变换无线电的频率，变换的频率序列是双方事先约定好的。

如表 2 和表 3 所列，本文通过车内传感装置，将监测到的车速、位置或流量情况上传给终端设备，并将其动态划分为 4 个区间，$V\in[v_1,v_2,v_3,v_4]$，基于跳频技术变换信息分离聚合算法和编码映射，从而保证隐蔽数据在复杂网络环境的安全性。

表 2　信息分离聚合算法的动态变换

Table 2　Dynamic transformation of information separationand aggregation algorithm

v_1	v_2	v_3	v_4
分离聚合 1	分离聚合 2	分离聚合 3	分离聚合 4
分离聚合 5	分离聚合 6	分离聚合 7	分离聚合 8
⋮	⋮	⋮	⋮
分离聚合 $n-3$	分离聚合 $n-2$	分离聚合 $n-1$	分离聚合 n

表 3　编码映射的动态变换

Table 3　Dynamic transformation of encoding mapping

	0x80	0x81	0x82	0x8A
v_1	00	01	10	11
v_2	00	01	11	10
v_3	00	10	01	11
v_4	00	10	11	01
⋮	⋮	⋮	⋮	⋮

3.5　隐蔽信道优化

隐蔽性是保护数据传输安全最关键的因素之一。然而，短时间内向接收方发送大量的携带隐蔽信息的数据帧，会出现网络流量异常的情况，极易被一些网络流量审计检测方法识别，导致信道的隐蔽性大打折扣。因此，在模拟发送端发送 Websocket 数据帧时需要仿照正常流量的访问时间间隔。根据文献[20]对一些常用协议网络流量的统计和估算，大多数网络流量数据包的时间间隔近似服从泊松分布。

假定 Websocket 流中的正常数据帧发送也遵循泊松分布。为了将隐蔽信道的网络流量模拟成正常信道的网络流量，本文提出通过最小二乘优化算法来求取正常信道与隐蔽信道误差的全局最优解，从而模拟真实的网络流量，提高隐蔽性，具体算法步骤如算法 1 所示。

算法 1 最小二乘算法

输入：数据集$((x_i,y_i))$，其中$(i=1,2,\cdots,N)$，目标函数$(f(x))$，初始参数估计(θ_0)，收敛容差(ε)

输出：最优参数估计 $\hat{\theta}$

1. 初始化参数估计：$(\theta^{(0)}=\theta_0)$，迭代计数器$(k=0)$
2. 重复以下步骤直到收敛或达到最大迭代次数：
   2.1. 对每个样本$((x_i,y_i))$计算残差$(e_i=y_i-f(x_i,\theta^{(k)}))$
   2.2. 计算目标函数的梯度$(\nabla J(\theta))$（即误差函数对参数的偏导数）
   2.3. 计算参数更新量$(\Delta\theta=-(\nabla J(\theta^{(k)}))^{T}\nabla J(\theta^{(k)})^{-1}\nabla J(\theta^{(k)}))$
   2.4. 更新参数估计：$(\theta^{(k+1)}=\theta^{(k)}+\Delta\theta)$
   2.5. 检查是否满足收敛条件：若$(\|\Delta\theta\|<\varepsilon)$或达到最大迭代次数，则停止迭代
   2.6. 更新迭代计数器：$(k=k+1)$
3. 返回最优参数估计$(\hat{\theta}=\theta^{(k)})$

4 实验与结果分析

4.1 实验设置

隐蔽通信场景如图 5 所示。实验环境主要由 5 台主机和 1 台交换机构成。其中，PC1 和 PC2 模拟了车辆通信过程中的发送端和接收端；PC3 作为网络环境模拟器搭载 Netem，通过设置不同的丢包率来模拟实际复杂的网络环境；PC4 搭载了 Windows 防火墙、360 安全卫士、Snort 入侵检测系统等安全防护软件，用于检测信道的隐蔽性；PC5 作为车辆的传感装置，用于模拟车辆的实时速度、位置和流量情况。整个通信过程在 Linux 平台搭建下完成。

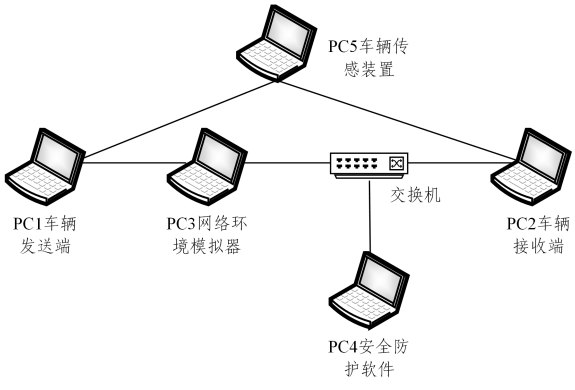

图 5 隐蔽通信场景示意图

Fig. 5 Schematic diagram of covert communication scenario

整个实验场景适用于车联网中常见的几种信息交互的模式（如车对车、车对人等）。由于隐蔽信道本身采用的是点对点的通信方式，因此其信息的编解码方式、映射方式也只有唯一的收发双方知道。故在本实验场景中，利用一台主机模拟车辆的发送端，另外一台主机模拟车辆的接收端（包括车、人等移动接收设备）。此外，考虑到本文设计的信息分离聚合算法和编码映射表的变换方式是依据车辆传感器将检测到的影响网络环境的因素上传给终端设备，故用另外一台主机模拟真实的车辆传感装置。最后，为了模拟出动态拓扑的车联网网络环境，利用一台主机搭载网络环境模拟器 Netem，从而设置不同的丢包率以还原真实网络环境。交换机则可以收集流经网关的数据包，以便另一台主机配置相关的检测系统，检验整体设计的隐蔽信道的隐蔽性强弱如何。整体实验场景具有一般性，符合一些常见的车辆通信场景。

4.2 隐蔽性分析

隐蔽性作为实现隐蔽信道的根本要求，主要是指隐蔽信道不被发现的能力。为了验证信道的隐蔽性，首先通过 Snort 入侵检测系统、Windows 防火墙、360 安全卫士等安全防护软件对信道的隐蔽性进行测试，结果如表 4 所列。可以看出，隐蔽信息在传递的过程中，Snort 入侵检测系统等安全防护软件均未发生报警拦截，说明隐蔽信息对于一般网络防护软件具有很强的穿透性，信道的隐蔽性较好。

表 4 隐蔽性测试结果

Table 4 Concealment test results

安全防护软件	是否报警
Snort 入侵检测系统	否
Windows 防火墙	否
360 安全卫士	否
诺顿防火墙	否

其次，每隔 1 s，测试了 1 000 次正常 Websocket 数据流的网络流量分布情况，图 6 和图 7 分别给出了正常流量的分布折线图和直方图。从图中可以看出，Websocket 正常流量的单位时间发包量近似服从 40 个/秒的泊松分布。对此，采用 3.5 节的最小二乘优化算法，求取了正常信道与隐蔽信道二者误差的全局最优解，从而模拟了正常网络流量分布情况。其正常流量和隐蔽流量的单位时间内发包量对比实验结果如图 8 所示，可以看出两种通信方式产生的流量分布基本一致，没有明显区别。由此可得，利用最小二乘优化算法可以很好地模拟正常网络通信行为，从而降低某些审计流量检测的成功率，提高隐蔽信道的隐蔽性。

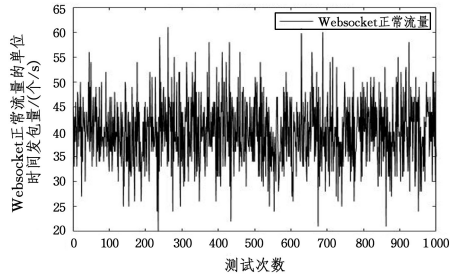

图 6 Websocket 正常流量分布折线图

Fig. 6 Line chart of normal traffic distribution of Websocket

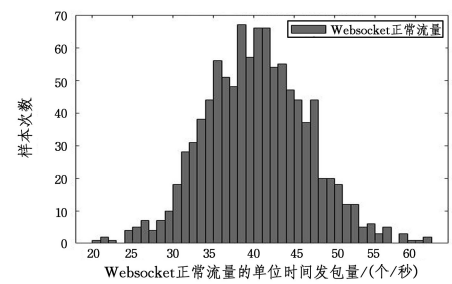

图 7 Websocket 正常流量分布直方图

Fig. 7 Histogram of normal traffic distribution of Websocket

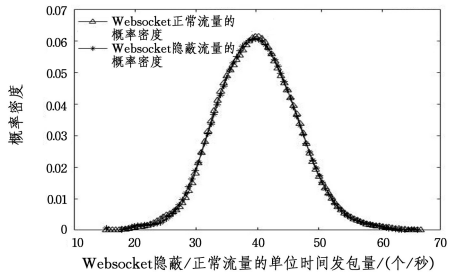

图 8　Websocket 正常流量和隐蔽流量的分布对比

Fig. 8　Comparison of the distribution of normal and covert Websocket traffic

4.3　鲁棒性分析

鲁棒性指隐蔽信道在复杂网络环境下抵御外来干扰并准确传输数据的能力。由于 Websocket 协议本身使用了面向连接的 TCP 作为传输层协议，具有良好的消息可靠传输机制，一定程度上避免了数据帧发生乱序、丢包、重复的现象。而在面对更为严苛的复杂网络环境时，为了验证信道抵御外来干扰的能力，通过网络环境模拟器 Netem 配置了丢包率在 5%，10%和 15%的网络环境，分别测试了传输 10kB 和 20kB 的隐蔽信息的正确率，结果如表 5 所列。可以看出，得益于 Websocket 协议本身优秀的可靠消息传输机制，即使在丢包率为 15%的网络环境中，其传输正确率也能达到 100%。

表 5　鲁棒性测试结果

Table 5　Robustness test results

隐蔽信息大小/kB	丢包率		
	5%	10%	15%
10	100.0	100.0	100.0
20	100.0	100.0	100.0

此外，针对不同的网络环境，统计并计算了基于 Websocket 协议的车联网隐蔽信道、基于数据包时间间隔的隐蔽信道和基于分布特征的时间型隐蔽信道的传输正确率，结果如表 6 所列。可以看出，由于传统时间型隐蔽信道主要利用协议数据单元的时间特性进行传输，网络的丢包、延迟会对其传输的正确率造成一定的影响，而本文构建的隐蔽信道在面对较差的网络环境时，受到的网络波动的影响较小，具有较好的鲁棒性。

表 6　不同隐蔽信道类型的鲁棒性测试结果

Table 6　Robustness test resultsof different covert channel types

隐蔽信道类型	丢包率		
	5%	10%	15%
基于 Websocket 协议的车联网隐蔽信道	100.0	100.0	100.0
基于数据包时间间隔的隐蔽信道	93.4	90.5	82.6
基于分布特征的时间型隐蔽信道	86.3	80.5	75.6

4.4　传输速率分析

信道的传输速率也称传输容量，一般指在单位时间内通过信道传输的隐蔽信息量，或是单个数据包能携带的隐蔽信息的比特数。文献[21]中提出的基于 MQTT 协议命令分组编码隐蔽信道模型使得单个命令可传输 8/3 比特信息；文献[22]中提出的基于 CoAP 协议参数序列的隐蔽信道模型可实现单次传输 3bit 的隐蔽信息；文献[23]中提出的基于 HTTP 协议组合的隐蔽信道模型每次最多可传输 5bit 数据。对此，本文每隔 20Byte 传输一次隐蔽信息，每组测试 10 次，统计并计算了文献[21-23]和基于 Websocket 协议的隐蔽信道在不同字节大小时的隐蔽传输速率，表 7 和图 9 分别给出了不同协议下隐蔽传输速率的测试结果和折线图。

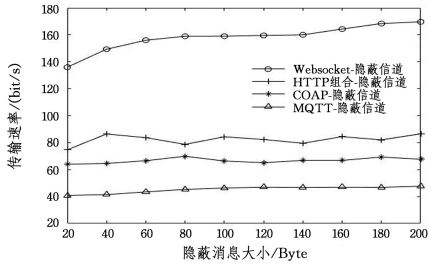

图 9　不同协议构建的隐蔽信道传输速率

Fig. 9　Transmission rates of covert channel constructed by different protocols

表 7　传输速率测试结果

Table 7　Transmission rate test results

(bit/s)

方法	单次传输的比特数/bit	20 字节	40 字节	60 字节	80 字节	100 字节	120 字节	140 字节	160 字节	180 字节	200 字节
本文方法	10	136.00	149.33	156.00	158.93	159.00	159.54	160.00	164.32	168.40	169.65
文献[21]	8/3	40.80	41.40	43.42	45.30	46.31	46.92	46.72	46.91	46.81	47.64
文献[22]	3	64.00	64.53	66.57	69.87	66.34	65.10	66.81	66.81	69.32	67.64
文献[23]	5	74.67	86.40	83.66	78.73	84.32	82.29	79.55	84.41	82.04	86.55

可以看出，相比其他协议使用不同方法构建的隐蔽信道，本文通过信息分离聚合算法构建的基于 Websocket 协议的隐蔽信道在单次传输的比特数和传输速率方面有着明显的优势。

结束语　针对传统车联网协议下的隐蔽信道构建方式单一、无法适用于复杂网络环境的问题，通过对轻量级物联网应用层协议 Websocket 进行研究，提出并实现了一种基于 Websocket 协议的车联网隐蔽信道构建方法。该方法打破了单一维度隐蔽信道构建的模式，实现了二维乃至多维信道的传输。另一方面，基于跳频技术动态变换了信息分离聚合算法和编码映射，适应了车联网网络环境的动态拓扑特征。最后，利用最小二乘优化算法模拟了真实的网络流量分布情况，降低了某些审计流量方法检测的成功率。实验结果表明，该方法构建的隐蔽信道具有较好的隐蔽性、鲁棒性和传输速率。下一步工作是更精确地评判车辆因素对隐蔽信道的影响，并发掘更多可构建隐蔽信道的载体。

参 考 文 献

[1]　TASLIMASA H, DADKHAH S, NETO E C P, et al. Security

issues in Internet of Vehicles (IoV): A comprehensive survey [J]. Internet of Things, 2023, 22: 100809.
[2] MAKHDOOM I, ABOLHASAN M, LIPMAN J. A comprehensive survey of covert communication techniques, limitations and future challenges [J]. Computers & Security, 2022, 120: 102784.
[3] AL-KHULAIDI N A, ZAHARY A T, HAZAA M A S, et al. Covert Channel Detection and Generation Techniques: A Survey [C]// 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA). IEEE, 2023: 1-9.
[4] ELSADIG M A, GAFAR A. Covert channel detection: machine learning approaches [J]. IEEE Access, 2022, 10: 38391-38405.
[5] LU J, DING Y, LI Z, et al. A timestamp-based covert data transmission method in Industrial Control System [C]// 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC). IEEE, 2022: 526-532.
[6] WANG J, ZHANG L, LI Z, et al. CC-Guard: An IPv6 Covert Channel Detection Method Based on Field Matching [C]// 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/Smart City/DependSys). IEEE, 2022: 1416-1421.
[7] DUA A, JINDAL V, BEDI P. Detecting and Locating Storage-Based Covert Channels in Internet Protocol Version 6 [J]. IEEE Access, 2022, 10: 110661-110675.
[8] SEMUSHIN S, SEYTNAZAROV S. HTTP Header Reordering-based Covert Channel Protocol [C]// 2023 6th International Conference on Signal Processing and Information Security (ICSPIS). IEEE, 2023: 145-150.
[9] SZARY P, MAZURCZYK W, WENDZEL S, et al. Analysis of reversible network covert channels [J]. IEEE Access, 2022, 10: 41226-41238.
[10] ABBAS M K, SANDIKKAYA M T. An efficient VoLTE covert timing channel for 5 G networks: RDCTC [J]. Optik, 2022, 270: 170076.
[11] HARRIS K, HENRY W, DILL R. A network-based IoT covert channel [C]// 2022 4th International Conference on Computer Communication and the Internet (ICCCI). IEEE, 2022: 91-99.
[12] XU J, WANG X, JIANG Y, et al. Secured Data Transmission Over Insecure Networks-on-Chip by Modulating Inter-Packet Delays [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41(11): 4313-4324.
[13] YING X, BERNIERI G, CONTI M, et al. Covert channel-based transmitter authentication in controller area networks [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(4): 2665-2679.
[14] ZHANG H, ZOU Y, YU D, et al. Covert communications with friendly jamming in Internet of vehicles [J]. Vehicular Communications, 2022, 35: 100472.
[15] TAHERI S, MAHDAVI M, MOGHIM N. A dynamic timing-storage covert channel in vehicular ad hoc networks [J]. Telecommunication Systems, 2018, 69: 415-429.
[16] SHARMA N, AGARWAL R. HTTP, WebSocket, and SignalR: A Comparison of Real-Time Online Communication Protocols [C]// International Conference on Mining Intelligence and Knowledge Exploration. Cham: Springer Nature Switzerland, 2023: 128-135.
[17] FU Y, GARCÍA-VALLS M. Security aspects of full-duplex web interactions and WebSockets [C]// 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA). IEEE, 2023: 1-8.
[18] BAYıLMıŞ C, EBLEME M A, ÇAVUŞOĞLU Ü, et al. A survey on communication protocols and performance evaluations for Internet of Things [J]. Digital Communications and Networks, 2022, 8(6): 1094-1104.
[19] KAVAS-TORRIS O, GELBAL S Y, CANTAS M R, et al. V2X communication between connected and automated vehicles (CAVs) and unmanned aerial vehicles (UAVs) [J]. Sensors, 2022, 22(22): 8941.
[20] LIU Y, GHOSAL D, ARMKNECHT F, et al. Robust and undetectable steganographic timing channels for iid traffic [C]// Information Hiding: 12th International Conference, IH 2010, Calgary, AB, Canada, June 28-30, 2010, Revised Selected Papers 12. Berlin: Springer, 2010: 193-207.
[21] DENG Y X, TANG Z G, ZHANG J, et al. Research on covert channels based on block coding of MQTT protocol commands [J]. Computer Engineering, 2019, 45(11): 138-143.
[22] GUO R, DU Y H, LU T L, et al. Covert channel based on CoAP protocol parameter sequence [J]. Computer Applications and Software, 2021, 38(8): 138-143.
[23] CHEN C, LUO S L, WU Q, et al. Research on Covert channel Construction Method Based on HTTP Protocol Combination [J]. Netinfo Security, 2020, 20(6): 57-64.

ZHAO Hui, born in 1980, Ph.D, professor, doctoral supervisor. Her main research interests include information security and vehicle networking security.

(责任编辑:何杨)