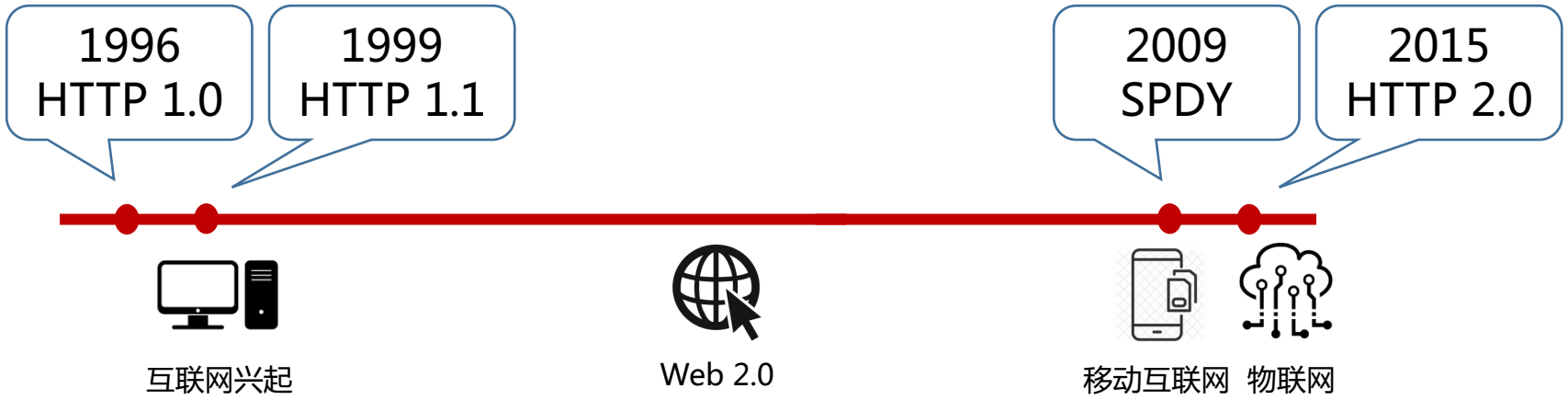
互联网数据传输协议QUIC 研究综述

李学兵, 陈阳, **周孟莹**, 王新

{xbli16, chenyang, **myzhou19,** xinw}@fudan.edu.cn

第八届中国互联网学术年会　CCF ICoC 2019

前期相关工作



优化措施

- TCP -> BBR拥塞控制算法
- SSL/TLS -> TLS 1.3
- HTTP -> SPDY, HTTP 2.0

协议结构性问题

- TCP的三次握手：延时
- TCP的可靠性：队头阻塞

在现有的 TCP、TLS 协议之上实现一个全新的应用层协议

没有连接的概念，不需要三次握手的UDP

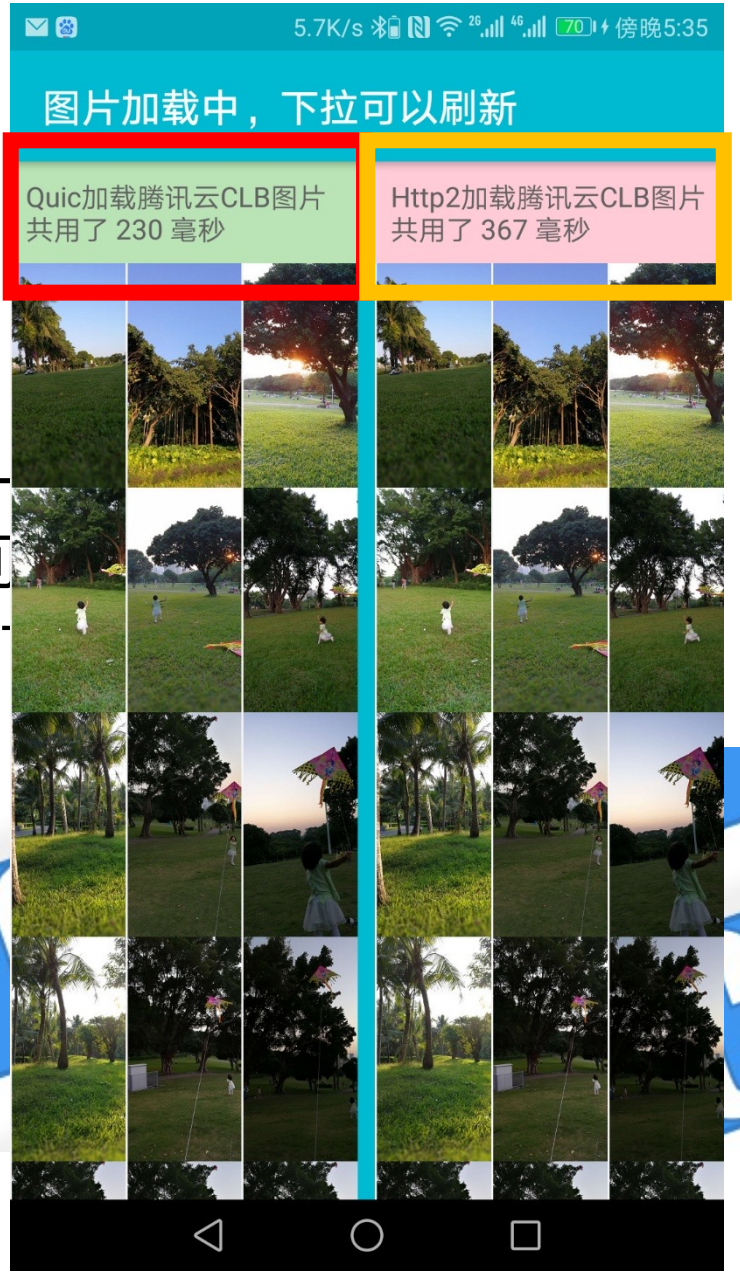
QUIC协议

Making the internet faster with...

Quick
UDP
Internet
Connections

协议特性

- QUIC汇集了 TCP 和 UDP 的优点：
  - **UDP**：传输数据以加快网络速度，降低延迟
  - **应用程序层面**：TCP 的可靠性，TLS 的安全性和 H
  - **只需要应用程序层面支持**：避开了操作系统和中间
- QUIC 相比现在广泛应用的 TCP + TLS + HTTP2 协议有如
  - 避免队头阻塞的多路复用
  - 减少了 TCP 三次握手及 TLS 握手时间



https://github.com/tencentyun/clb-quic-demo

协议特性

- 多路传输
  - QUIC 通过对多路传输的支持，解决了TCP中的队头阻塞问题，减少了延时。

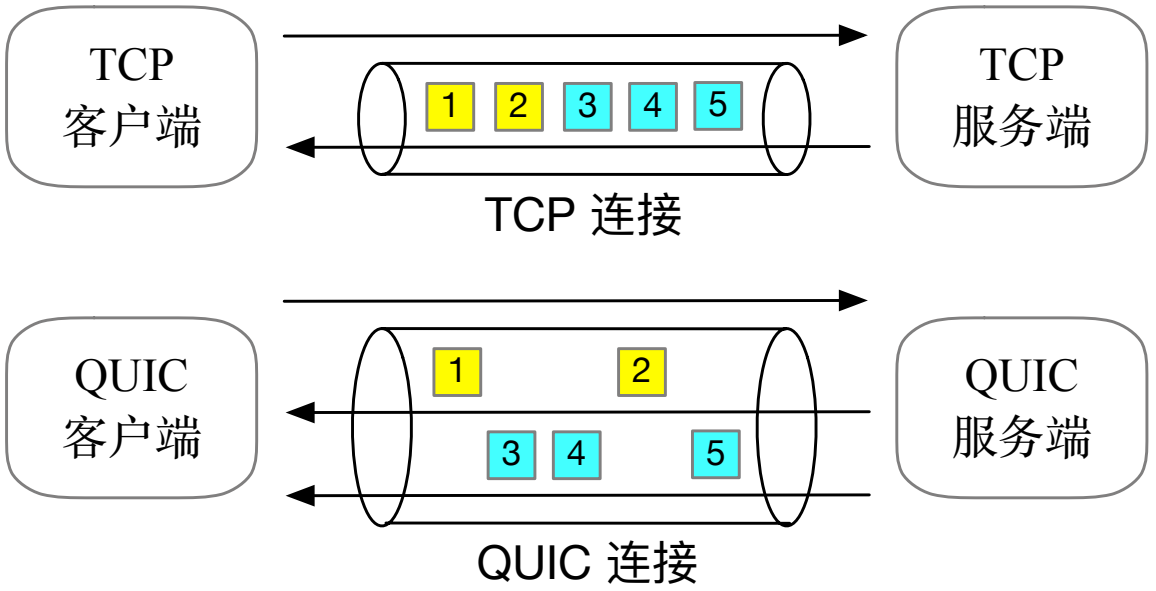


图 2　多路传输与单路传输的对比

协议特性

- 握手协议
  - QUIC 设计了自己的握手协议，达到了更低的握手延时，显著减少用户访问网络的延迟感，提升用户体验

往返时间
Round Trip Time, RTT

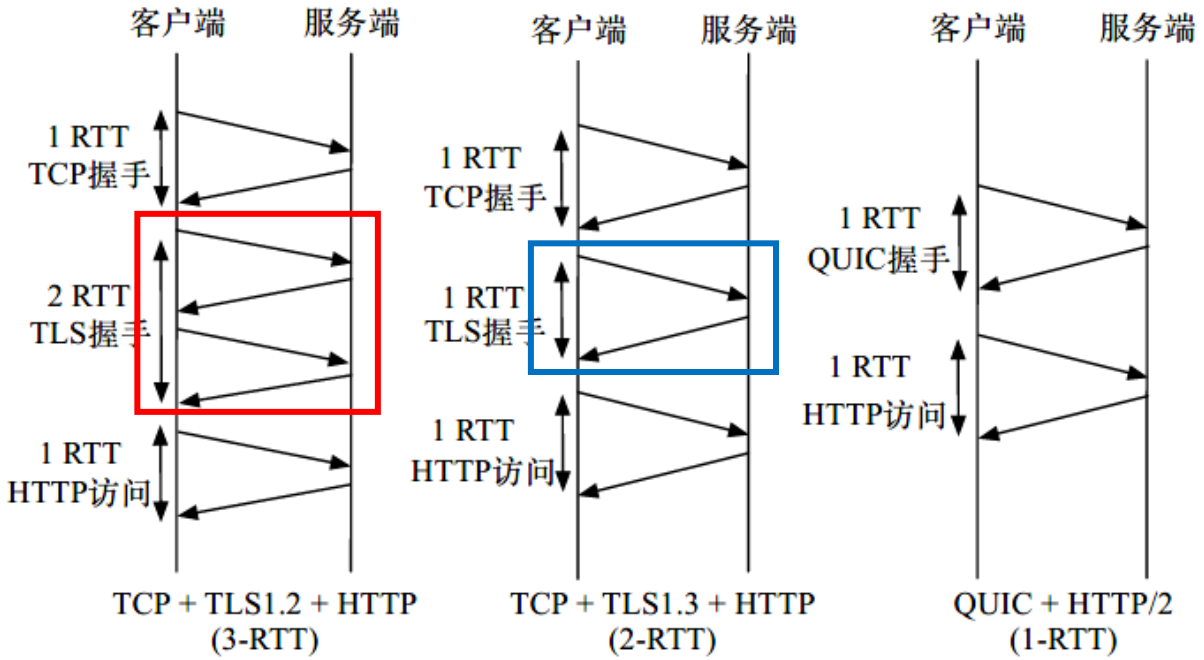


图 3　不同协议握手延时的对比

协议特性

- 握手协议
  - QUIC 设计了自己的握手协议，达到了更低的握手延时，显著减少用户访问网络的延迟感，提升用户体验

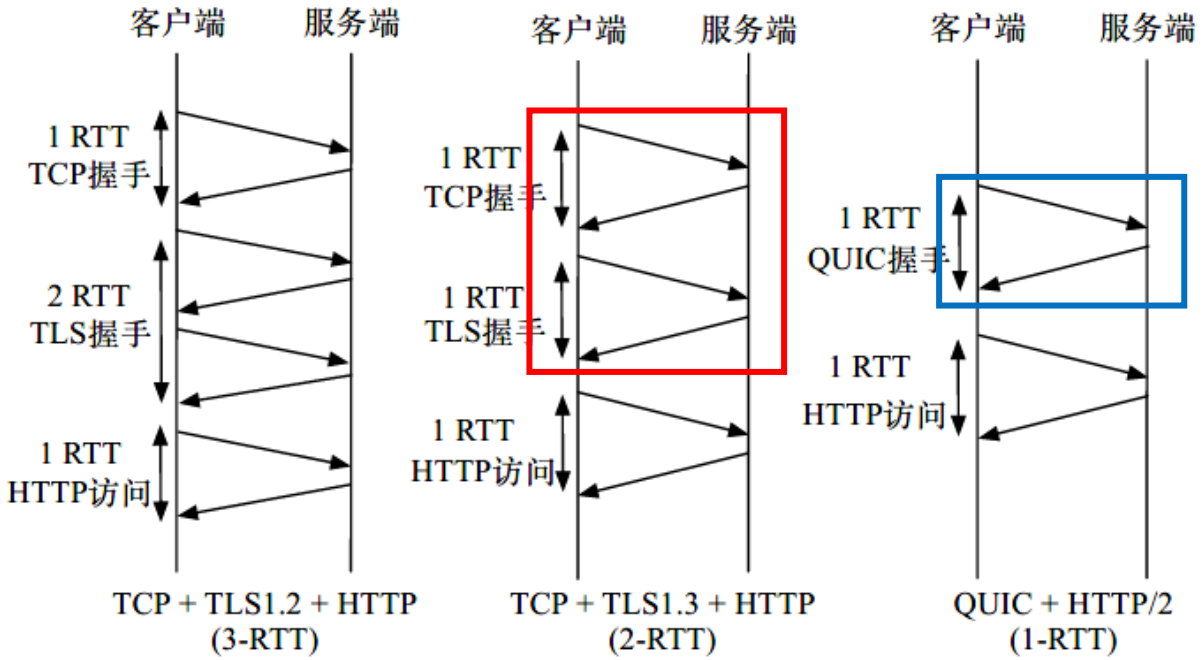


图 3　不同协议握手延时的对比

协议特性

- 握手协议
  - QUIC 设计了自己的握手协议，达到了更低的握手延时，显著减少用户访问网络的延迟感，提升用户体验

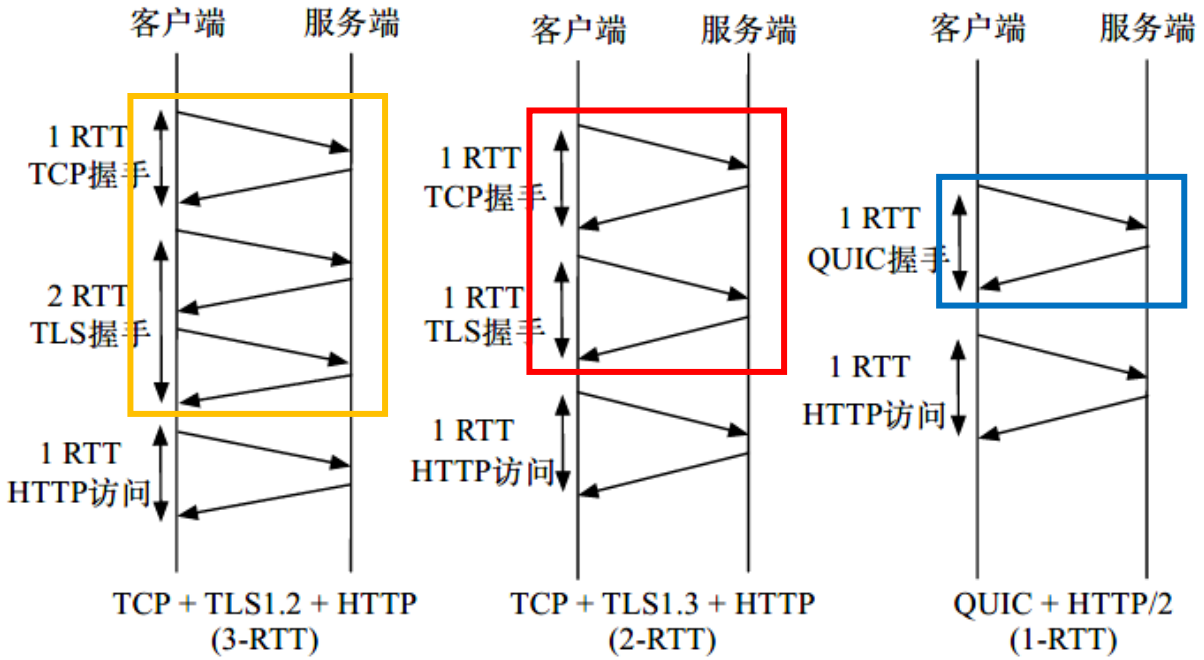


图 3　不同协议握手延时的对比

协议特性

- 握手协议
  - QUIC 设计了自己的握手协议，达到了更低的握手延时，显著减少用户访问网络的延迟感，提升用户体验

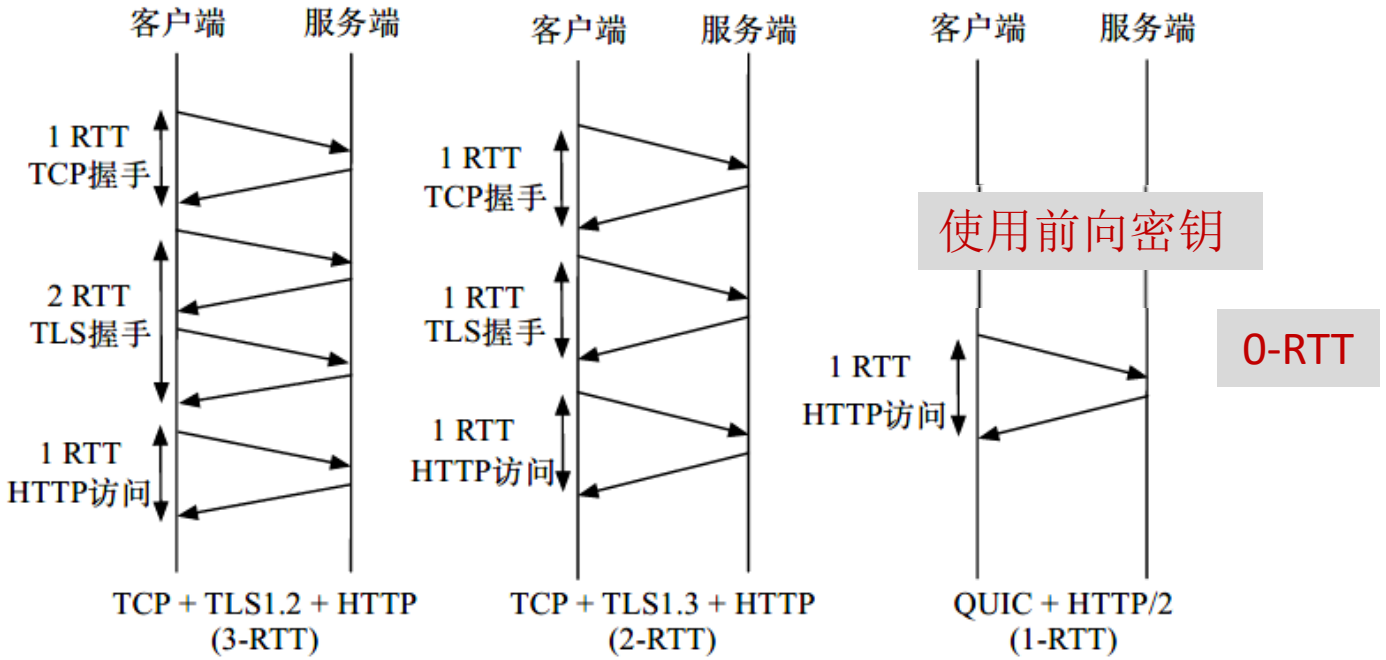


图 3　不同协议握手延时的对比

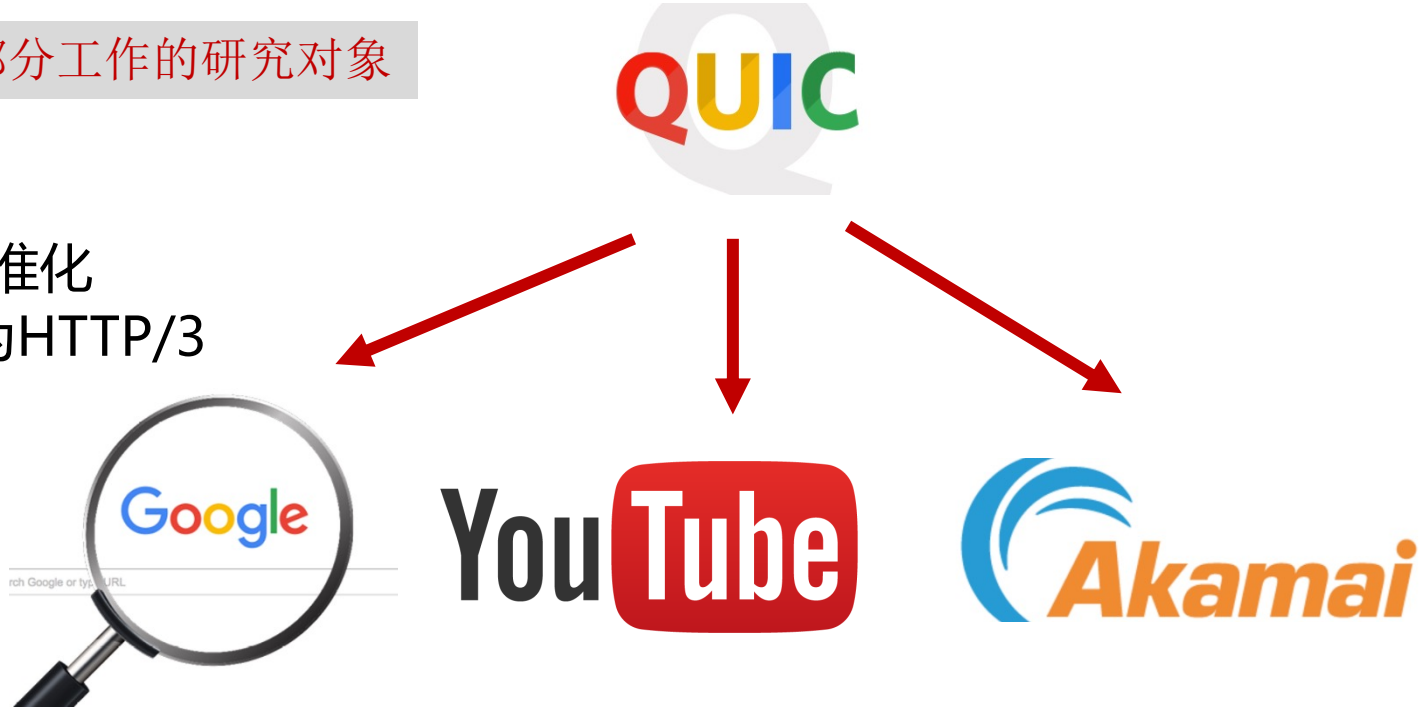
发展历史

- 2种版本：
  - gQUIC
    - Google开发
  - QUIC
    - 2015年6月： 由IETF进行标准化
    - 2018年10月: 认可QUIC成为HTTP/3

发展历史

- 2种版本：
  - gQUIC
    - Google开发
  - QUIC
    - 2015年6月： 由IETF进行标准化
    - 2018年10月: 认可QUIC成为HTTP/3

目前大部分工作的研究对象



研究现状分析

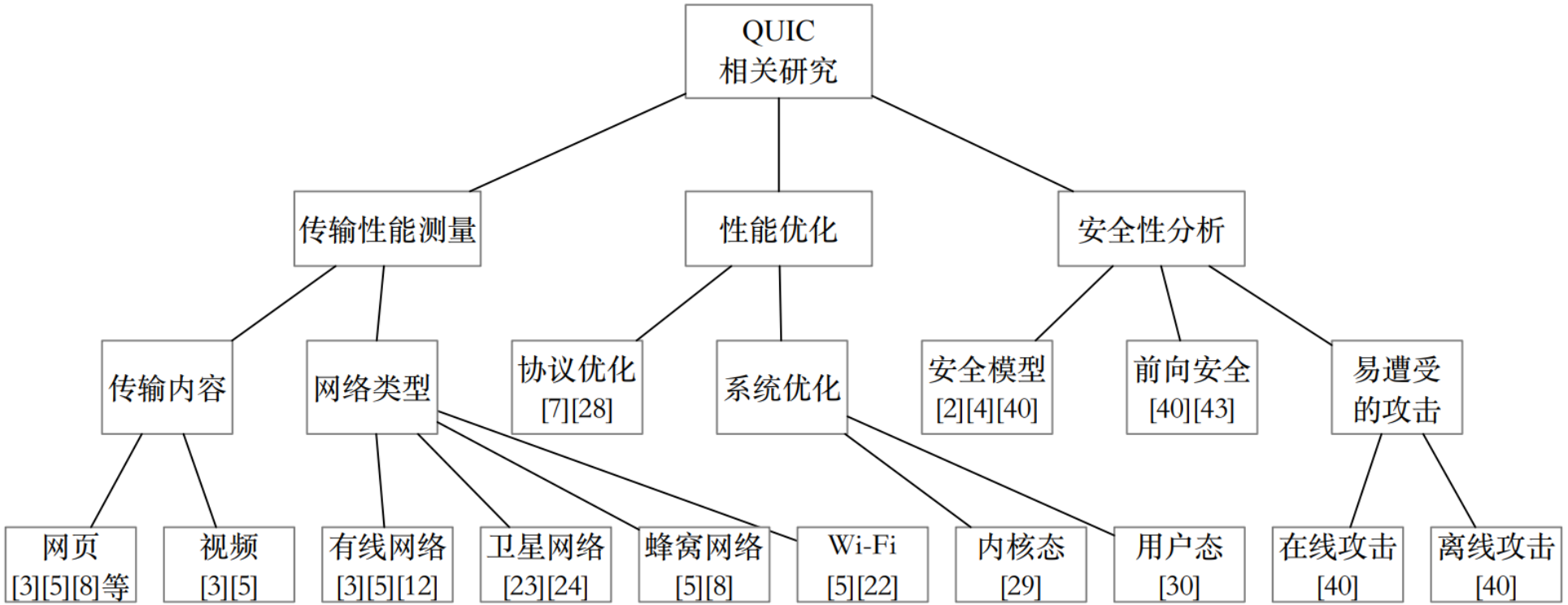
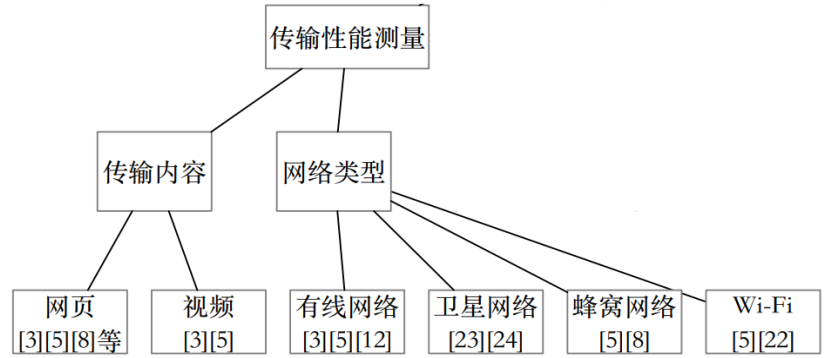


图 4　QUIC 相关工作的分类

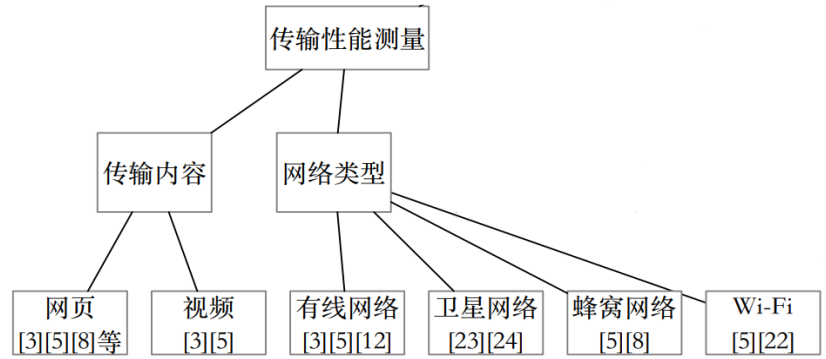
传输性能测量



作者	发表处	发表年份	应用场景	测试环境	网络环境	测试对象	主要结论
Das[12]	MIT thesis	2014年	网页浏览	模拟网络	**有线网络**	带宽，RTT	低带宽时QUIC更快，高带宽时TCP更快
Kharat 等学者[22]	ICCSP	2018年	网页浏览	模拟网络	**Wi-Fi网络**	带宽	在只有一条连接时，QUIC能够比TCP抢占更多的带宽；但有2条即以上连接时，则相反
Yang 等学者[23]	IWCMC	2018年	网页浏览	模拟网络	**卫星网络**	丢包率	QUIC在高延时的卫星网络下表现得比TCP更好

表1 QUIC性能分析的相关工作

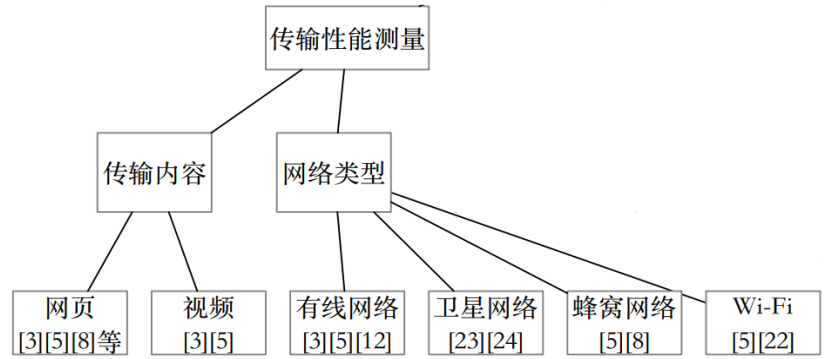
传输性能测量



作者	发表处	发表年份	应用场景	测试环境	网络环境	测试对象	主要结论
Das[12]	MIT thesis	2014年	网页浏览	模拟网络	有线网络	带宽，RTT	低带宽时QUIC更快，高带宽时TCP更快
Kharat 等学者[22]	ICCSP	2018年	网页浏览	模拟网络	Wi-Fi网络	带宽	在只有一条连接时，QUIC能够比TCP抢占更多的带宽；但有2条即以上连接时，则相反
Yang 等学者[23]	IWCMC	2018年	网页浏览	模拟网络	卫星网络	丢包率	QUIC在高延时的卫星网络下表现得比TCP更好
Rajiullah 等学者 [8]	WWW	2019年	网页浏览	**真实网络**	蜂窝网络	加载时间	支持QUIC的网站在引用其他不支持QUIC的网站是需要回滚到TCP，带来额外延时，并最终慢于TCP

表1 QUIC性能分析的相关工作

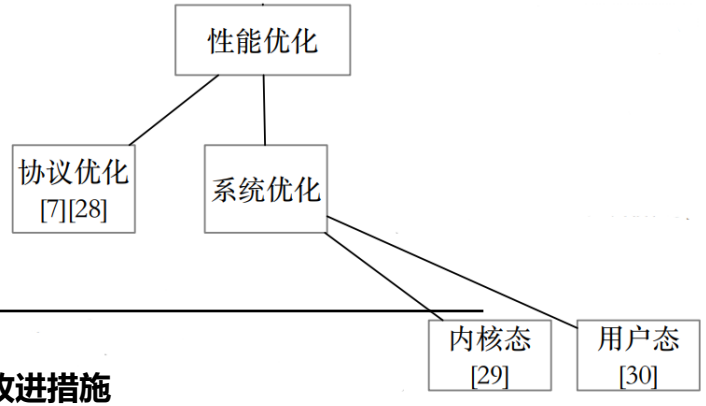
传输性能测量



作者	发表处	发表年份	应用场景	测试环境	网络环境	测试对象	主要结论
Das[12]	MIT thesis	2014年	网页浏览	模拟网络	有线网络	带宽，RTT	低带宽时QUIC更快，高带宽时TCP更快
Kharat 等学者[22]	ICCSP	2018年	网页浏览	模拟网络	Wi-Fi网络	带宽	在只有一条连接时，QUIC能够比TCP抢占更多的带宽；但有2条即以上连接时，则相反
Yang 等学者[23]	IWCMC	2018年	网页浏览	模拟网络	卫星网络	丢包率	QUIC在高延时的卫星网络下表现得比TCP更好
Rajiullah 等学者 [8]	WWW	2019年	网页浏览	真实网络	蜂窝网络	加载时间	支持QUIC的网站在引用其他不支持QUIC的网站是需要回滚到TCP，带来额外延时，并最终慢于TCP
Langley 等学者[5]	SIGCOMM	2017年	**网页浏览，视频传输**	真实网络	蜂窝网络	桌面端和移动端	对视频传输的丢包重传机制大幅度优化视频播放的质量
Kakhki 等学者[3]	IMC	2017年	**网页浏览，视频传输**	模拟网络	有线网络	带宽，延时，丢包率	QUIC过于激进的丢包判断机制导致其在高丢包率网络下性能严重下降

表1 QUIC性能分析的相关工作

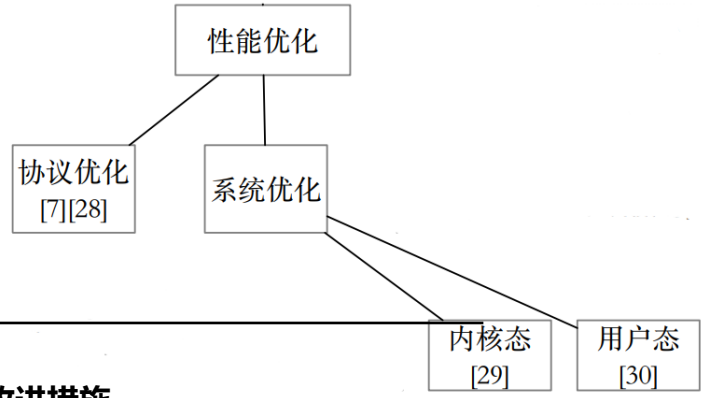
性能优化



	作者	发表处	发表年份	主要改进措施
多路径QUIC	Quentin 等学者[7]	CoNEXT	2017年	MPQUIC:在Stream之下定义了Path，用于描述数据传输所使用的物理网络路径
	Viernickel 等学者[28]	ICC	2018年	通过不同的UDP 套接字直接区分不同的物理网络路径

表2 QUIC性能优化的相关工作

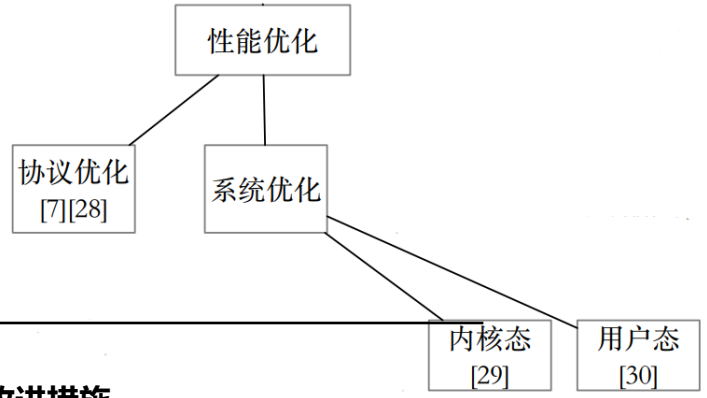
性能优化



	作者	发表处	发表年份	主要改进措施
多路径QUIC	Quentin 等学者[7]	CoNEXT	2017年	MPQUIC:在Stream之下定义了Path，用于描述数据传输所使用的物理网络路径
	Viernickel 等学者[28]	ICC	2018年	通过不同的UDP 套接字直接区分不同的物理网络路径
用户态与内核态	Duan 等学者[30]	KBNets	2017年	在用户空间实现了包括UDP在内的gQUIC协议栈
	Wang 等学者[29]	MSWiM	2018年	在内核空间实现了gQUIC，用于在公平的环境下进行 gQUIC 和 TCP 的性能对比

表2 QUIC性能优化的相关工作

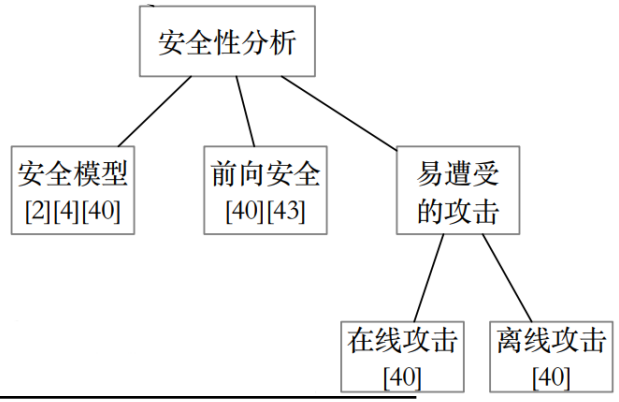
性能优化



	作者	发表处	发表年份	主要改进措施
多路径QUIC	Quentin 等学者[7]	CoNEXT	2017年	MPQUIC:在Stream之下定义了Path，用于描述数据传输所使用的物理网络路径
	Viernickel 等学者[28]	ICC	2018年	通过不同的UDP 套接字直接区分不同的物理网络路径
用户态与内核态	Duan 等学者[30]	KBNets	2017年	在用户空间实现了包括UDP在内的gQUIC协议栈
	Wang 等学者[29]	MSWiM	2018年	在内核空间实现了gQUIC，用于在公平的环境下进行 gQUIC 和 TCP 的性能对比
加速 QUIC 数据包处理的速度:		QUIC 性能的瓶颈在于加密与解密算法的开销		将加密解密相关的操作移到 GPU 上进行执行,从而降低 CPU 负载并加速数据包的处理

表2 QUIC性能优化的相关工作

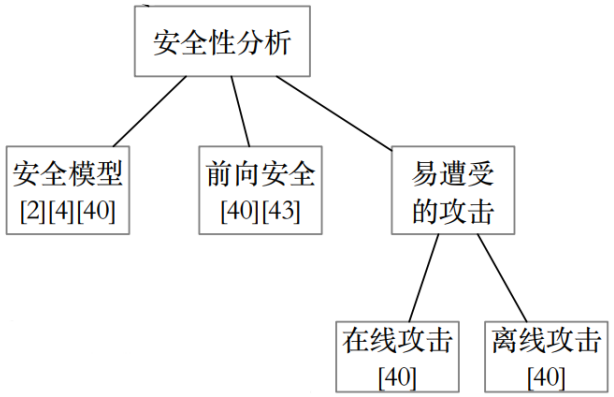
安全性



	作者	发表处	发表年份	主要内容
安全模型	Fischlin 等学者[2]	CCS	2014年	QUICi：采用了更为复杂的密钥生成机制
	Lychev 等学者[40]	IEEE S&P	2015年	提出了快速通信协议的概念，用于描述在最终会话密钥生成之前先使用初始会话密钥的做法
	Jager 等学者[4]	CCS	2015年	模拟攻击结果表明，TLS1.3和QUIC通过增加Bleichenbacher攻击所消耗的时间来消解此攻击

表3 QUIC安全性的相关工作

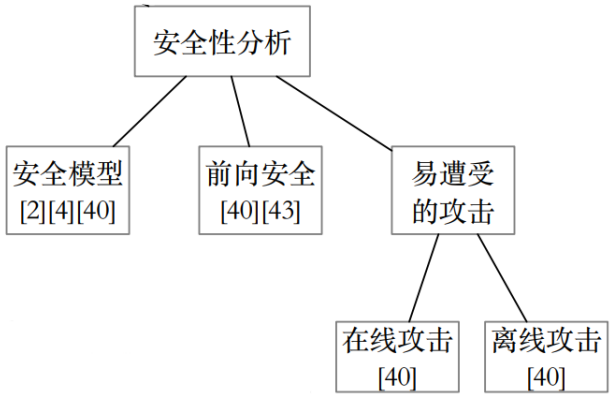
安全性



	作者	发表处	发表年份	主要内容
安全模型	Fischlin 等学者[2]	CCS	2014年	QUICi：采用了更为复杂的密钥生成机制
	Lychev 等学者[40]	IEEE S&P	2015年	提出了快速通信协议的概念，用于描述在最终会话密钥生成之前先使用初始会话密钥的做法
	Jager 等学者[4]	CCS	2015年	模拟攻击结果表明，TLS1.3和QUIC通过增加Bleichenbacher攻击所消耗的时间来消解此攻击
前向安全	Gunther 等学者[43]	PLDI	2016年	一次性密钥和不可多次解析密文的密钥设计

表3 QUIC安全性的相关工作

安全性



	作者	发表处	发表年份	主要内容
安全模型	Fischlin 等学者[2]	CCS	2014年	QUICi：采用了更为复杂的密钥生成机制
	Lychev 等学者[40]	IEEE S&P	2015年	提出了快速通信协议的概念，用于描述在最终会话密钥生成之前先使用初始会话密钥的做法
	Jager 等学者[4]	CCS	2015年	模拟攻击结果表明，TLS1.3和QUIC通过增加Bleichenbacher攻击所消耗的时间来消解此攻击
前向安全	Gunther 等学者[43]	PLDI	2016年	一次性密钥和不可多次解析密文的密钥设计
离线攻击	Lychev 等学者[40]	IEEE S&P	2015年	Server Config重复攻击，Crypto Stream Offset攻击
在线攻击	Lychev 等学者[40]	IEEE S&P	2015年	连接ID篡改攻击，Source-Address Token篡改攻击

表3 QUIC安全性的相关工作

目前工作的局限性

- 缺乏对IETF 版本QUIC的分析
- 软件实现对分析结果的影响过大
  - 大多局限于特定的实现
  - 普遍根据测量结果猜测造成差异的原因，没有进行严格的对比
- CPU成为QUIC的性能瓶颈
  - TLS1.3达到了更高的安全性。但是随之而来的是加密解密复杂度的提高以及CPU负载的增加

未来研究方向

- **传输性能测量**：
  - 提高QUIC算法选择灵活性
- **性能优化:**
  - 提高QUIC的系统性能和降低数据包处理的延时
  - 内核旁路、GPU、CPU并行
- **安全性**：
  - 平衡安全性与计算开销
  - QUIC连接容易攻击者所中断

总结

- 本文从传输性能测量、性能优化、安全性分析对现有的QUIC的研究进行了总结分析
- 本文对现有研究成果可能的进一步提高之处进行了总结，并对QUIC带来的新的研究课题及其挑战进行了展望

Q & A

Thank you!