CSN-341 PROJECT REPORT

TEAM MEMBERS

Name	Enrollment No	Email ID	Contribution
Sutirtha Ghosh	21324025	s_ghosh@cs.iitr.ac.in	QUIC
Sachin Jangid	21114086	s_jangid@cs.iitr.ac.in	DoT
Alhan Charan Beshra	21114011	a_cbeshra@cs.iitr.ac.in	SCTP
Shambhoolal Narwaria	21114095	s_narwaria@cs.iitr.ac.in	DoH
Manoj Kumar Sial	21114059	m_ksial@cs.iitr.ac.in	TFO
Ganga Srujan	21114035	g_srujan@cs.iitr.ac.in	TLS 1.3
Abhishek Raj	21114004	a_raj@cs.iitr.ac.in	WebSocket
Ayushka Sahu	21114024	a_sahu@cs.iitr.ac.in	HTTP/3
Chinchole Tushar	21114032	c_traju@cs.iitr.ac.in	BBR

PROBLEM STATEMENT:

In the dynamic realm of web technologies, the advent of emerging network protocols, notably exemplified by the Quick UDP Internet Connections (QUIC) protocol, holds the promise of reshaping web application performance and user experience. This comprehensive problem statement aims to explore the multifaceted challenges and opportunities inherent in analyzing the impact of these innovative protocols.

Web applications have become integral to modern online experiences, serving diverse users across varied devices and network conditions. Traditional protocols, such as Transmission Control Protocol (TCP), exhibit strengths but also limitations. Emerging alternatives like QUIC offer transformative potential, sparking interest in their ability to revolutionize data transmission on the internet.

Understanding the implications of adopting emerging network protocols is crucial for stakeholders ranging from developers to end-users. The analysis is significant as it provides insights into potential benefits and challenges, influencing decisions related to protocol adoption, infrastructure optimization, and user-centric design.

Primary objectives of this research include evaluating how protocols like QUIC enhance web application performance, addressing issues like latency and head-of-line blocking. Robust loss recovery mechanisms and their effectiveness in diverse network conditions are crucial considerations. The impact on the user experience, encompassing perceived speed and overall satisfaction, is a central focus. Additionally, the ability of protocols to facilitate seamless connection migration between different networks is examined, as is their standardization and compatibility with existing infrastructure.

The research methodology employs empirical studies, performance benchmarking, user surveys, and real-world simulations, covering diverse scenarios. Anticipated outcomes extend beyond theoretical insights, aiming to provide practical information for web development, network optimization, and user experience design. The goal is to contribute to best practices for implementing emerging network protocols in diverse web environments, shaping a digital landscape that is both efficient and user-centric in the ever-evolving digital era.

QUIC

QUIC, or Quick UDP Internet Connections, is an experimental network protocol created by Google to minimize latency compared to TCP.

- LOW LATENCY: QUIC reduces latency for new connections to recently visited sites by eliminating head-of-line blocking in TLS and TCP.
- ENCRYPTION TRANSPORT: Encryption and privacy are fundamental to QUIC, connections are protected from tampering and disruption, and most of the headers of the headers not visible to third parties.
- CONNECTION MIGRATION: QUIC addresses the "parking lot" issue through 18-byte connection IDs, enhancing loss recovery for connections in poor network conditions.

DoT(DNS over TLS)

DNS over TLS (DoT) encrypts DNS queries and responses using TLS, boosting user privacy and security by preventing eavesdropping. It operates on port 853, requiring support from both DNS clients and servers. Many popular web browsers, operating systems, and DNS services now embrace DoT for enhanced privacy and security.

BENEFITS:

- Encryption of DNS traffic
- Securing sensitive information
- Mitigating DNS spoofing and preventing DNS tampering
- Standardization and Interoperability

SCTP(Stream Control Transmission Protocol)

New applications are avoiding TCP due to issues like delays from head-of-line blocking, extra overhead in handling continuous data streams, and vulnerability to denial-of-service attacks like SYN attacks.

DoH(DNS over TLS)

DNS over HTTPS (DoH) encrypts DNS resolution using HTTPS, improving user privacy by concealing accessed websites from network observers, including ISPs.

IMPACT ON USER EXPERIENCE:

- Privacy and Security
- Control Over Online Experiences
- Minimal Impact on Web Browsing

TFO(TCP Fast Open)

TCP Fast Open (TFO) is a protocol extension that enables faster establishment of TCP connections by allowing data to be exchanged during the initial handshake, reducing latency in the communication process.

TLS 1.3

TLS 1.3 is the latest version of the Transport Layer Security (TLS) protocol, enhancing security and performance in communication over the internet by minimizing handshake complexity and improving encryption algorithms.

WebSocket Protocol

WebSocket is a communication protocol that provides full-duplex communication channels over a single, long-lived connection, allowing for real-time data exchange between a client and a server in web applications.

HTTP/3

HTTP/3 is an application layer protocol that utilizes the QUIC transfer protocol over UDP. It retains the familiar request-response model, status codes, and reliance on URLs seen in previous HTTP versions. Notably, HTTP/3 offers backward compatibility for a seamless transition in existing web infrastructure and introduces multiplexing to facilitate concurrent data transfers.

BBR

BBR is a congestion control algorithm by Google that enhances TCP performance. It optimizes data transmission by dynamically adjusting the sending rate based on the characteristics of the network, aiming for high throughput and low latency. This is particularly beneficial for improving network performance in activities like web browsing and file transfers.

DRAP (A Proposed Protocol)

DRAP optimizes network performance through dynamic resource allocation, employing a specialized header for priority and efficient data transmission. It uses decentralized decision-making, adaptive algorithms, and security features like encryption. DRAP allows customization through QoS negotiation, includes congestion detection, and aims to balance adaptability and efficiency for enhanced network performance.