Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

QUICUP: Secure User Plane Tunneling for Cellular Networks

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann
Communication Networks Lab, Technical University of Darmstadt
{firstname.lastname}@tu-darmstadt.de

***Abstract*—Integrating new services and applications like edge computing in current and future generations of cellular networks leads to new challenges regarding the security and privacy of user plane traffic. The GPRS Tunneling Protocol in the user plane (GTP-U) was first introduced within 2G networks and is still used in 5G and beyond cellular networks. This protocol lacks integrated security mechanisms such as tunnel endpoint authentication or integrity validation of encapsulated user data and depends on deployment of IPSec and implementation-specific validation procedures to attain baseline security guarantees. Furthermore, GTP-U provides limited extensibility, hindering advanced transport layer optimizations necessary for modern network demands.**

In this paper, we propose QUICUP, a novel tunneling solution for GTP-U traffic based on QUIC. QUIC enhances web communication through integrated application-layer encryption which enables strong binding to user sessions and significantly reduces the attack surface on shared network infrastructure.

Our research presents a mapping between GTP-U and QUICUP, and the prototypical implementation within a 5G core network demonstrates QUIC's capability to effectively replace GTP-U as a tunneling protocol in mobile networks. Ultimately, the proposed transition aligns with ongoing industry movements toward protocol modernization and to better accommodate security and privacy within mobile networks.

***Index Terms*—Connection Authentication, UP Authenticity, QUIC, 6G, GTP-U**

I. Introduction

In 2024, the FBI actively promoted end-to-end encryption when using mobile networks after it became known that attackers were exploiting lawful interception interfaces to spy on data traffic [1]. It is well established that the requirements for lawful interception knowingly create a backdoor. While traffic between User Equipment (UE) and Next generation Node B (gNB) is encrypted, the protocol used in the user plane between gNB and core network for (de-)multiplexing, i.e., GPRS Tunneling Protocol – User Plane (GTP-U), offers no authentication or encryption. Instead, this protocol should only be used in secure private networks to prevent direct attacks on GTP-U. Providers shift the responsibility to users by expecting user traffic to be end-to-end encrypted. Against this backdrop, the developments through which more and more members of third parties are being integrated into the infrastructure of Mobile Network Operators (MNOs) appear particularly interesting. Together with the increasing decentralization of mobile networks and the advancing development of new user groups in the industry, e.g., for dedicated campus networks or edge computing applications, other stakeholders besides the network provider are able to gain access to network components of the user plane. Thus, preventing unauthorized access to the user plane is becoming increasingly complex. In addition, virtualization and cloudification of network functions are used to optimize adaptation to the current workload and to dynamic user requirements. Modern protocols are therefore required to adapt dynamically to changing routes, e.g. through connection migration.

Detecting ongoing attacks by an attacker within the infrastructure of third parties is difficult. Preventing such attacks without disrupting valid traffic is even more challenging. The current solution is not suitable because it does not support a fine granular access control to user traffic and an adaptive management of tunnels. Hence, we propose QUICUP, a tunneling protocol based on QUIC for the User Plane (UP) of cellular networks. The contributions in this paper are summarized as follows:

- We present our QUIC based solution for user plane tunnels on N3 and N9 interfaces of 5G only networks.
- We look into existing vulnerabilities of GTP-U and analyze how QUICUP overcomes those threats.
- We discuss the existing protocol GTP-U and show the mapping between GTP-U and QUICUP.

II. User Plane Tunneling in 5G Networks

The 5G network consists of the Next generation Node B (gNB) and the 5G core network, which in turn can consist of more than 30 Virtualized Network Functions (VNFs). Figure 1 shows a simplified representation of the network, in which the User Equipment (UE) connects to the gNB via the air interface. The different network interfaces use a variety of protocols. One important protocol in cellular networks is the GPRS Tunneling Protocol (GTP). GTP comprises three different IP-based protocols, i.e., GTP-C in the control plane, GTP-U in the user plane and GTP' for the transport of charging data. GTP-C is mainly used to manage data associated with user sessions in different network nodes. In 5G networks, GTP-C has been replaced by the Packet Forwarding Control Protocol (PFCP). GTP-U is a simple tunneling protocol to transport user data between network nodes. All three protocols share a common header structure where the respective protocol type is determined by three header fields, i.e., version, protocol type and message type. In this paper, we focus on GTP-U.

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

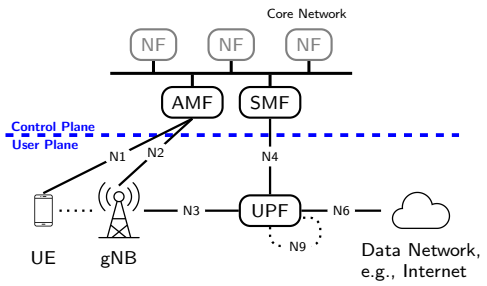


Fig. 1: Overview of the 5G network architecture highlighting the core network components with its network functions (NFs), and the end-to-end data path from the User Equipment (UE) via the gNB and the User Plane Function (UPF) to external networks such as the Internet.

After the successful registration in the core network, the UE requests one or more Protocol Data Unit (PDU) sessions. PDU sessions provide end-to-end connectivity between the UE and the Data Network (DN). Figure 2 depicts the protocol stack of the 5G user plane. Between the UE and the gNB, user traffic is sent over-

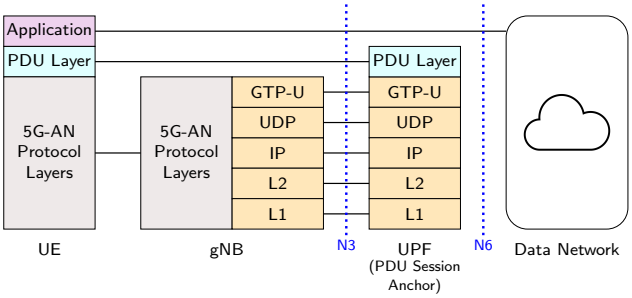
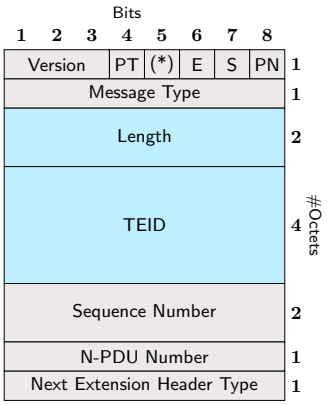


Fig. 2: 5G protocol stack in the user plane.

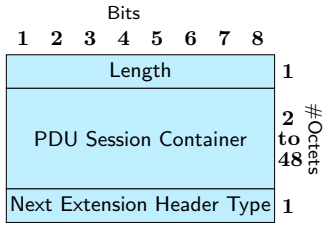
the-air and uses the same path as control plane traffic. On the N3 interface between the gNB and the User Plane Function (UPF) and on the N9 interface between two connected UPFs, each PDU session is associated with a pair of GTP-U tunnels, one tunnel in upstream and one in downstream direction. During session establishment, each receiving tunnel endpoint generates a unique Tunnel Endpoint Identifier (TEID) [2]. These values are then exchanged between the gNB and the core network via control plane protocols. The sending tunnel endpoint encapsulates a packet with a GTP-U header containing the respective TEID and transmits the packet using User Datagram Protocol (UDP) as transport protocol. The receiving tunnel endpoint parses the GTP-U header, removes the outer headers and processes the inner packet. A UPF connected to the DN via the N6 interface acts as PDU Session Anchor (PSA). It terminates the PDU layer between UE and 5G core network and is responsible for the mapping between a PDU session and the allocated IP address/ prefix.

A. Dissecting the GTP-U Header

GTP-U is crucial for maintaining PDU sessions that provide end-to-end connectivity between the UE and the PSA UPF. The



(a) GTP Header



(b) Extension Header: PDU Session Container

Fig. 3: GTP-U Header

GTP header shown in Figure 3a is the common structure for GTP-C, GTP-U and GTP'. Grey fields hold the same values for all GTP-U packets that carry user data and are set as follows: GTP-U is only specified for GTPv1 and thus the `Version` is always set to 1. The next bit specifies the `Protocol Type (PT)`, i.e., either 0 for GTP' or 1 for GTP. `(*)` is a spare bit and is set to 0. The `Extension Header flag (E)` indicates the existence of an extension header. A GTP-U packet that carries user data needs at least one extension header of the type `PDU Session Container` and thus, this flag is set to 1, too. If there are several extension headers, the first extension header is always the `PDU Session Container` and so, the `Next Extension Header Type` is set to `1000 0101`. Also, the `Message Type` is set to `G-PDU` to indicate the presence of a PDU Session Container. The `N-PDU Number` field is optional and its presence is indicated by the `N-PDU Number Flag (PN)`. It is not used in 5G networks and so, `PN` is set to 0. The `Sequence Number` field is optional for G-PDUs. It is used for Inter-RAT Handover scenarios, e.g. a handover from a 5G network to a 4G network. Thus, for our 5G only scenario the corresponding `Sequence Number Flag (S)` is set to 0 and the Sequence Number field itself does not exist. The remaining fields are not fixed. The `Length` field contains the length of the payload in bytes following the mandatory part (first 8 octets) of this header. The `Tunnel Endpoint Identifier (TEID)` is used to identify the PDP context in the receiving tunnel endpoint node.

The extension header starts directly after the GTP Header. The first octet is the `Length` of the extension header. It is followed by the extension header content with a variable length. The last field consists of the `Next Extension Header Type`. An extension header of the type `PDU Session Container` is shown in Figure 3b. The content of this container is either a `Downlink PDU Session Information (PDU Type 0)` frame or an `Uplink PDU Session Information (PDU Type 1)` [3]. Both container types are used to transmit PDU session information, for example the QoS Flow Identifier

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

(QFI) or different time stamps for monitoring purposes. If there is no further extension header, this header is then followed by the user payload.

B. Security Mechanisms for GTP-U Traffic

The security architecture for the control plane of cellular networks is based on the assumption that every part of the network belongs to a security domain and every security domain belongs to a single network provider [4]. It is explicitely stated that only GTP-C traffic needs to be protected by IPSec and that user traffic itself should be end-to-end encrypted, i.e., between the user device and the destination in a data network. Nevertheless, another 3GPP document [5] states explicitely that IPSec is mandatory for GTP-U over the the N3 interface while providers are allowed to use security gateways to terminate IPSec tunnels on the side of the core network. In addition, there are also recommendations from IETF, ITU and GSMA for the usage of security mechanisms like IPSec or Transport Layer Security (TLS) in the user plane to protect user traffic [6], [7].

IPSec policies can be used to decide which traffic should be encrypted, bypassed without encryption, or blocked. IPSec is located at the network layer and policies defined in the Security Policy Database (SPD) are based on source and destination IPs, protocols, and ports. When an IPsec policy permits the transmission of GTP-U packets between a source and destination host, it typically does not enforce additional safeguards against protocol-specific attacks targeting GTP-U. This limitation becomes increasingly significant in the context of decentralized cellular core networks and the deployment of edge services, where the proliferation of distributed endpoints broadens the potential attack surface. To mitigate these risks, specialized GTP firewalls are employed to restrict unauthorized access and defend against a wide range of threats across all GTP protocol variants, including GTP-U. These firewalls frequently leverage Deep Packet Inspection (DPI) techniques to detect malicious traffic patterns, protocol anomalies, and non-compliant GTP messages.

III. Related Work

Over the years, numerous proposals have emerged to replace GPRS Tunneling Protocol – User Plane (GTP-U) with alternative tunneling protocols, addressing security risks that GTP-U was not originally designed to mitigate. In the following, we present alternative tunneling protocols along with a selection of identified attacks targeting GTP-U.

A. Alternative Tunneling Protocols

In 2019, 3GPP finished a case study to determine if Segment Routing with IPv6 (SRv6) could be used to replace GTP-U in the user plane of 5G networks [8]. The main incentive was to enable advanced routing on the N9 interface between User Plane Functions (UPFs) and to enhance network slicing in the transport network. Since the responsible workgroup decided to not standardize the usage of SRv6 without GTP-U in the user plane of mobile networks, related work focuses on the coexistence and efficient transitions between the two protocols [9]–[11].

Gebert and Wich compared several protocols in the context of industrial 5G networks for real time applications [12]. They compare two Ethernet based alternatives to two IP based user plane protocols and based on the special requirements for deterministic traffic, they recommend the usage of Provider Backbone Bridging instead of GTP-U for industrial settings.

Multiplexed Application Substrate over QUIC Encryption (MASQUE) [13] is a protocol framework developed by the IETF to enhance internet communication by enabling the tunneling of various network traffic types, such as UDP, IP, and even QUIC itself, through HTTP/3 connections over QUIC. MASQUE builds upon the established HTTP CONNECT method, traditionally used for proxy support when supported by servers, and significantly expands its capabilities through CONNECT-IP and CONNECT-UDP extensions. These extensions facilitate proxying of unreliable traffic, such as UDP datagrams or raw IP packets. Central to MASQUE's capabilities is the use of HTTP datagrams [14], enabling the transmission of unreliable data within HTTP/3 connections. However, MASQUE is missing capabilities that GTP-U and QUICUP provide, such as seamless session handover and session continuity.

Wireguard is a VPN protocol, which is designed to transmit IP packets via UDP datagrams [15]. It is integrated in the Linux kernel and has gained popularity as a general-purpose encrypted transmission, due to its simplicity and security. However, as with MASQUE, it lacks features concerning the seamless session handover and session continuity. Additionally, applying WireGuard to GTP-U scenarios, which involve creating overlay connections between Next generation Node B (gNB) and UPF, would still face the same problems that GPT-U has in regards to traffic authenticity, because the wireguard tunnel cannot be tightly bound to a specific Tunnel Endpoint Identifier (TEID).

B. Vulnerabilities in GTP

The GPRS Tunneling Protocol (GTP) was first used within 2G networks. Vulnerabilities and possible attacks on the protocol are known for all network generations [6], [16]–[18]. A distinction can be made between attacks on GPRS Tunneling Protocol – Control Plane (GTP-C) and attacks on GTP-U. Attacks on GTP-C focus on manipulating session control, while attacks on GTP-U concern data transport and user data manipulation. We focus on previous research exploiting vulnerabilities that are possible due to the lack of mechanisms for authentication between GTP endpoints, integrity protection and encryption within the protocol.

1) GTP-in-GTP: A malicious User Equipment (UE) sends a GTP packet to the mobile network. The GTP packet is treated as normal payload and thus, it is encapsulated within a GTP-U packet. If the inner packet is a GTP-C packet, adversaries can execute a range of attacks like scanning for internal network infrastructure, enabling unauthorized allocation, modification, or deletion of PDP session contexts [16]–[20]. These activities may

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

result in resource exhaustion, and disruption of data services for authorized users. Park et al. describe a similar attack targeted on 5G networks in which the inner packet is a Packet Forwarding Control Protocol (PFCP) packet [21]. Salim, a researcher from Trend Micro identified a vulnerability in a 5G core implementation by crafting and sending a malformed GTP-U packet that resulted in a denial of service (DoS) of the UPF 0 [22]. Mitigation strategies involve discarding user traffic identified as GTP or PFCP, and restricting the use of core network protocols exclusively to authenticated and authorized peers.

2) Exposed GTP Endpoints: If a GTP endpoint is exposed to the internet, an attacker can directly send GTP packets from outside the mobile network to this endpoint. The attacker either targets the network infrastructure or relays malicious traffic through the mobile network to connected user devices [16], [17], [19], [20]. In 2023, Trend Micro identified more than 150 000 GTP interfaces exposed to the internet [23]. Identification of GTP endpoints is performed by transmitting GTP Echo Request messages and analyzing the received responses [20]. Endpoint authentication can effectively mitigate scanning activities and prevent subsequent attacks that exploit discovered GTP endpoints.

3) Adversary-in-the-Middle Attacks: Many researchers have only looked at attacks originating from outside the network, i.e., from UEs or servers in the data network. With the rise of verticals like V2X or Industry 4.0 in 5G networks, it is likely that more stakeholders with different policies regarding trust gain access to network infrastructure [24]. This increases the attack surface as a whole. Mahyoub et al. [6] assess existing vulnerabilities of GTP-U on the N3 and N9 interface of 5G networks using the STRIDE model [25]. They state that an attacker with access to network infrastructure may intercept or modify user traffic. This enables an adversary to gain unauthorized access to sensitive user information and may compromise the confidentiality and integrity of communications between the user and the intended recipient. Furthermore, the injection or replay of traffic can result in fraudulent charging, potentially leading to overbilling of users. In 2000, 3GPP proposed for the first time to secure GTP with the help of IPSec [26]. It was emphasized that this would not require any changes to GTP. In 5G networks, several new security measures have been introduced to mitigate GTP vulnerabilities that were already present in 2G, 3G, and 4G networks [5]. For GTP-C, those measures include certificate-based authentication of core network functions and mandatory encryption. In roaming scenarios, the Security Edge Protection Proxy (SEPP) encrypts GTP-C traffic between different operators and ensures message integrity and authentication. In addition, slicing allows the application of specific firewall rules for each slice to enhance the security of GTP. Even when IPsec is employed, a tunnel endpoint may forward GTP-U traffic without being the legitimate anchor for the associated user session. To mitigate this risk, mandatory filtering of GTP-U packets at the UPF is implemented to ensure that only authorized and session-relevant traffic is processed [5].

IV. System Overview

Cooperation of Mobile Network Operators (MNOs) is widely used for commercial and environmental reasons. Commonly known techniques like roaming agreements and shared usage of masts enhance connectivity and availability of network services. To improve network coverage, different MNOs can also share network infrastructure. Additionally, new technologies, such as Multi-Access Edge Computing (MEC) and the increasing virtualization of network functions, mean that other parties besides MNOs also have access to nodes within the 5G network.

We consider a 5G network where besides the responsible MNO multiple other stakeholders have access to network infrastructure as shown in Figure 4. Scenario *(i)* shows a private

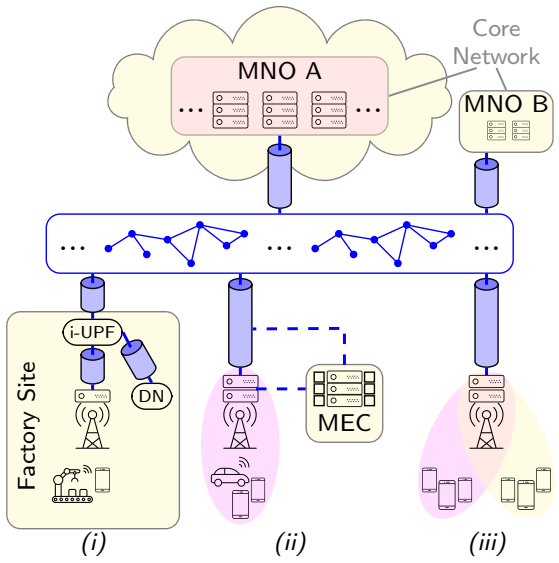
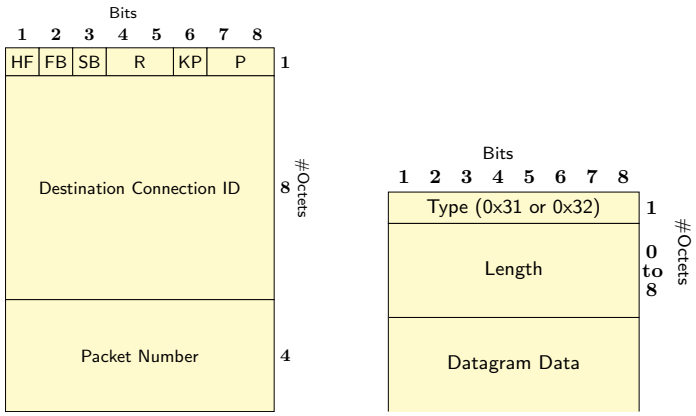


Fig. 4: Overview of the 5G network. Resources from third parties are marked in yellow. Data paths using GTP-U tunnels are marked in blue.

campus network where the Next generation Node B (gNB) is deployed on the factory site. Scenario *(ii)* integrates MEC services from a third party. Those services share the physical connection between the gNB and the User Plane Function (UPF) in the core network. In scenario *(iii)*, several network provider use the same gNB to serve their customers, known as active network sharing [27], [28]. All gNBs are connected to a cloud-native 5G core network running on infrastructure of a cloud service provider. In summary, this means that various stakeholders have access to tunnel endpoints to forward encapsulated user traffic using the transport network between gNBs and the 5G core network. As described in Section II-B, encryption and integrity protection of Data Radio Bearers (DRBs) between User Equipments (UEs) and gNBs is mandatory. Following the guidelines of 3GPP, the user traffic on the N3 and N9 interface is secured by IPSec. The encapsulation of user payload within GPRS Tunneling Protocol – User Plane (GTP-U) headers is functionally decoupled from the subsequent encapsulation and encryption of GTP-U

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.



(a) Short Header. (b) Datagram Frame.

Fig. 5: Structure of the QUIC Header.

packets using IPsec. In deployment scenarios involving multiple stakeholders, the use of IPsec following GTP-U encapsulation may be insufficient to ensure the authenticity, integrity, and confidentiality of user plane traffic. This architectural separation undermines security guarantees in the user plane. Consequently, additional verification mechanisms are required upon reception of a GTP-U packet to confirm that the originating node was authorized to handle and transmit user traffic for the Protocol Data Unit (PDU) session identified by the Tunnel Endpoint Identifier (TEID) in the GTP-U header.

V. QUICUP

We propose QUICUP, a secure tunneling protocol for the user plane of future mobile networks based on QUIC. QUIC is a UDP based transport protocol between two endpoints [29]. QUIC packets are encrypted by default using Transport Layer Security (TLS) 1.3. With QUICUP, we bind the encapsulation procedure to the authentication and encryption of user traffic and thus, we leverage security-by-design in the user plane. Additionally, the protocol supports multiplexing of several streams over one connection and connection migration to a new client IP address which offers the necessary flexibility for user mobility.

A. Dissecting QUIC

In general, QUIC uses two different types of headers: The long header is primarily used during connection establishment, including the exchange of cryptographic and transport handshake messages, as well as version negotiation. The short (see Figure 5a) header is used for 1-RTT packets after the cryptographic keys are set. The first octet of the short header consists of six different flags: `Header Form (HF)`, `Fixed Bit (FB)`, `Spin Bit`, two bits as `Reserved Bits`, `Key Phase` and two bits for `Packet Number Length (P)`. The next field contains the `Destination Connection Identifier (DCID)`. Connection IDs are initially proposed by the client in the INITIAL packet during the handshake. Each connection uses distinct Connection IDs for each endpoint. The server adopts the client's proposed DCID to identify incoming packets, and uses the Source Connection ID when sending responses back on the same connection. Importantly, each endpoint is free to change its own Connection ID at any time during the connection. The `Packet Number` has a variable length of one to four bytes and its length is given in the `P` field.

To minimize the amount of meta data in the packet header, QUIC uses several different frame types to carry information for connection management, e.g., `ACK` frames, `PING` frames or `CONNECTION_CLOSE` frames [29]. QUIC employs session tickets to facilitate 0-RTT and 1-RTT connection resumption, thereby optimizing performance by eliminating the need for full cryptographic handshakes during subsequent connections between the same client and server. The lifetime of session tickets is defined by the server during the initial handshake. Efficient resumption mechanisms contribute to improved recovery from network disruptions and play a critical role in supporting seamless connection migration. The payload of a QUIC packet consists of one or more frames, either control frames or frames that carry application data.

During packet construction, the Authenticated Encryption with Associated Data (AEAD) function processes the packet header as associated data and the payload as input [30]. The function returns the encrypted payload and appends the 16 byte `Authentication Tag`. With the usage of the packet header as associated data, both the payload and the header are integrity-protected. Then, header protection is applied to encrypt the Reserved bits, the Key Phase bit, the Packet Number Length field, and the Packet Number of the short header.

Although originally not designed for this purpose, there are now several approaches that use QUIC for tunneling scenarios, specifically the already mentioned MASQUE (see Section III-A). Those approaches make use of the Datagram extension of QUIC [31]. While the initial tunnel establishment needs to be reliable, the transmission of IP packets through the tunnel needs to be unreliable to avoid problems like the TCP-meltdown problem [32]. With this extension, application data is sent within `Datagram` frames as shown in Figure 5b. Each `Datagram` frame starts with the `Type` field. If the `Len` bit of this field is set, it is then followed by the `Length` field, encoded as variable-length integer, to indicate the length of the datagram data in bytes.

B. Translating GTP-U to QUICUP

In the following, we describe the mapping between GTP-U and QUIC headers. We do not want to replace GTP-C and GTP' and thus, we do not need to map those header fields that are meant to discriminate between different GTP protocols like Version or Protocol Type as described in Section II-A. Instead, we aim to provide the functionality of the GTP-U protocol but with enhanced security as we bind encryption and authentication to the application that encapsulates user traffic. QUICUP uses individual QUIC connections with mutual authentication for each PDU session. The provisioning and

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

GTP-U Message Type	Usage	QUIC
Echo Request Echo Response	Keep alive, verification of reachability	PING Frame ACK Frame
Supported Ext. Headers Notification	Answer to an unsupported but mandatory Ext. Header	Version negotiation during connection setup
Error Indication	Endpoint received a valid G-PDU but has no matching PDU session: a) Error: PDU session was lost b) Attack: Spoofing attempt Both cases must be handled by the control plane.	Valid packets carrying user traffic belong to active connections: a) Error: PDU session was lost b) – Restoration of the PDU session must be handled by the control plane.
Tunnel Status (optional)	Status information related to a GTP-U tunnel	Negotiation during connection setup, various frame types for signalling
End Marker	End of the payload stream on a given tunnel	CONNECTION_CLOSE Frame
G-PDU	Payload	DATAGRAM Frame

TABLE I: Mapping from GTP-U message types to QUIC frames or procedures.

management of X.509 certificates and associated private keys for both client and server entities are orchestrated by the control plane. The specific operational procedures governing this process fall outside the scope of this work. Figure 6 shows the overhead that is induced by the usage of GTP-U in combination with IPSec in tunnel mode. Thus, the TEID (32 bit) of GTP-U is mapped to the DCID (up to 64 bit) of QUICUP. As described in Section II, GTP-U exchanges TEIDs using the control plane and afterwards, tunnel endpoints can directly transmit user traffic without additional handshake procedures. Using QUICUP, it is still possible to use existing methods to assign DCIDs and link them to established user sessions. For connection setup, QUICUP uses the QUIC handshake. User traffic is directly encapsulated in datagram frames. QUIC encrypts the entire payload of its packets using ciphers and keys established during the handshake [30]. Additionally, it applies header protection to specific header fields by sampling the encrypted payload and using that data to encrypt those fields. As a result, an external observer can only see a limited set of information: the QUIC version, the length field, and the Connection ID. Notably, the version and length fields are present only in the long header format, which is primarily used during the initial handshake. The Connection ID is visible to support routing and key selection during packet processing, which is the same reason why the TEID is unencrypted in GPT-U packets. QUIC employs an AEAD scheme that generates a 16-byte authentication tag over the entire packet, ensuring that any tampering with the packet is detectable. If a tunnel endpoint wants to transmit monitoring data, it can use a datagram frame or even communicate via reliable streams, depending on their reliability requirements.

A comparison of GTP-U with IPSec and QUICUP is shown in Table II. Both protocols may use the same ciphers but QUIC leverages TLS 1.3 for key exchange and encryption, whereas IPsec uses ESP with IKEv2. QUICUP reduces the header overhead user plane packets and incorporates key transport layer features essential for mobile network environments, such as stream multiplexing and support for seamless connection migration.

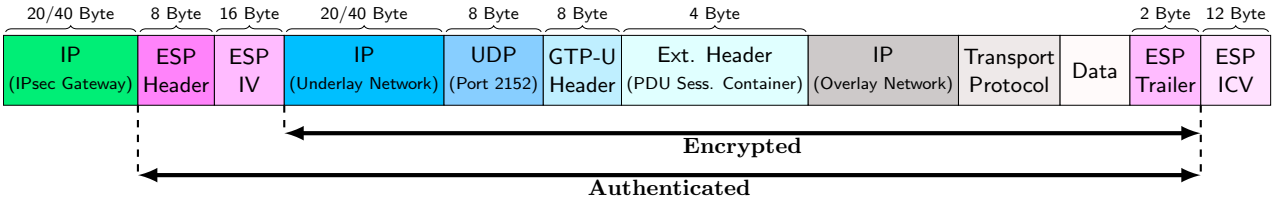
C. Traffic Flow Confidentiality with QUICUP

Traffic analysis attacks are used to reveal patterns and metadata even from encrypted traffic. Various techniques exist to obfuscate traffic patterns, with some approaches tailored to specific types of network traffic, such as those associated with IoT devices [36]. IPSec uses the `Next Header` field to specify the type of the inner packet. The information in this field is confidential and thus, it is part of the encrypted ESP trailer. Also, IPSec provides optional Traffic Flow Confidentiality (TFC) padding to obscure the size of the payload.

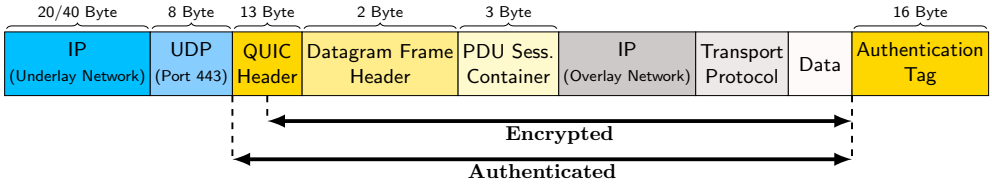
QUIC exposes the DCID field in the packet header to enable correct routing and packet processing, which at first glance may appear to make connection tracking trivial. However, as previously mentioned, QUIC allows each endpoint to change its own Connection ID during the lifetime of a connection. Such updates are securely communicated to the peer within the encrypted payload using `NEW_CONNECTION_ID` and `RETIRE_CONNECTION_ID` frames. As a result, these transitions between Connection IDs are not observable to external parties. So even though the DCID is exposed in the header, its ability for rotation and unlinkability reduce the effectiveness of long-term tracking.

To limit traffic analysis based on the size of the sent packets, `Padding` [29] frames or dummy packets might alleviate issues, however their impact might be limited [37], [38]. In addition to the usage of `Padding` frames, we propose to multiplex user data from different users over one QUICUP tunnel to reveal characteristics of individual user floe. Hence, in this case, we need an additional identifier to differentiate between datagram frames from different users sent in one QUICUP packet. This identifier is then part of the `Datagram Data` field as suggested in [31]. The tunnel endpoints are responsible to assign several user flows to one QUICUP connection in a way that fits to the existing traffic patterns of these user flows. Exact procedures and necessary traffic analysis and scheduling for the optimal placement of user flows in QUICUP connections is outside the scope of this paper.

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.



(a) Tunneling with GTP-U and IPSec in Tunnel mode results in a minimal overhead of 98 Byte for IPv4 and 138 Byte for IPv6 traffic.



(b) Tunneling with QUICUP results in a minimal overhead of 62 Byte for IPv4 and 82 Byte for IPv6 traffic.

Fig. 6: Tunneling overhead comparison.

	GTP-U + IPSec (Tunnel Mode)	**QUICUP**
OSI Layer	Network Layer (Layer 3)	Transport Layer (Layer 4)
Encryption Protocol	Encapsulating Security Payload (ESP)	TLS 1.3
Encryption Algorithms	AES-CBC, AES-GCM, ChaCha20-Poly1305	AES-GCM, ChaCha20-Poly1305
Authentication	IKEv2 certificates-based	TLS 1.3 mutual authentication
Connection Establishment	IKE negotiation	TLS handshake; 0-RTT and fast connection reuse
Multiplexing Support	No	Yes
Header Overhead	IPv4: 98 Byte, IPv6: 138 Byte	IPv4: 62 Byte, IPv6: 82 Byte
Mobility / Connection Migration	Limited: IP address is tied to the IPSec tunnel	Support for connection migration and NAT rebinding
Protocol Standard	RFC 4301 [33], RFC 7296 (IKEv2) [34], RFC 4303 (ESP) [35]	RFC 9000 (QUIC) [29], RFC 9001 (TLS over QUIC) [30], RFC 9221 (QUIC Datagram Ext.) [31]

TABLE II: Comparison of GTP-U with IPSec and QUICUP.

D. Revisiting GTP Vulnerabilities

In light of the vulnerabilities associated with GTP, we evaluate the behavior of QUICUP under analogous threat scenarios. In accordance with the system architecture outlined in Section IV, legitimate tunnel endpoints establish distinct QUIC connections for each PDU session, authenticated through pre-configured certificates. The TLS session secrets associated with a specific QUICUP connection are exclusively shared between the two authenticated endpoints, ensuring that no other QUICUP nodes can intercept or inject valid QUIC packets into the session. This cryptographic isolation mitigates the vulnerabilities inherent to GTP, as outlined in Section III-B.

1) GTP-in-GTP: QUICUP connections are exclusively established between a gNB and a UPF, or between two UPFs. A malicious UE does not possess the necessary TLS session secrets and is therefore incapable of generating valid QUIC packets that would be accepted by a QUICUP node, such as a UPF.

2) Exposed GTP Endpoints: In the event of a misconfiguration, a QUICUP endpoint may become exposed to the public Internet. An adversary lacking the pre-configured client certificate is unable to complete the mutual TLS authentication, resulting in a failed handshake. Furthermore, QUIC packets employing a short header, e.g. when the attacker uses a spoofed DCID, are silently discarded by the QUICUP endpoint, in accordance with QUIC's security model designed to mitigate amplification and resource exhaustion attacks.

3) Adversary-in-the-Middle Attacks: An adversary with access to the network infrastructure must also possess the corresponding TLS session secrets to successfully intercept or modify QUICUP traffic. Provided that these cryptographic secrets remain protected from unauthorized disclosure, the adversary is effectively prevented from performing such actions. The establishment of a QUICUP connection ensures mutual authorization of the communicating entities to handle user traffic associated with a specific PDU session, as identified by the DCID. Consequently, UPFs are not required to independently verify whether the sender is authorized to process traffic for the corresponding user session.

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

VI. Proof of Concept

We demonstrate the feasability of QUICUP by integrating a QUIC based user plane into an end-to-end 5G testbed, see Figure 7. The virtual machines (VMs) were deployed on a

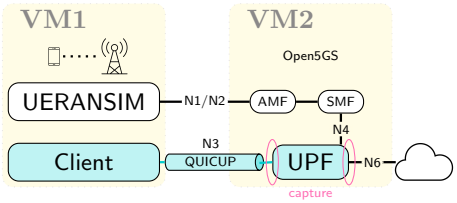


Fig. 7: Testbed setup with QUICUP user plane.

hypervisor operating on an Intel Xeon Gold 6248R processor. Each VM was configured with 16 CPUs and 16 GB of RAM, and both instances ran Ubuntu 22.04.5 LTS with the Linux kernel version 5.15.0-136-generic. We modified the UPF of the Open5GS 5G core implementation (v2.7.2) [39] running on VM2 and included a simple QUIC server based on the MsQuic API (v2.4.8) [40]. UERANSIM (v3.2.7) [41], an open source simulator for 5G UE and gNBs, running on VM1 establishes the control plane connection with the core. The QUICUP client application acts as gNB tunnel endpoint and connects to the UPF. The corresponding TLS secrets are exported to enable the decryption of captured packets for subsequent analysis. After the successful handshake, the client encapsulates packets within datagram frames and sends them to the UPF. In our experiments, the QUIC packets carrying the datagram frame also include padding frames. The UPF decrypts received QUIC packets and extracts the inner packets. Then, these packets are forwarded to the destination. This procedure is illustrated in Figure 8, in which the encapsulated inner packet is an ICMP message. We

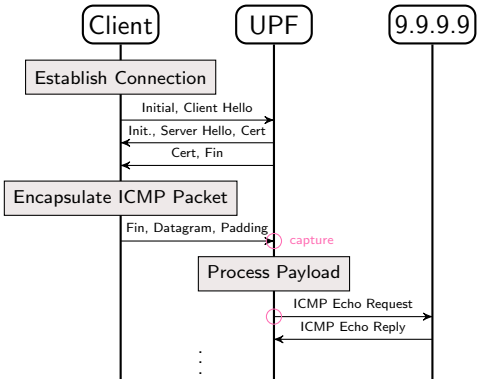


Fig. 8: Experiment setup to determine the UPF latency with QUICUP.

capture ingoing traffic at the N3 interface and outgoing traffic at the N6 interface to determine the processing time of the modified UPF. We compare this processing time, i.e. the latency of the QUICUP based UPF, with the latency of the unmodified GTP-U based UPF without IPSec, see Figure 9. The median processing latency observed for QUICUP is $364.72\mu s$, compared

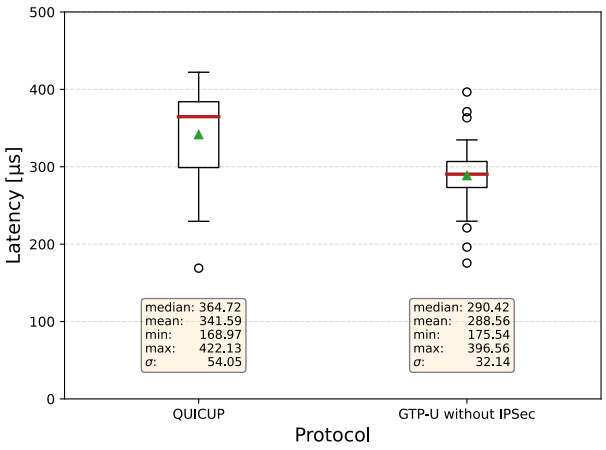


Fig. 9: Relation between protocol type and UPF latency.

to $290.42\mu s$ for the GTP-U-based UPF. The broader interquartile and total whisker ranges associated with QUICUP indicate increased latency variability relative to GTP-U. Nonetheless, both protocols demonstrate similar latency magnitudes, despite the absence of performance optimizations in the QUICUP prototype. Given that the integration of IPsec typically introduces additional transmission overhead, the proposed approach remains competitive with respect to latency performance.

VII. Conclusion

The integration of heterogeneous stakeholders into beyond 5G mobile network architectures expands the attack surface and introduces new challenges for securing user plane tunneling between gNBs and core network components. To promote the adoption of security-by-design principles, we introduce QUICUP, a QUIC-based tunneling mechanism for the N3 and N9 interfaces. In contrast to the conventional approach of encapsulating GTP-U within IPsec in tunnel mode, QUICUP directly links the authentication to PDU session contexts instead of GTP-U tunnel endpoints. We provide a comprehensive analysis of the mapping between GTP-U and QUICUP, demonstrating that QUICUP effectively mitigates inherent security vulnerabilities of GTP-U. The practicality of the proposed approach is validated through a prototypical implementation deployed in an end-to-end 5G network environment.

Acknowledgement

This work has been co-funded by the German Research Foundation (DFG) within the Collaborative Research Center (CRC) 1053 MAKI. The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the project "Open6GHub" (grant number: 16KISK014).

References

[1] K. Collier. (2024) U.S. officials urge Americans to use encrypted apps amid unprecedented cyberattack. [Online]. Available: https://www.nbcnews.com/tech/security/us-officials-urge-americans-use-encrypted-apps-cyberattack-rcna182694

Lisa Wernet, Sebastian Rust, Silas Gerock, Tobias Meuser, Björn Scheuermann. "QUICUP: Secure User Plane Tunneling for Cellular Networks."
In: *Proceedings of the 50th Annual IEEE Conference on Local Computer Networks (LCN).* 2025, pp. 1–9.

[2] 3GPP, "Universal Mobile Telecommunications System (UMTS); LTE; 5G; General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)," Tech. Spec. (TS) 29.281 version 18.3.0, 2025.

[3] 3GPP, "5G; NG-RAN; PDU session user plane protocol," Tech. Spec. (TS) 38.415 version 18.1.0, 2024.

[4] 3GPP, "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security," Tech. Spec. (TS) 33.210 version 18.1.0, 2024.

[5] 3GPP, "5G; Security architecture and procedures for 5G System," Tech. Spec. TS) 33.501 version 18.9.0, 2025.

[6] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, "Security Analysis of Critical 5G Interfaces," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 4, pp. 2382–2410, 2024.

[7] GSM Association, "5G Security Guide Version 3.0," 2024. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/5g-security-guide-version-3-0/

[8] 3GPP, "Study on User Plane Protocol in 5GC," Tech. Report (TR) 29.892 version 16.0.0, 2019.

[9] C. Lee, K. Ebisawa, H. Kuwata, M. Kohno, and S. Matsushima, "Performance Evaluation of GTP-U and SRv6 Stateless Translation," in *15th International Conference on Network and Service Management (CNSM)*. IEEE, 2019.

[10] M. Gramaglia, V. Sciancalepore, F. J. Fernandez-Maestro, R. Perez, P. Serrano, and A. Banchs, "Experimenting with SRv6: a Tunneling Protocol supporting Network Slicing in 5G and beyond," in *IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2020.

[11] C. Lee, N. Mori, Y. Ohara, T. Murakami, S. Asaba, and S. Matsushima, "The Latency Characteristics of GTP-U and SRv6 Stateless Translation on VPP Software Router," in *IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021.

[12] J. Gebert and A. Wich, "Comparison of Provider Backbone Bridging, TRILL, GRE and GTP-U in 5G for Time Sensitive Industrial Applications," in *IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2018.

[13] T. Pauly, D. Schinazi, A. Chernyakhovsky, M. Kühlewind, and M. Westerlund, "Proxying IP in HTTP," IETF, RFC 9484, 2023.

[14] D. Schinazi and L. Pardue, "HTTP Datagrams and the Capsule Protocol," IETF, RFC 9297, 2022.

[15] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," in *24th Annual Network and Distributed System Security Symposium, NDSS*. The Internet Society, 2017.

[16] C. Xenakis, "Malicious actions against the GPRS technology," *Journal in Computer Virology*, vol. 2, no. 2, pp. 121–133, 2006.

[17] X. Peng, W. Yingyou, Z. Dazhe, and Z. Hong, "GTP Security in 3G Core Network," in *Second International Conference on Networks Security, Wireless Communications and Trusted Computing*. IEEE, 2010, pp. 15–19.

[18] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, "5G Security Threat Assessment in Real Networks," *Sensors*, vol. 21, no. 16, p. 5524, 2021.

[19] G. Murphy and O. Whitehouse, "Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks," 2004.

[20] S. Park, B. Choi, Y. Park, D. Kim, E. Jeong, and K. Yim, *Vestiges of Past Generation: Threats to 5G Core Network*. Springer International Publishing, 2020, pp. 468–480.

[21] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session Management for Security Systems in 5G Standalone Network," *IEEE Access*, vol. 10, pp. 73 421–73 436, 2022.

[22] S. I. Salim, "Attacks on 5G Infrastructure From Users' Devices," 2023, Trend Micro Research.

[23] S. I. Salim, "Outside Looking In: How a Packet Reflection Vulnerability Could Allow Attackers to InfiltrateInternal 5G Networks," 2023, Trend Micro Research. CTOne.

[24] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.

[25] Microsoft. (2022) STRIDE model. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[26] 3GPP, "Protect GTP signalling messages by IPSec," Document for Discussion TSG SA WG3 Security – S3 #14, 2000.

[27] D. Renga, M. Ni, M. A. Marsan, and M. Meo, "Network Sharing to Enable Sustainable Communications in the Era of 5G and Beyond," in *IEEE International Conference on Communications (ICC)*. IEEE, 2024, pp. 2840–2846.

[28] M. Kassis, S. Costanzo, and M. Yassin, "Flexible Multi-Operator RAN Sharing: Experimentation and Validation Using Open Source 4G/5G Prototype," in *Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 205–210.

[29] M. T. J. Iyengar, "QUIC: A UDP-Based Multiplexed and Secure Transport," IETF, RFC 9000, 2021.

[30] M. Thomson and S. Turner, "Using TLS to Secure QUIC," IETF, RFC 9001, 2021.

[31] D. S. T. Pauly, E. Kinnear, "An Unreliable Datagram Extension to QUIC," IETF, RFC 9221, 2022.

[32] O. Honda, H. Ohsaki, M. Imase, M. Ishizuka, and J. Murayama, "Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency," in *Performance, Quality of Service, and Control of Next-Generation Communication and Sensor Networks III*, vol. 6011, International Society for Optics and Photonics. SPIE, 2005.

[33] K. Seo and S. Kent, "Security Architecture for the Internet Protocol," IETF, RFC 4301, 2005.

[34] C. Kaufman, P. E. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)," IETF, RFC 7296, 2014.

[35] S. Kent, "IP Encapsulating Security Payload (ESP)," IETF, RFC 4303, 2005.

[36] I. Hafeez, M. Antikainen, and S. Tarkoma, "Protecting IoT-environments against Traffic Analysis Attacks with Traffic Morphing," in *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019, pp. 196–201.

[37] P. Zhan, L. Wang, and Y. Tang, "Website fingerprinting on early QUIC traffic," *Computer Networks*, vol. 200, pp. 1389–1286, 2021.

[38] S. Siby, L. Barman, C. Wood, M. Fayed, N. Sullivan, and C. Troncoso, "You get PADDING, everybody gets PADDING! You get privacy? Evaluating practical QUIC website fingerprinting protections for the masses," 2022. [Online]. Available: https://arxiv.org/abs/2203.07806

[39] Open5GS, "Open Source implementation for 5G Core and EPC, i.e. the core network of LTE/NR network (Release-17)," 2025. [Online]. Available: https://open5gs.org/

[40] Microsoft, "MsQuic API," 2025. [Online]. Available: https://microsoft.github.io/msquic/msquicdocs/docs/API.html

[41] UERANSIM, "Open source 5G UE and RAN (gNodeB) implementation," 2025. [Online]. Available: https://github.com/aligungr/UERANSIM