December 2021

A Method to Provide Cellular QoS for Tethered Clients

Jayachandran C

Hui Wang

A Method to Provide Cellular QoS for Tethered Clients

Abstract

A host device includes a quality of service (QoS) access control module to establish and manage connections having levels of QoS between tethered devices and a network. The QoS access control module authenticates a tethered device to ensure that the tethered device is authorized to use a connection having the requested QoS, establishes a network route and rules for accessing the connection and establishes a secure connection between the host device and the tethered device. As a result, in some cases, the system prevents erroneous operation due to tethered devices attempting to perform tasks that require a connection having a certain QoS without receiving a network connection having that QoS.

Background

A host device, such as a mobile device or user equipment (UE), may share the host device's network connections with other connected devices, a process called tethering. For example, a UE may provide access to a mobile network to other devices for tasks such as internet browsing, voice calling, text messaging, and streaming. Certain time-sensitive use cases such as real-time calls, text messaging, and streaming, require respective levels of QoS to avoid erroneous operation. Devices with modems, such as host devices, can request certain levels of QoS. However, tethered devices do not have a way to request and receive levels of QoS. Additionally, in many cases, only certain ports within the host device can provide the requested levels of QoS. However, in some cases, applications running on the tethered devices do not have a way to request that a specific port of the host device be used for traffic of the applications. As a result, levels of QoS are difficult to guarantee over a tethered network.

Description

A host device may implement a QoS access control module that establishes and moderates connections having requested QoS parameters. For example, the access control module may control network routes and rules for the connection to the tethered client application or device. Further, the access control module may control several connections in parallel and coordinate the connections with other modules of the host device such that each connection with each tethered device receives a requested QoS.

FIG. 1 below illustrates an example system where tethered devices connect to a network via a host device. In some cases, the tethered devices may connect to the host device directly. In other cases, applications of the tethered devices may connect to the host device. The host device may include a tethering service that implements a QoS access control module. The QoS access control module may authenticate tethered devices or applications running on tethered devices, establish secure connections between the host device and the tethered device, and establish and moderate connections having certain QoS guarantees. In some cases, the QoS access control module communicates messages for authentication, QoS requests and responses, and QoS registrations via the secure connections.

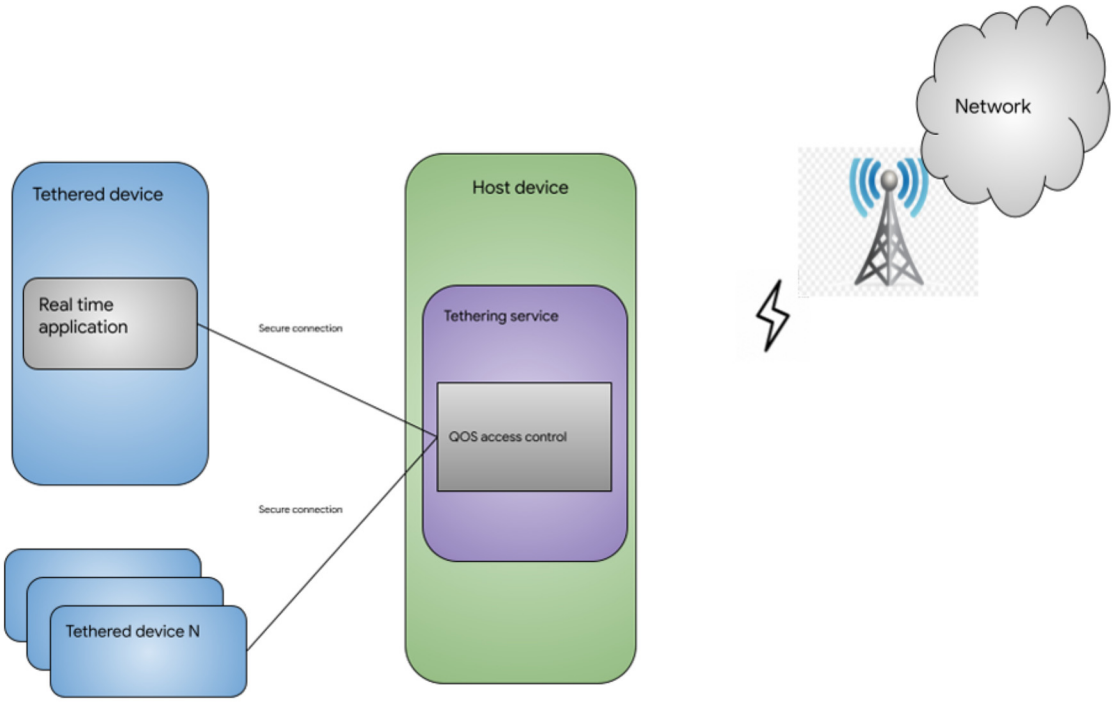

FIG. 1

Turning to FIG. 2, various processes for establishing and moderating QoS connections are depicted. In some cases, as illustrated in both FIGs. 2 and 3 and as further described below with reference to FIG. 3, a tethered device or application requests a respective QoS for a connection to the network. In other cases, the host device assigns a QoS to a connection of a tethered device or application in response to an indication from the network.

In cases where the network requests a connection having a particular QoS, the client application may register for a callback to the host device. In response to the callback, the QoS access control module may check whether the tethered device or application is to be authenticated. If the tethered device or application is to be authenticated, the QoS access control module authenticates the tethered device or application by checking whether the tethered device or application is authorized to use QoS connections using an authentication protocol (e.g., an extensible authentication protocol (EAP)). In some cases, tethered devices may only be authorized to use

connections having certain QoS and thus a requested QoS may be considered as part of the authorization. In response to determining that the tethered device or application is authorized to use the connection, the QoS access control module may establish a network route, coordinate with other modules on the host device to establish rules to control how the tethered device or application accesses the connection, or both. Subsequently, the QoS access control module may cause a secure connection (e.g., a transport layer security (TLS) connection) to be established between the tethered device and the host device. Further, the QoS access control module may cause the host device to establish a connection to the network having the requested QoS properties. As described above, the QoS access control module may communicate with the tethered device or application via the secure connection to notify the tethered device or application of the result of the QoS request.

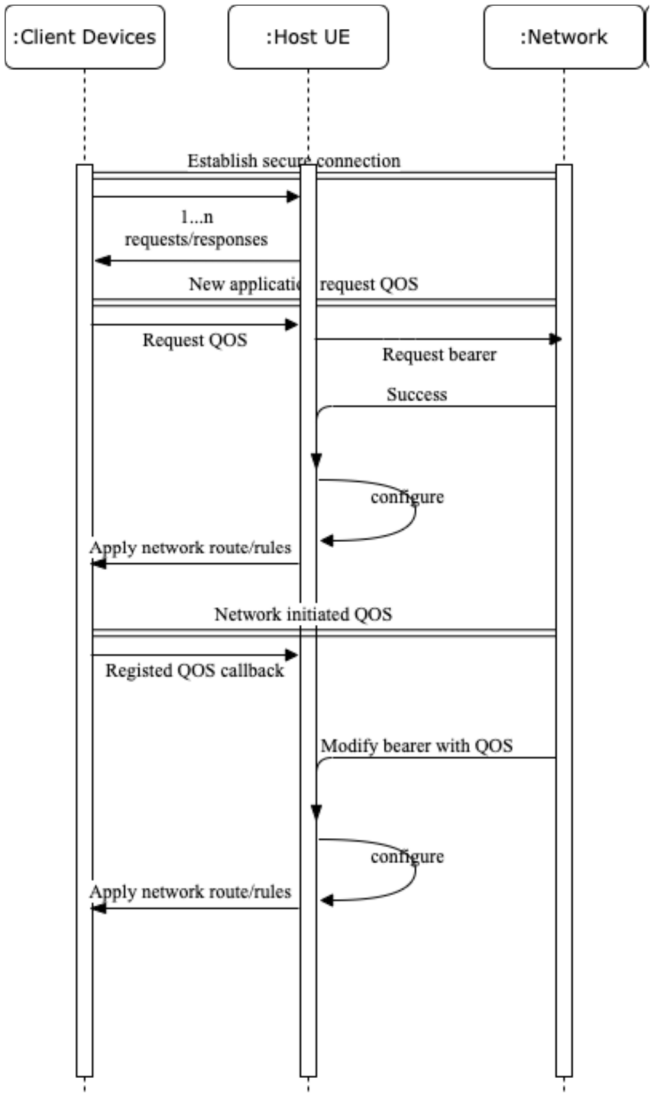

FIG. 2

Turning to FIG. 3, a process for establishing a connection having a requested QoS in response to a request from a tethered device or application is depicted. In response to the tethered device or application requesting a connection having a particular QoS, the QoS access control module determines whether the tethered device or application is to be authenticated. If the tethered device or application is to be authenticated, the QoS access control module authenticates the tethered device or application by checking whether the tethered device or application is authorized to request QoS connections using an authentication protocol (e.g., an extensible

authentication protocol (EAP)). In some cases, tethered devices may only be authorized to request connections having certain QoS and thus a requested QoS may be considered as part of the authorization. In response to determining that the tethered device or application is authorized to request the connection, the QoS access control module may establish a network route, coordinate with other modules on the host device to establish rules to control how the tethered device or application accesses the connection, or both. Subsequently, the QoS access control module may cause a secure connection (e.g., a transport layer security (TLS) connection) to be established between the tethered device and the host device. Further, the QoS access control module may cause the host device to establish a connection to the network having the requested QoS properties. As described above, the QoS access control module may communicate with the tethered device or application via the secure connection to notify the tethered device or application of the result of the QoS request.

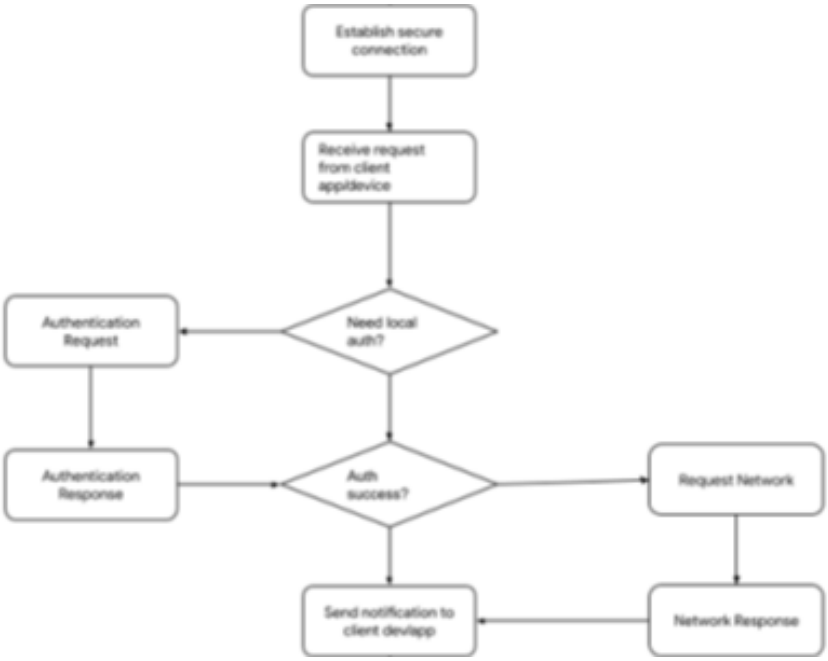

FIG. 3

References

1. S. Tartarelli and G. Nunzi, "QoS Management and Congestion Control in Wireless Hotspots," 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006, 2006, pp. 95-105, doi: 10.1109/NOMS.2006.1687542.
2. Host-based quality of service for wireless communications. US Patent Application Publication No. 20090067372. Filed September 3, 2008.
3. Tethering parameters for a tethering connection. US Patent Application Publication No. 20160007394. Filed July 1, 2014.
4. Processing method and device as well as acquisition method and device for security information. CN Patent Publication No. 107094127. Filed February 18, 2016.