June 2023

METHOD TO OPTIMISE E-UTRA AND WIRELESS LOCAL AREA NETWORK (WLAN) HANDOVERS

Jis Abraham

Hajimulla Shajahaan

METHOD TO OPTIMISE E-UTRA AND WIRELESS LOCAL AREA NETWORK (WLAN) HANDOVERS

AUTHORS:
Jis Abraham
Hajimulla Shajahaan

ABSTRACT

Handovers between wireless local area networks (e.g., Wi-Fi networks) and Evolved UMTS Terrestrial Radio Access (E-UTRA) Radio Access Technology (RAT) networks (e.g., Wi-Fi to E-UTRA or E-UTRA to Wi-Fi) are common scenarios for wireless user equipment. Presented herein are techniques that can avoid, per handover, at least one N4 interaction being performed between a Session Management Function (SMF) and a User Plane Function (UPF), which can help to achieve quicker handovers, can help to avoid data loss during handovers, and can improve SMF and UPF performance by reducing processing of such network functions.

DETAILED DESCRIPTION

For a cellular mobile core network architecture, an SMF or a control-plane Packet Data Network Gateway (PGW-C) triggers the creation of a data tunnel between a UPF and/or a user-plane Serving Gateway (SGW-U) (e.g., for an S5-U tunnel) when a user equipment (UE) attaches to an E-UTRA RAT network. Similarly, the SMF/PGW-C triggers the creation of a data tunnel between a UPF and an evolved Packet Data Gateway (ePDG) (e.g., for an S2b-U tunnel) when a UE attaches to an untrusted WLAN (e.g., Wi-Fi) RAT network. When the UE moves from an untrusted WLAN RAT to an E-UTRA RAT or vice versa, the SMF triggers an N4 modification with a new Packet Detection Rule (PDR) to the UPF for creation of new tunnel for uplink traffic. Old tunnels (e.g., in the old RAT) are deleted once the data path is switched to the new RAT.

Figure 1, below, is a call flow illustrating details for Third Generation Partnership Project (3GPP) standards-based operations performed for an untrusted WLAN to E-UTRA handover (HO) and Figure 2 is a call flow illustrating operations for an E-UTRA to untrusted WLAN HO.

Published by Technical Disclosure Commons, 2023

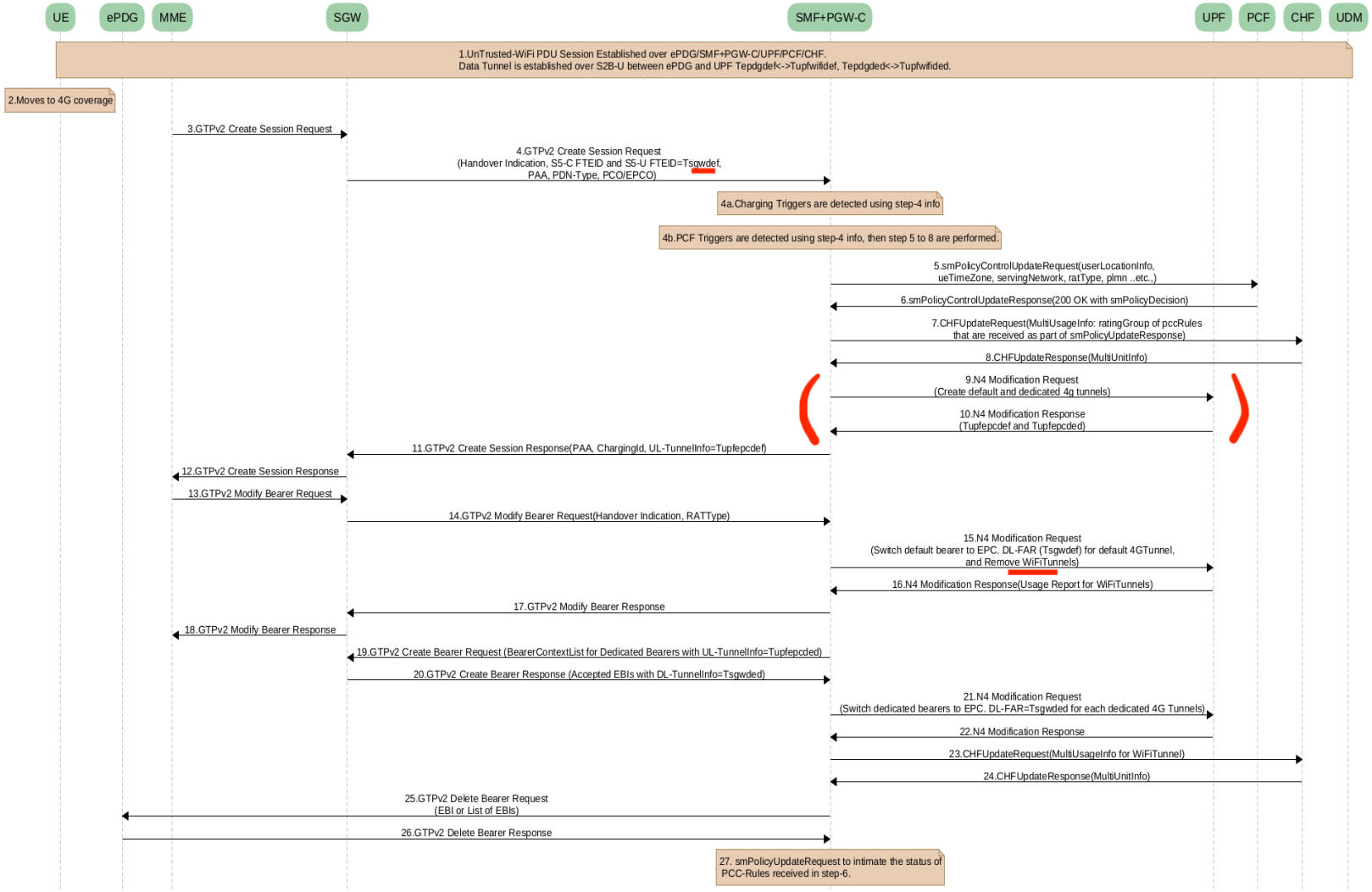

Figure 1: Standards-based Untrusted WLAN to E-UTRA Handover Operations

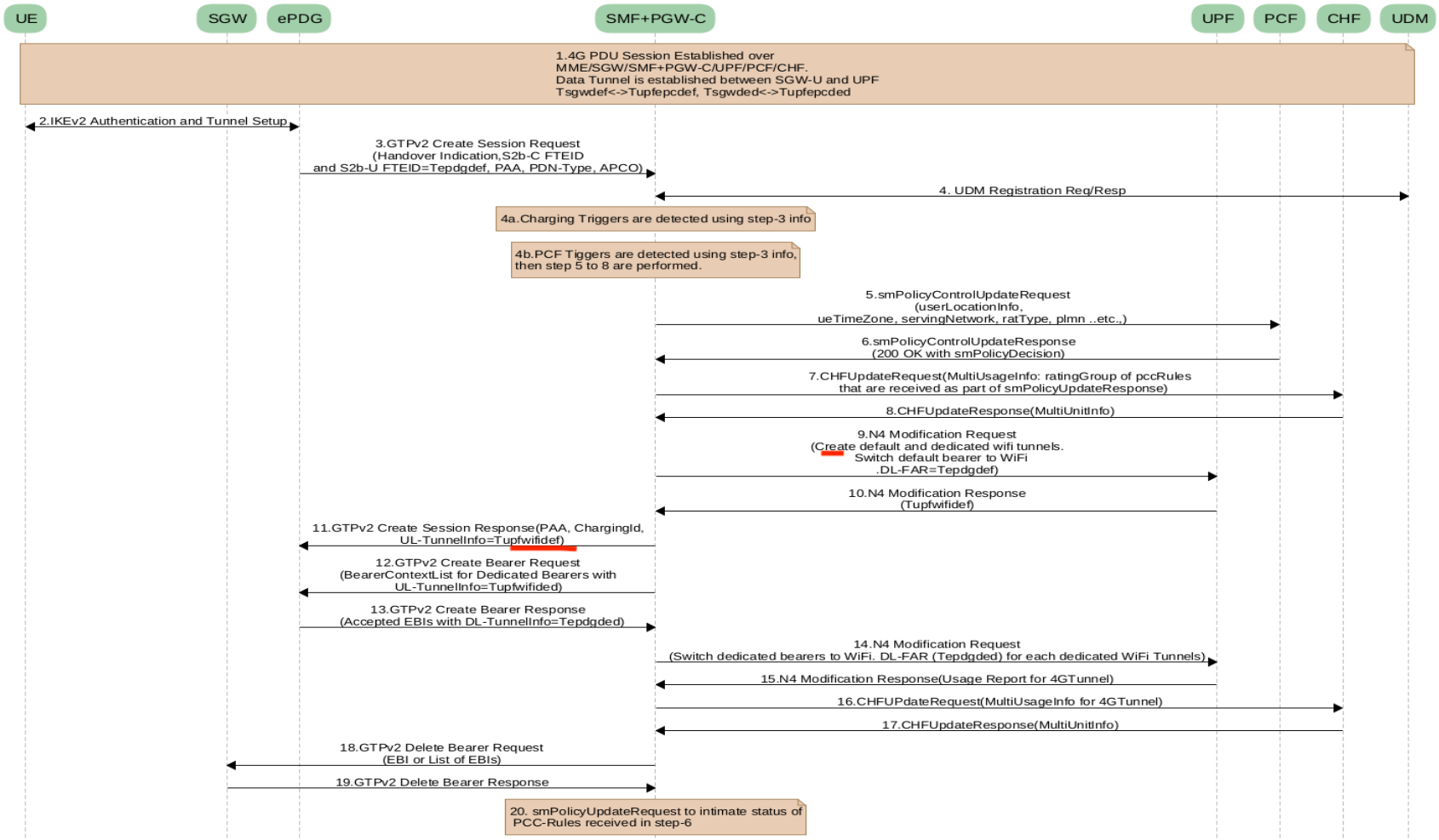

Figure 2: Standards-based E-UTRA to Untrusted WLAN Handover Operations

Under the standards-based procedure for a scenario involving an untrusted WLAN to E-UTRA (e.g., Long-Term Evolution (LTE)) handover, as shown in Figure 1, above, the SMF creates a new uplink PDR upon receiving a create session request from the SGW with a Handover Indication (HI). The UPF then creates a new tunnel and sends a Tunnel Endpoint Identifier (TEID) for the tunnel back to the SMF and the SMF responds to the create session request with the TEID. Thereafter, the SGW switches the uplink traffic to this TEID and the SMF switches the downlink data path to SGW-U upon receiving a modify bearer request from the SGW. Similar operations can be performed for a scenario involving an E-UTRA to untrusted WLAN handover, except that downlink data path switching occurs on receiving a create session request itself (from the ePDG), as shown in Figure 2, above. If dedicated bearers are present in the old RAT, the SMF can trigger the creation of a new tunnel in the new RAT for each of the dedicated bearers. Old tunnels for the dedicated bearers in the old RAT are deleted as part of the handover procedure.

Proposed herein are techniques for optimizing the call flows for untrusted WLAN to E-UTRA and E-UTRA to untrusted WLAN handovers in order to improve (reduce) latency, reduce messaging, and reduce processing load on the SMF and UPF for such handover scenarios.

For example, in accordance with techniques of this proposal, upon receiving a create session request including a HI indication from the new RAT for a handover, the SMF can reuse the UPF TEID (for the GPRS Tunnelling Protocol (GTP) tunnel) created in the old RAT and send the same UPF TEID to the SGW (for an untrusted WLAN to LTE HO scenario) or ePDG (for an LTE to untrusted WLAN HO scenario) in the create session response. Further, the SMF will not trigger an N4 modification request for creation of uplink PDRs for new tunnels; rather, the old PDRs can be reused for the new RAT such that N4 modifications may only be performed for updating the peer TEID for downlink data transfers.

Figure 3, below, is a call flow example illustrating details for operations that can be performed in accordance with techniques of this proposal for an untrusted WLAN to E-UTRA (LTE) HO and Figure 4 is a call flow illustrating example details for operations that can be performed in accordance with techniques of this proposal for an E-UTRA to untrusted WLAN HO.

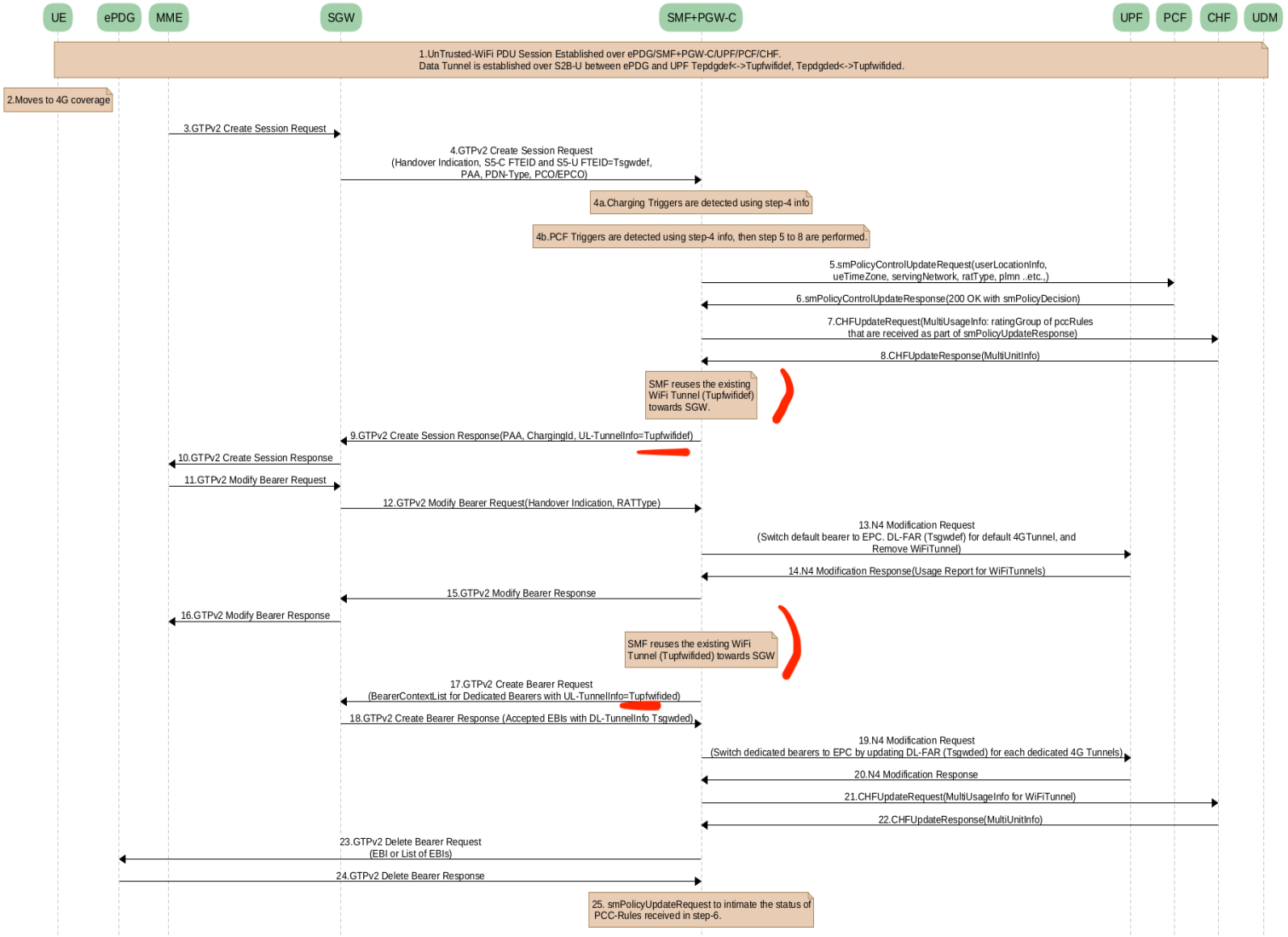

Figure 3: Optimized Untrusted WLAN to E-UTRA Handover Operations

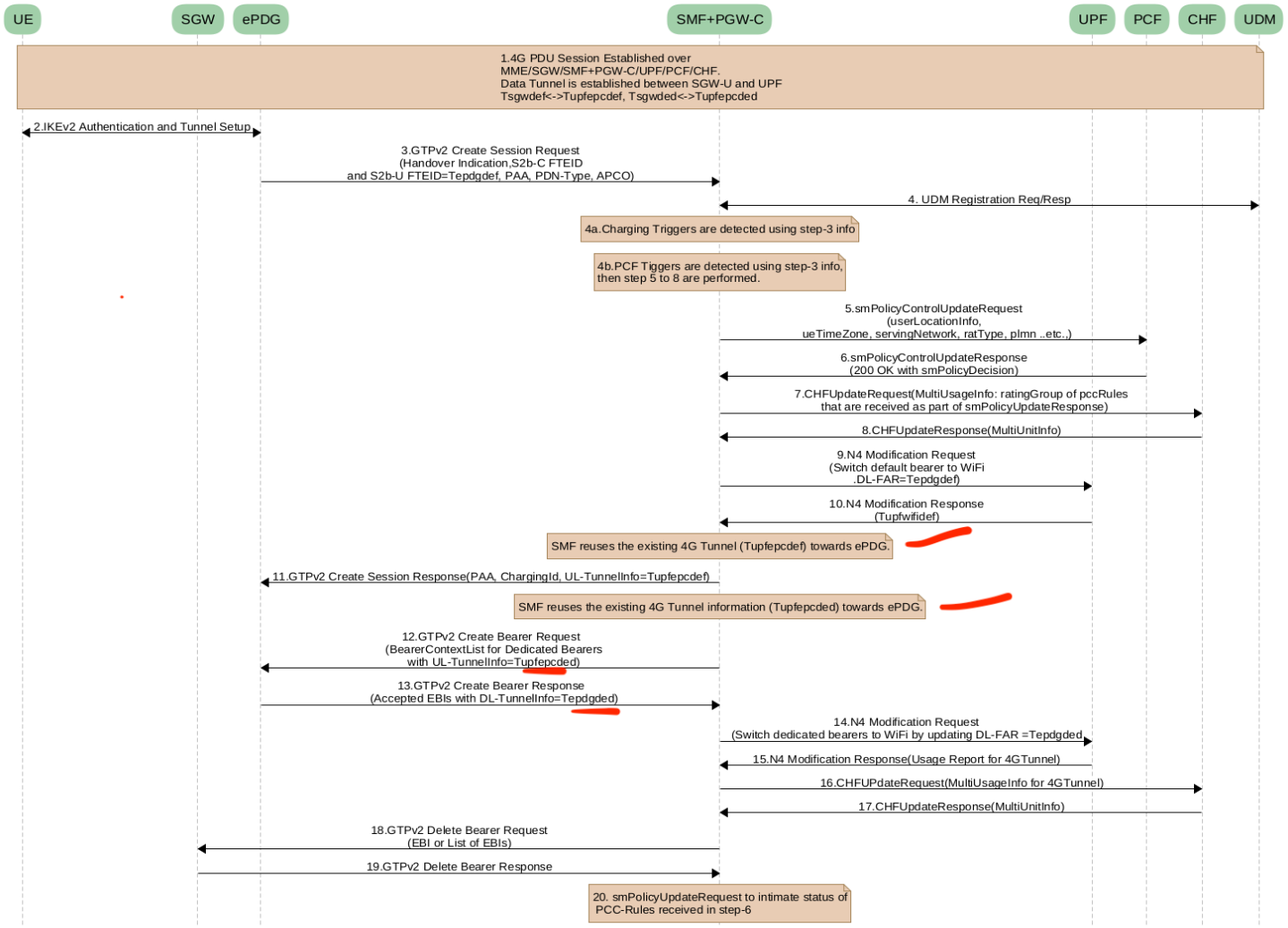

Figure 4: Optimized E-UTRA to Untrusted WLAN Handover Operations

Accordingly, as shown in Figures 3 and 4, techniques as proposed herein may saves one N4 interaction between the SMF and the UPF during every WLAN to LTE handover and may also save extra processing on the SMF and the UPF. Such techniques as proposed herein may also improve the handover execution time and may also avoid any data drops in the downlink path during handover.

In scenarios involving LTE to untrusted WLAN handovers, N4 modification may only be performed for switching the data path to the ePDG. No new PDRs are created and no new tunnel is created in accordance with the optimizations provided by this proposal, which can save processing on the SMF and UPF, can improve handover execution time and can also help to avoid any data drops in the downlink path during handover.