Technical Disclosure Commons

Defensive Publications Series

November 27, 2018

# “FAST TRANSITION” INTO WIRELESS NETWORK USING 5G SECURITY CONTEXT

Indermeet Gandhi

# "FAST TRANSITION" INTO WIRELESS NETWORK USING 5G SECURITY CONTEXT

AUTHORS:
Indermeet Gandhi

## ABSTRACT

Techniques are described for using the concept of 802.11r Fast Base Station Subsystem (BSS) Transition in the security context generated between User Equipment (UE) and a 5G Radio Access Network (RAN) (UE – Next-Generation NodeB (gNB) security context) to provide "Fast Transition" into the wireless network. This eliminates the need for a separate handshaking mechanism, allowing security negotiation and requests for wireless resources to occur in parallel, thereby enabling faster, secure communication through the wireless link.

## DETAILED DESCRIPTION

With 5G and wireless converged architecture, the client station (STA) can associate to both the 5G New Radio (NR) and Wi-Fi® links at the same time with a Next-Generation NodeB (gNB) performing the control plane anchoring.

After the client associates to the Wireless Local Area Network (WLAN) Access Point (AP), it needs to perform the four-way handshake for securing communication in the Wi-Fi domain.

The separate four-way handshake is an overhead for clients running delay-sensitive applications such as voice and video.

In regular movement of the User Equipment (UE) to Wi-Fi coverage, this would mean exchange of 802.11 Authentication Request/Response and 802.11 Association Request/Response followed by the four-way handshake to unblock dot1x security port for successful (secure) session and data exchange.

Techniques described herein involve applying the concept of 802.11r Fast Base Station Subsystem (BSS) Transition to the security context generated between a UE and 5G Radio Access Network (RAN) (UE - gNB security context) and using it to provide "Fast Transition" into the wireless network.

This eliminates the need for a separate handshaking mechanism, allowing security negotiation and requests for wireless resources to occur in parallel, thereby enabling faster secure communication through the wireless link.

Using the following steps, the initial handshake with the new AP may be performed even before the client associates to the target AP using the 5G-UE cellular security key.

1. The NG RAN base station (gNB or ng-eNB) derives the UE security key based on $K_{gNB}$ and the counter.
2. The gNB or Next Generation Evolved Node B (ng-eNB) sends the UE security key to the WLAN infrastructure - WLC and AP over Xw interface.
3. In another embodiment, the gNB exchanges the UE security to the WLAN infrastructure through a RAN controller (anchor) via an Application Programming Interface (API). In a variant, the RAN controller may be a Software Defined Networking (SDN) controller or Software Defined Spectrum Controller (SDSC).
4. In one embodiment, the 5G UE derives the same security key autonomously based on the counter received from the gNB in Resource Reservation Control (RRC) signaling and its own $K_{gNB}$.
5. In another embodiment, the 5G UE obtains the security key from the gNB or ng-eNB directly in the RRC signaling.
6. The 5G client uses the 5G UE security key as a Pairwise Master Key (PMK) by initializing the PMK Security Association (PMKSA). To use the key as PMK, the UE may initialize the PMKSA with a PMK Identifier (PMKID) set to Truncate-128(HMAC-SHA-256(PMK, “PMK Name” || AA || SPA)), where AA = WLAN AP MAC address and SPA = UE MAC address.
7. The AP may be enhanced to advertise its support for “Fast Transition” into the wireless network using the 5G UE security context through a subfield in existing Fast BSS Transition Information Element (IE). Optionally, this may be adaptive (e.g., for known client infrastructures this may be automatically set to true without advertisement for example for preferred vendors).

Leveraging 802.11r principles to achieve “Fast Transition” in parallel during the WLAN resource allocation, the following two “Fast Transition” methods may be used. The first is over the 5G NR, and the second is over the Wi-Fi radio.

The first method allows the UE (STA) to connect to the target AP using a “Fast Transition” Action Frame and “Fast Transition” (Re)Association via the 5G RAN. “Fast Transition” key hierarchies are derived from the PMK (generated from the UE - 5G security context). In this method, the RRC message is enhanced to transport the 802.11 “Fast Transition” Action Frame (“Fast Transition” Request) from the client over the 5G NR RRC signaling.

The 5G RAN function may be enhanced to send the 802.11 FT Action Frame over the Xw interface to the Wireless LAN Controller (WLC) / AP as a transparent container. In another embodiment, the 5G RAN function may exchange the 802.11 “Fast Transition” Action Frame via the RAN controller (e.g., SDN controller, 5G-Wi-Fi Spectrum Manager, etc.). The WLC/AP may be enhanced to send the Action Frame “Fast Transition” Response over the Xw interface towards the 5G RAN.

In another embodiment, the 5G RAN function and WLC/AP may exchange the 802.11 FT Action Frame (Req/Resp) via a RAN controller (e.g., SDN controller, 5G-Wi-Fi Spectrum Manager, etc.). The 5G gNB transports the “Fast Transition” Response to the client in RRC signaling as a transparent container. The STA then starts the “Association” towards the target AP to complete Fast Association - (Re)Association Req/Resp - and further communication uses security keys established through the aforementioned steps (Pairwise Transient Key (PTK) and Group Temporal Key (GTK) keys are generated) over the radio link. Thus, an explicit four-way handshake is avoided. The dot1x security port is unblocked leading to successful (secure) session and data exchange

In the second method, a “Fast Transition” Authentication Request is sent over the air to the target AP after the FT key hierarchies are derived from the PMK (from step 6 above). The 802.11 Association Request following the “Fast Transition” Authentication Req/Resp is enhanced to participate in the Fast Association procedure (generating PTK and GTK keys) helping in completing the four-way handshake in a parallel manner.

The STA sends the target AP a “Fast Transition” Authentication-Request (FTAA, 0, RSNIE[PMKR0Name], MDIE,FTIE[SNonce, R0KH-ID]). The target AP sends the STA a “Fast Transition” Authentication-Response (FTAA, Status, RSNIE[PMKR0Name], MDIE,FTIE[ANonce, SNonce, R1KH-ID, R0KH-ID]). The STA sends the target AP a (Re)Association Request. The target AP sends the STA a (Re)Association Response.

Following this, dot1x security port is unblocked leading to successful (secure) session and data exchange.

In summary, techniques are described for using the concept of 802.11r Fast BSS Transition in the security context generated between UE and a 5G RAN (UE – gNB security context) to provide "Fast Transition" into the wireless network. This eliminates the need for a separate handshaking mechanism, allowing security negotiation and requests for wireless resources to occur in parallel, thereby enabling faster, secure communication through the wireless link.