September 2020

ACCESS POINT NAME (APN)/DATA NETWORK NAME (DNN) BASED AUTO-ANCHORING OF FIFTH GENERATION/NEXT GENERATION TRAFFIC IN WI-FI

Vinay Saini

Rajesh I. V

ACCESS POINT NAME (APN)/DATA NETWORK NAME (DNN) BASED AUTO-ANCHORING OF FIFTH GENERATION/NEXT GENERATION TRAFFIC IN WI-FI

AUTHORS:
Vinay Saini
Rajesh I V

ABSTRACT

Private Third Generation Partnership Project (3GPP) Fifth Generation/next Generation (5G/nG) network environments will have a mix of access technologies, such as Wi-Fi6 and 5G/nG Radio Access Network (RAN) technologies. Techniques presented herein provide for the capability to transport and intelligently anchor 5G/nG data using a Wi-Fi system, which may allow for private 5G/nG onboarding utilizing the Wi-Fi system.

DETAILED DESCRIPTION

When a private 5G/nG network is deployed in an industrial or enterprise environment, it is likely that it will have both Wi-Fi® (e.g., Wi-Fi6, etc.) and 5G/nG radio coverage. Further, it is likely that user equipment (UE) operating within such a network will have both 5G/nG and Wi-Fi capabilities and will be allowed to roam between the 5G/nG and Wi-Fi networks. The 5G/nG network will have different Access Point Names (APNs) and/or Data Network Names (DNNs) configured to provide differentiated services and/or to be used for network slicing mappings. In a Wi-Fi network, a different type of Service Set Identifier (SSID) can created to achieve similar behavior, especially for Radio Frequency (RF) settings. However, creating more SSIDs can create problems with high channel utilization and/or interference. As such, there is a need for an intelligent mechanism which can auto-anchor data from UEs when they roam from a 5G/nG radio to Wi-Fi6 using the common SSID.

This proposal provides techniques for dynamic and auto-anchoring of 5G UE traffic once onboarded to the Wi-Fi network. In one instance, techniques proposed may be viewed in the context of a private 5G network in which Enterprise is managing both Wi-Fi6 and a 5G/nG core + RAN. However, it is to be understood that techniques of this proposal may

be applicable to other deployments, such as a hybrid setup in which part of the 5G/nG network is managed by both a service provider (SP) and an Enterprise.

Figure 1, below depicts one example scenario in which APN/DNN configuration and settings are controlled by an Enterprise and may be configured for different use-cases within an Enterprise facility. As an example, a private 5G APN might be set per Plant in a large manufacturing setup. This is a typical requirement/configuration that may be utilized to provide isolation and group-specific plants that may need to share information with each other.

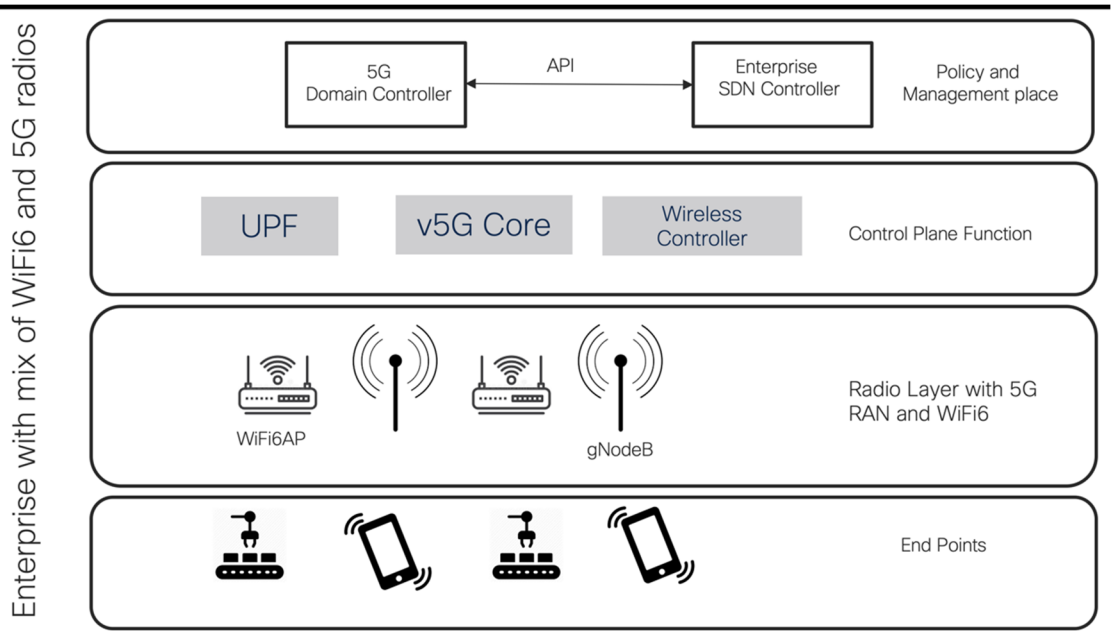

Figure 1

In one example considering a plant use-case, separate DNNs/APNs may be configured such that devices (e.g., programmable logic controllers (PLCs) or the like) connected in Plant A with an APN "Plant A" might need to talk only with specific PLC or Supervisory Control and Data Acquisition (SCADA) systems that are part of a different plant and, hence, served by a separate APN. This may work fine as long as a UE remains on the 5G network. However, once the UE roams to the Wi-Fi network, it is on a common network and the wireless local area network (LAN) controller (WLC) and access point (AP) to which it attaches do not have any information regarding the critical communication path required by the UE. This communication could be local within the plant or a specific destination outside the plant (e.g., in a cloud, specific server, etc.).

Creating multiple SSIDs with a one to one APN/DNN mapping may not be desired in such a case, as it can result in high channel utilization and interference in an environment that likely already has lots of multipath and signal reflections due to the presence of heavy machinery.

Thus, it would be advantageous to establish:

1) Trust between a Wi-Fi6 and private 5G/nG network to allow only specific UE's to have priority access to the Wi-Fi6 network.

2) A mechanism to auto-anchor traffic from a UE to specific destinations within the private 5G/nG network or an external network.

Techniques of this proposal address these issues by establishing trust between a 5G/nG network and a Wi-Fi network at two levels. When considering a plant use-case, as shown in Figure 2 below, for example, trust can be established between Wi-Fi AP groups serving a plant and a 5G RAN and also between a domain controller for the 5G RAN and a network controller (CTRL) and/or a WLC for the Wi-Fi access network.

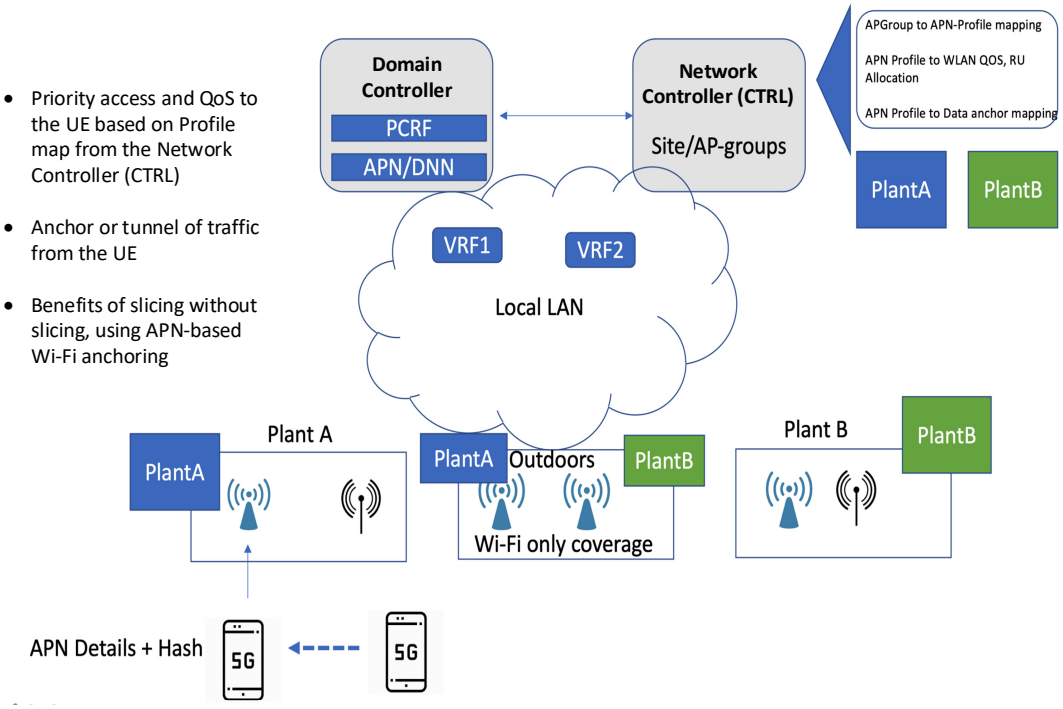

Figure 2

In one example, trust can be established by configuring a common Network Identifier (e.g., a string) on the domain controller and the network controller/WLC. A hash

of this string can be shared with the Wi-Fi6 APs and the 5G RAN that are part of the same area in which roaming and auto-anchoring are to be utilized.

In one instance, the hash can be provided to the UE as part of an association on the 5G network and the UE may share this hash with the Wi-Fi6 AP along with APN/DNN details. The AP can validate the hash value, which ensures it is legitimate UE requiring priority access on the network. This method avoids issues that may arise from an attempt to impersonate a valid UE by just sending APN details.

The same string value can be used between the domain controller and network controller/WLC to establish trust for sharing APN/DNN specific details. For example, the network controller/WLC can fetch the details of the APN/DNN from the domain controller. Information about the traffic anchoring point and/or Quality of Service (QoS) needs per APN/DNN can also be provided by the domain controller. This information is then pushed to the AP groups/sites where there is an overlap of Wi-Fi6 and 5G RAN.

Such operations may provide a critical part of the private 5G/nG techniques of this proposal, which allows priority access and QoS for roaming/offload of the traffic without the need for end to end network slicing. Thus, the techniques of this proposal may reduce dependency on slicing implementations.

Further operations as depicted in Figure 3 below may include the UE adding the details of the DNN/APN in a probe/association request, which can be extracted by the AP and sent to network controller/WLC, which provides awareness to the network controller/WLC regarding the presence of a UE seeking a Wi-Fi connection with specific needs. The APs of the Wi-Fi access network, having the APN/DNN configuration profiles, as discussed above, can send a probe response with a new Information Element (IE) confirming the priority access for configured APNs/DNNs. The UE can then send the hash of the Network Identifier and APN details as part of its association request to the Wi-Fi access network and the AP can validate and onboard the UE to the network. Extensible Authentication Protocol (EAP) Subscriber Identity Module (SIM)/Authentication and Key Agreement (AKA) techniques now known here or hereafter developed may be utilized to complete onboarding for the UE.

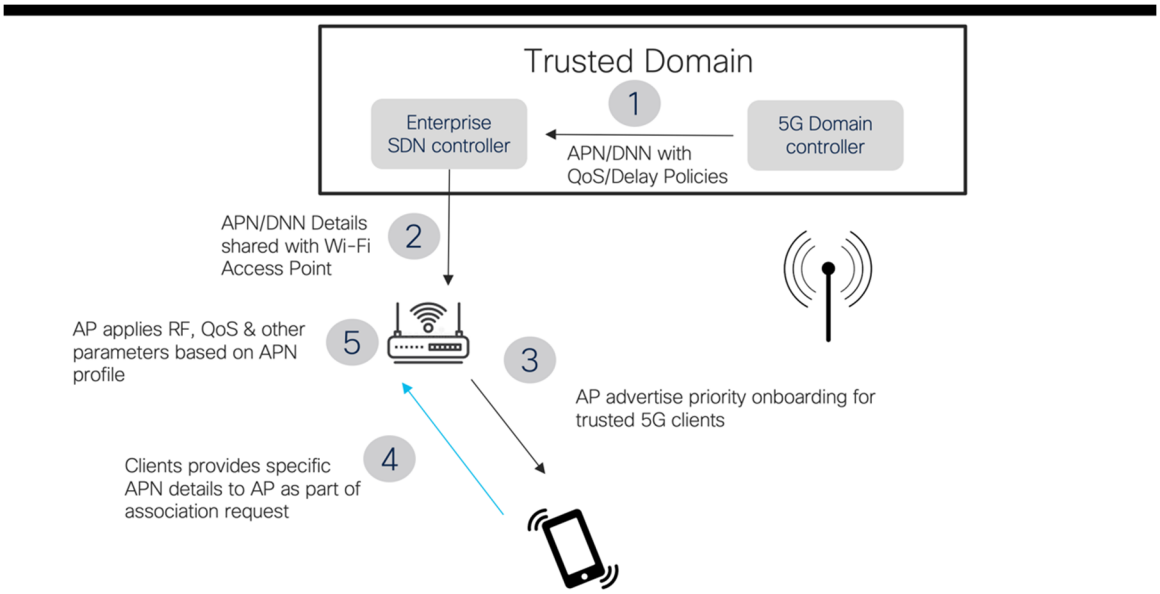

Figure 3

By utilizing techniques of this proposal, access points may provide priority access and/or services to the UE based on the values configured in the profiles (e.g., mapped to APN/DNN). Such priority access/services may include, but not be limited to: allocation of resource units (RUs) to the UE; providing an appropriate QoS level on Wi-Fi and marking the same for related Control and Provisioning of Wireless Access Points (CAPWAP), General Packet Radio Service (GPRS) Tunneling Protocol (GTP), and/or client data; other RF priority mechanism(s) on an AP or AP group can be triggered, such as to facilitate dynamic updating of thresholds for determining whether to demodulate/decode a frame in order to provide better coverage to UEs in marginal coverage; beamforming; and/or the like.

Thus, traffic from a UE that has roamed from the trusted 5G RAN will be auto-anchored based on the value of the profile, which may include, but not be limited to: an AP creating a GTP tunnel to a specific destination based on an agreement between the network controller/WLC and the domain controller for specific traffic of a client; an AP creating an anchor tunnel to another WLC in the demilitarized zone (DMZ); creating an AP/WLC tunnel to a specific server or virtual private network (VPN) gateway; and/or the like.

In summary, techniques herein may provide capabilities to transport and intelligently anchor 5G/nG data using a Wi-Fi system, which may allow for private 5G/nG onboarding utilizing the Wi-Fi system.