May 2023

INDICATIONS FOR SIGNALLING THE PRESENCE OF A PRIVATE 5G NETWORK

Roberta Maglione

Gioacchino Castorio

Suresh Krishnan

Josh Halley

Neha Pradeep

INDICATIONS FOR SIGNALLING THE PRESENCE OF A PRIVATE 5G NETWORK

AUTHORS:
Roberta Maglione
Gioacchino Castorio
Suresh Krishnan
Josh Halley
Neha Pradeep

ABSTRACT

Private 3rd Generation Partnership Project (3GPP) fifth-generation (5G), or Private 5G (P5G), networks are local networks or local area networks (LANs) that are built using 3GPP 5G wireless technology to carry traffic within a specified area, such as within an organization, on a campus, or within an industrial space. A growing number of enterprise and public sector companies are considering building their own P5G networks to address their need for clean spectrum, high bandwidth, low latency, higher availability, and increased visibility. With the introduction of P5G networks, there may be scenarios where both Wi-Fi and P5G networks are present in the same area. When both technologies are available in the same location, current User Equipments (UEs) are designed and configured to prefer the Wi-Fi network for data connectivity. However, there are circumstances that would benefit from the use of P5G connectivity instead of a Wi-Fi network. Techniques are presented herein that support three new mechanisms to inform a UE about the presence of a P5G network and list the services that could benefit from using such media access instead of Wi-Fi when the UE enters the P5G network coverage area. The first mechanism is based on Bluetooth Low Energy (BLE) beacons broadcasted by Wi-Fi access points (APs), the second mechanism leverages stand-alone BLE tags, while the third mechanism employs Internet Protocol version 6 (IPv6) router advertisement (RA) options. The different mechanisms require minimal changes to existing devices, as the underlying technologies that are used are already implemented on both commercially available access points (APs) and UEs. In addition, such mechanisms provide several benefits in terms of power savings and the possibility of immediately transitioning to a P5G network when coverage is available.

DETAILED DESCRIPTION

Private 3rd Generation Partnership Project (3GPP) fifth-generation (5G), or P5G, networks are local networks, or local area networks (LANs), that are built using 3GPP 5G wireless technology to carry traffic within a specified area, such as within an organization, on a campus, or within an industrial space. A growing number of enterprise and public sector companies are considering building their own P5G networks to address their need for clean spectrum, high bandwidth, low latency, higher availability, and increased visibility. Such organizations include manufacturing concerns, ports, airports, stadiums, healthcare facilities, transportation businesses, hospitality establishments, and entities in other industrial sectors.

The radio spectrum that is used for P5G networks may vary depending upon the use case and on the country. For instance, P5G networks in the United States employ the Citizens Broadband Radio Service (CBRS) spectrum. While other countries allow different frequency bands, some countries have not yet allocated any spectrum for P5G networks. Up to this point, the most common technology that has been used to provide indoor or outdoor (in limited or restricted areas) connectivity is Wi-Fi.

With the introduction of P5G networks, scenarios may arise where a P5G network may be deployed alongside a Wi-Fi network in the same area. When this happens, a User Equipment (UE) is currently designed and configured to prefer the Wi-Fi network for data connectivity. However, new services requiring ultra-low latency or higher bandwidth would benefit from using P5G connectivity instead of a Wi-Fi network.

Currently, a UE must continuously scan a specific range of spectrum bands for which it has been provisioned (through, for example, being associated to a Subscriber Identity Module (SIM)) in order to learn about the presence of a P5G network to which it could request to attach. Such a process of continuous frequency scanning consumes power and reduces the UE's battery life.

To address the problem that was described above, techniques are presented herein that support mechanisms that may be employed to inform a UE about the availability or presence of a P5G network. Aspects of the presented techniques inform a UE, when the UE enters a P5G network coverage area, of the services that could benefit from using such media access instead of Wi-Fi connectivity.

The presented techniques signal the availability and the capabilities of a P5G network using one of three different mechanisms, each of which will be briefly introduced below and then described and illustrated later in the instant narrative.

The first mechanism encompasses Bluetooth Low Energy (BLE) beacons that are broadcast by Wi-Fi access points (APs) in the coverage area of a P5G network. A second mechanism encompasses BLE beacons that are advertised by standalone beaconing devices called BLE tags. A third mechanism encompasses Internet Protocol version 6 (IPv6) router advertisements (RAs) that are sent by a first hop router.

For the first and third mechanisms, when a UE enters an area that is covered by both Wi-Fi and P5G networks, the UE will first attach to the Wi-Fi network and then it will obtain information about the P5G network, either from a remote server or a local cache, using the network identifiers that are embedded in the BLE beacons or IPv6 RAs. After receiving such information, the UE (which was preconfigured to detach from the Wi-Fi network) can initiate the procedure to connect to the P5G environment.

The next portion of the instant narrative discusses the first mechanism, which, as introduced above, employs BLE beacon advertisements.

BLE is a form of wireless communication that is designed specifically for short-range communication. BLE beacons may be used to repeatedly transmit the same protocol data unit (PDU) in a region around the BLE tag that is transmitting them. The techniques presented herein leverage this behavior by allowing a UE to determine when it enters a coverage region and develop an estimate of its proximity to a beaconing tag. The beacons may be used as dedicated beaconing channels for a P5G network.

BLE operates in the 2.4 gigahertz (GHz) industrial, scientific and medical (ISM) radio band, which does not typically require special licensing, by splitting the band into 40 channels, each channel having two megahertz (MHz) of bandwidth. The beacons are the payload of BLE advertisement frames, which are broadcast periodically (e.g., every 20 milliseconds (ms) to 10.24 seconds) on channels that, by design, do not overlap with Wi-Fi channels. Furthermore, BLE employs a frequency hopping (FH) technique.

Figure 1, below, presents the PDU for one popular BLE beacon.

Prefix (9 bytes)	**UUID** (16 bytes)	**Major Number** (2 bytes)	**Minor Number** (2 bytes)	**TX Power** (1 byte)

Figure 1: Protocol Data Unit

As depicted in Figure 1, above, the PDU comprises five fields. A nine-byte Prefix field contains a fixed value that identifies the specific BLE beacon. A 16 byte universally unique identifier (UUID) field contains a value that is usually leveraged to single out a specific beacon service among neighboring ones in the same area. A two-byte Major Number field and a two-byte Minor Number field are used to hierarchically segment and distinguish areas within the same location. A one-byte signal (e.g., TX) power field contains a received signal strength indicator (RSSI) value that may be expected when a receiver is one meter away from the tag and which may be used to perform distance estimation between a client and the tag.

A UE may be configured to react, when one or more beacons are observed, by retrieving the P5G network parameters for the location. The UE may fetch the information from a remote server, assuming the UE has network connectivity through either a public cellular network or the Wi-Fi network, by using the triplet (UUID, Major Number, and Minor Number) to uniquely identify its current location. Once the UE establishes a connection to the network (through either 5G connectivity or any other access technologies) the UE may cache the information in its local memory. As a prerequisite, the techniques presented herein assume that a UE knows the set of valid UUIDs for which it should react and a secret seed S0 so that the UUIDs may be periodically updated according to the following formula:

$$S_n = \quad hashUUID_p, \quad S_0$$

$$UUID_n = Gen_{uuid} S_n$$

It is important to note that the first mechanism, according to the techniques presented herein, is robust with respect to possible attacks.

A first possible attack encompasses BLE sniffing. Regarding this approach, BLE beacons are broadcast in plain text (i.e., with no encryption) as the information identifying a location would be meaningless to any unauthorized over-the-air recipient. Only the remote server can associate the triplet for any given location with the P5G network parameters (which are never advertised over the air). The information that is exchanged is further described in the following sections of the instant narrative.

A second possible attack encompasses impersonation attacks. Regarding this approach, the first mechanism, according to the techniques presented herein, acknowledges the possible presence of malicious tags that are broadcasting triplets. If an attacker attempts to inject triplet combinations without knowing the current seed, the UE will simply disregard the beacon. The behavior of the UE may be easily modified by changing the responses that are sent by the centralized server when receiving a triplet. The server may include a service profile with a list of services that would benefit from P5G connectivity.

Figure 2, below, presents elements of a call flow for the first mechanism according to the techniques presented herein and reflective of the above discussion regarding the BLE beacon mechanism.

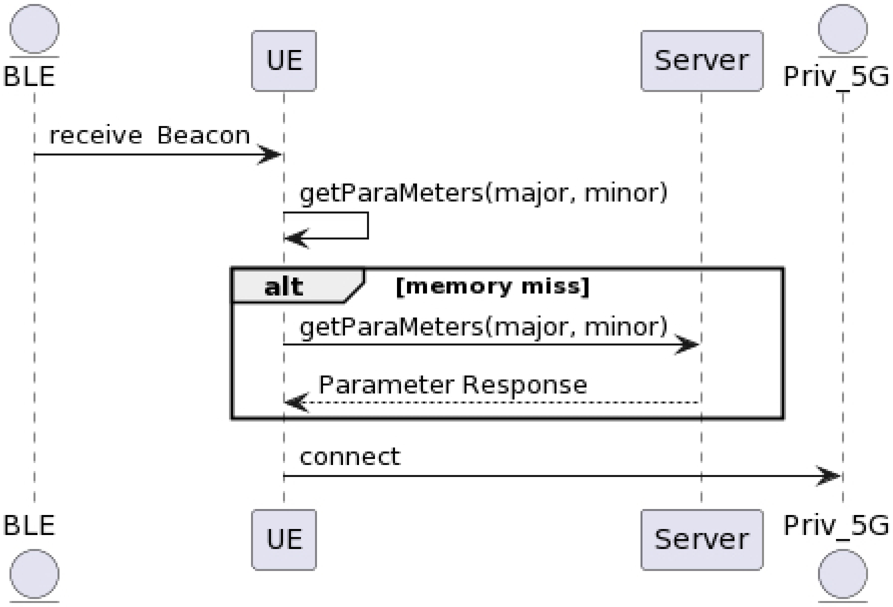


Figure 2: Call Flow

After obtaining information about a P5G network and the available services, a UE may detach from the Wi-Fi network and begin the procedure to connect to the P5G network.

The next portion of the instant narrative discusses the second mechanism, which, as introduced above, employs a BLE beacon mechanism that is advertised by a standalone BLE beacon device having no preexisting network reachability. This mechanism is a variant of the first mechanism, as BLE beacons are sent to an area with no preexisting network reachability before connecting to a P5G Network.

In scenarios where BLE tags are present announcing the beacons with the triplet (UUID, Major Number, and Minor Number) and a UE has no available network reachability either through Wi-Fi coverage or public cellular service, the actions that are described below may be performed by the UE to transition to a P5G network.

First, if the UE has a cache containing the information regarding the broadcast triplets in a previously visited location, where it could in the past connect to a local P5G network, then it may proceed with the operations that were described above for the first mechanism. If the UE receives a beacon matching any of the cached triplets, it may use the stored information to connect to the P5G network. Once the UE obtains network connectivity, it may update the cache to refresh stale entries.

Second, the UE may have a prepopulated cache representing a “connectivity baseline.” If the UE has never connected to any P5G Network, the device may use the baseline cache and attempt to connect to a P5G network and then reach a server to refresh its policy. The same refresh attempt may be executed in the event that the UE obtains network reachability (through, for example, Wi-Fi connectivity).

The use of a BLE beacon-based approach, as described above, offers a number of benefits.

Within the context of the techniques presented herein, BLE beacons were selected because they are already implemented in most of the commercially available UEs, and network equipment vendor APs may act as programmable BLE tags. Consequently, the presented techniques require minimal hardware changes in the infrastructure. The instant approach guarantees security as the identifier triplets have only local validity and contain no information regarding a P5G network’s parameters. Furthermore, the communication between a UE and a remote server should be encrypted, ideally through secure protocols such as the Hypertext Transfer Protocol Secure (HTTPS) protocol.

In the case of a device that is only provisioned with P5G connectivity (i.e., it has no public wireless connectivity), having a mechanism that supports notifying a UE about the presence of a P5G network when the UE enters the network's coverage area allows the device to keep the radio interface off until a notification is received. As BLE was specifically designed to be low power, the proposed solution fosters power saving on the UE, as the device would have a mechanism to be notified about the presence of the P5G network when it enters the coverage area and thus need not continuously scan the frequency spectrum. Additionally, in the event that a UE is already connected to a Wi-Fi network the device may be configured to switch to a P5G network immediately after receiving a beacon. This behavior would allow the UE to leverage the cellular connection without having to go away from the Wi-Fi service area. The procedure used by the UE to attach to a 5G cellular network is described in Section 5.3 of the 3GPP technical specification (TS) 23.501.

As described and illustrated above, the first and second mechanisms leverage the capabilities of BLE beacons. The units that are broadcasting such BLE beacons may be placed within the boundary of a customer's premises in an area with full P5G coverage. Such a placement would guarantee that a UE is able to reach a gNodeB (gNB) upon the first connection and, potentially, have the possibility of moving further away from it without risking connectivity flapping.

Further, the beacons may be broadcast either by network-connected APs or non-connected ones, such as BLE tags. Tags have the advantage of not requiring inline power and may be strategically placed in difficult to reach areas. This scenario would likely be more common in areas such as mining, oil and gas exploration, an automotive environment, and defense settings. In the first case, a UE may consider connecting to both a P5G network and a wireless LAN (WLAN), as advertised with 802.11 compliant beacon frames, potentially offloading the ultra-reliable, low-latency communications (URLLC) traffic to a private cellular network. In the second case, a UE is simply informed that a P5G network is available, and it may connect to it based on its configuration.

In connection with the first and second mechanisms, one existing approach employs Wi-Fi APs sending cellular details in a probe response frame, which according to the standards must follow a probe request. This operation implies a low-level change at both the AP, including injecting new fields (such as, perhaps, capability fields) into the probe responses, and a UE, which would need to interpret such data. BLE beacons come out of the box with the above-described triple (UUID, Major Number, and Minor Number) and clients can natively read these fields (at, for example, an application level).

Furthermore, the BLE-based approach according to the techniques presented herein does not require the client to transmit anything towards an AP. A typical transmit power is usually up to 15 decibels per milliwatt (dBm), although it is important to note that one network equipment vendor's solution may broadcasts at 0 dBm, while a Wi-Fi power level may be up to 30 dBm depending on the regulatory domain. The approach according to the presented techniques is efficient because an AP can broadcast a single beacon at its selected BLE TX Power level while a UE does not need to transmit anything to the AP.

The existing approach that was noted above requires the transmission of at least a Wi-Fi beacon from an AP, a probe request from a UE, and a probe response from the AP. Under such an approach an AP consumes power to transmit a Wi-Fi beacon at 12 dBm (a UE maximum), a UE processes the same, the UE transmits a probe request at 12 dBm, the AP processes the same, and the AP transmits a probe response at 12 dBm.

In contrast, under the BLE-based approach according to the techniques presented herein an AP consumes power to transmit a BLE beacon at 0 dBm and a UE then processes that beacon, translating into to a net energy and processing savings both on the UE and at the AP.

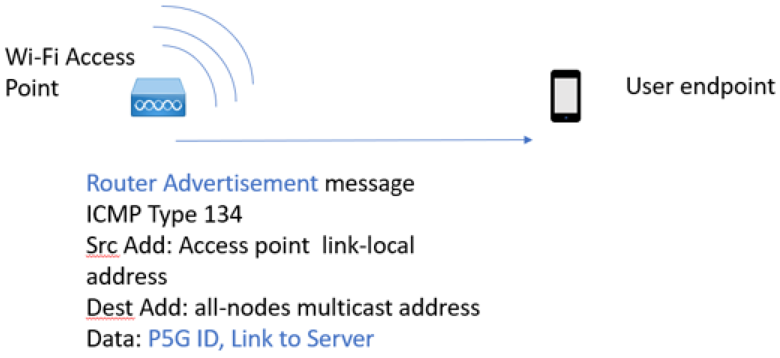
It is important to note that under the first and second mechanisms, the scanning frequency on a UE device for BLE availability and Wi-Fi service takes place based on manufacturer settings. Activities on a mobile handset, for instance, change depending upon the activities of an actual operator. Among other things, when unlocking a phone most operating systems will begin a rescanning of a Wi-Fi network. For BLE, scanning for systems can also take place on demand depending upon the device. As described above, BLE beacons are advertised on the 2.4 GHz ISM radio band and the frequency of the advertisement is sometimes configurable (e.g., one product offering employs an interval of 100 ms as a best effort).

The next portion of the instant narrative discusses the third mechanism, which, as introduced above, employs IPv6 RAs.

In an IPv6 network, RA messages, as specified in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 4861, are used by first hop routers to advertise, either periodically or in response to a router solicitation message, their presence on a link together with various optional configuration parameters.

To solve the problem that was described above, the techniques presented herein employ the RA message that is sent over Wi-Fi by a first hop router to signal the presence of a P5G network (through, for example, a P5G identifier) and identify a link to the provisioning server from which the UE can download additional information (such as a list of services that would benefit from the different communication classes for the exchanged data). The P5G identifier and the link to the server may be signaled inside of the RA message using the PvD option (as defined in RFC 8801) or by other means.

Figure 3, below, presents elements of an exemplary arrangement for the third mechanism according to the techniques presented herein and reflective of the above discussion regarding router advertisement.



Router Advertisement message
ICMP Type 134
Src Add: Access point link-local address
Dest Add: all-nodes multicast address
Data: P5G ID, Link to Server

Figure 3: Exemplary Arrangement

After receiving the above-described information in an RA, a UE (which must be provisioned with a P5G SIM as a prerequisite) may connect to the provisioning server and download additional configuration information. This approach mimics the behavior that was described above in connection with the first (BLE beacon-based) mechanism. After receiving the configuration information from the server, the UE may detach from the Wi-Fi network and begin the procedure to attach to a P5G network.

Regular UEs, without a P5G SIM or configuration, may ignore the information that is received in an RA message and continue using the Wi-Fi connection.

Regarding security considerations, although some solutions such as Internet Protocol Security (IPsec) or Secure Neighbor Discovery (SEND), as defined in RFC 3971, can be used to secure the IPv6 Neighbor Discovery Protocol, in practice actual deployments largely rely on link-layer or physical-layer security mechanisms (such as, for example, the Institute of Electrical and Electronics Engineers (IEEE) standard 802.1x) in conjunction with RA Guard (as defined in RFC 6105).

The use of an RA-based approach, as described above, offers a number of benefits.

Within the context of the techniques presented herein, one of the reasons for selecting RA messages to signal the presence of a P5G network is because those messages are already implemented on all of the IPv6-capable devices. Consequently, the presented techniques require only minimal changes to an existing infrastructure. Devices would only need to be upgraded to support the new RA options that are defined to carry a P5G identifier and the list of available services.

In the case of devices that are provisioned with P5G connectivity, having a mechanism that supports notifying a UE about the presence of a P5G network when the UE enters the coverage area allows the device to keep the radio interface off until a notification is received. This behavior supports the saving of power on the UE.

Additionally, having a mechanism to notify a UE about the presence of a P5G network when it enters the coverage area avoids the need for the device to continuously scan the frequency spectrum as it will be notified when a P5G network becomes available.

Moreover, a UE may be configured to immediately switch to a P5G network and start taking advantage of the benefits that are offered by the P5G network instead of having to wait to lose a Wi-Fi signal.

It is important to note that in connection with the third mechanism, routers may be placed at the perimeter of the area that would define a P5G network radio footprint, allowing for a simplistic association into the P5G network architecture. Based on actual field deployments, many customers today have AP placements at the entry points to their campus, connected to car park entrances, and even deployed within roadside bollards.

In summary, techniques have been presented herein that support three new mechanisms to inform a UE about the presence of a P5G network and list the services that could benefit from using such media access instead of Wi-Fi when the UE enters the P5G network coverage area. The first mechanism is based on BLE beacons, the second mechanism leverages stand alone BLE tags, while the third mechanism employs IPv6 RA options. The different mechanisms require minimal changes to existing devices, as the underlying technologies that are used are already implemented on both commercially available APs and UEs. In addition, such mechanisms provide several benefits in terms of power savings and the possibility of immediately transitioning to a P5G network when coverage is available.