March 2022

PACKET LOSS DETECTOR AND ANALYSER SERVICE IN 5G DEPLOYMENTS

NIRANJAN M M

PACKET LOSS DETECTOR AND ANALYSER SERVICE IN 5G DEPLOYMENTS

AUTHOR:
NIRANJAN M M

ABSTRACT

5G technology offers higher bandwidth and lower delays, hence lower packet loss than previous RAN technologies, but packets loss can happen in the intermediate devices (gNB/routers/Switches/UPF etc.,) while packet travel from source (UE) to the destination (core network) and vice-versa. Packet loss is a very common problem in the networks, and it is very challenging for the network operators to identify where it is getting dropped and what is the reason. Any of the intermediate devices between source and destination could drop the packet due to many reasons viz., Network congestion, Security threats, TTL expiry (hop-limit expiration), unhandled MTU size, ACL drop, Next hop/host/port unreachable, QoS tail drop, Network hardware problems, Software bugs, Overtaxed devices etc., The techniques presented herein defines a method to allow 5G operators to detect the intermediate devices which are dropping packets of the user plane traffic. Also, the technique incorporate method to know the root cause (reason) for the packet drop with some more information that would help the operators to fix the issue.

DETAILED DESCRIPTION

The 5G technology offers higher bandwidth and lower delays, hence lower packet loss than previous technologies, but once packet leaves the source (i.e., device sitting on the edge of the core network, from where internet traffic enters the service provider's core network), it has multiple intermediate devices (e.g., Routers, Switches, UPF, gNB/RAN) to travel before it reaches the destination (e.g., UE) and vice-versa. There is a possibility of packet drop at any intermediate device due to network congestion, faulty hardware, or drivers etc., There are techniques to reduce the packet loss in the network i.e., congestion control mechanisms (like that of TCP), priority-based classification, proactive discarding of the packets before queue is full etc., but no method as such to provide zero packet loss.

Also, considering the Quality-of-Experience (QoE) and SLA (Service Level Agreement), troubleshooting packet loss in the 5G network is utmost important for the operator. Even packet loss causes accountability issues where user is charged for the dropped packets, i.e., when a packet is dropped in intermediate devices, the source which calculates the network usage, does not come to know that the packet is dropped, but the UE is charged for the dropped packets.

In general, packet loss is a very common problem in the networks, and it is very challenging for the network operators to identify where it is getting dropped and what is the reason. Packet loss can be defined as "one or more packets are not reaching their destination after being transmitted from the source across a network (through multiple intermediate devices)".

Any of the intermediate devices between source and destination could drop the packet due to any of the following reasons:

- Network congestion (due to high traffic): This in-turn causes queue-full and subsequent packet drop.
- Security threats:
    - Compromised router/switch can cause packet drop attack or block-hole attack: where-in the cybercriminals hack into the router/switch and instruct it to drop/discard the packets instead of forwarding.
    - DoS attack: where-in the hacker would flood the network with too much traffic, so that even legitimate packets are dropped (due to the existing device limitations viz., tx/rx queue full etc.,).
- TTL expiry (hop-limit expiration): This can cause due to forwarding loop formation.
- Unhandled MTU size: This can cause due to change in MTU between the intermediate devices (bad network design).
- ACL drop: This is due to packet drop in the intermediate device by the ACLs.
- Next hop/host/port unreachable: This can cause due to next hop reachability failure or FIB issue.
- QoS tail drop: This is due to packet drop from the low priority queue to accommodate high priority traffic.
- Network hardware problems: This is due to hardware such as firewall/router/switches would consume a lot of power and can weaken network signals.
- Software bugs: This is due to buggy software running on the network device e.g., packet drop due to programming errors in Forwarding Information Base (FIB) or Routing Information Base (RIB) of the Line cards etc.,
- Overtaxed devices: This is when network is operating at a higher capacity than it was designed to handle.

With the above background, troubleshooting the packet loss problem is multi-folded and very challenging, which includes:

- Detecting an end-to-end packet loss.
- Detecting the intermediate device where the packet loss has happened.
- Detecting the root cause for the packet loss.

There are techniques to detect the intermediate device where the packet loss has happened:

- By having packet counters on ingress and egress of each device on the packet path (for this we need to know the flow that experiences end-to-end packet loss, possibly using source routing such as SRv6). Compare the counters to detect the device which is causing the packet drop.
- Once device is identified, need to debug hardware counters to find out the root cause of the packet drop.
- This is very difficult to achieve and not scalable due to the following reasons:
    - There could be many intermediate devices between source and destination, enabling on all devices is not scalable.
    - There could be many numbers of flows/paths between source and destination, enabling on all flows/paths is not scalable.
    - Manual process of validating the counters is an operational challenge and cannot scale.

- Even automated solution of fetching (pull/push method) the counters from every device and periodically is not scalable.
- In these days, telemetry is one of the ways to troubleshoot the issues, but telemetry information is not helpful and not scalable for troubleshooting packet loss issue due to the following reasons:
  - Telemetry system need to stream the counters periodically.
  - Telemetry streaming periodically consumes more CPU cycles which is required for running other critical services/functionality.
  - Once telemetry information is collected at the server (e.g., network assurance server etc.,) it needs to process the huge amount of telemetry information to detect the packet loss.
  - The interval at which telemetry information streamed is slow (in seconds or 10s of seconds) and hence detecting packet loss also is slower.

None of the existing techniques describe any method to detect packet loss between UE and UPF in 5G network deployments. Existing methods are not sufficient for 5G deployment as the user plane traffic (over N3 interface between gNB and UPF) is encapsulated in GTP-U. Also, the way to identify, forward, process, and reporting of the user plane traffic is available only with the SMF and informed to the UPF over N4 interface over PFCP. Hence, we need techniques which efficiently detect end-to-end packet loss, detect the intermediate device where the packet loss has happened and root cause the reason for packet loss in 5G network deployments.

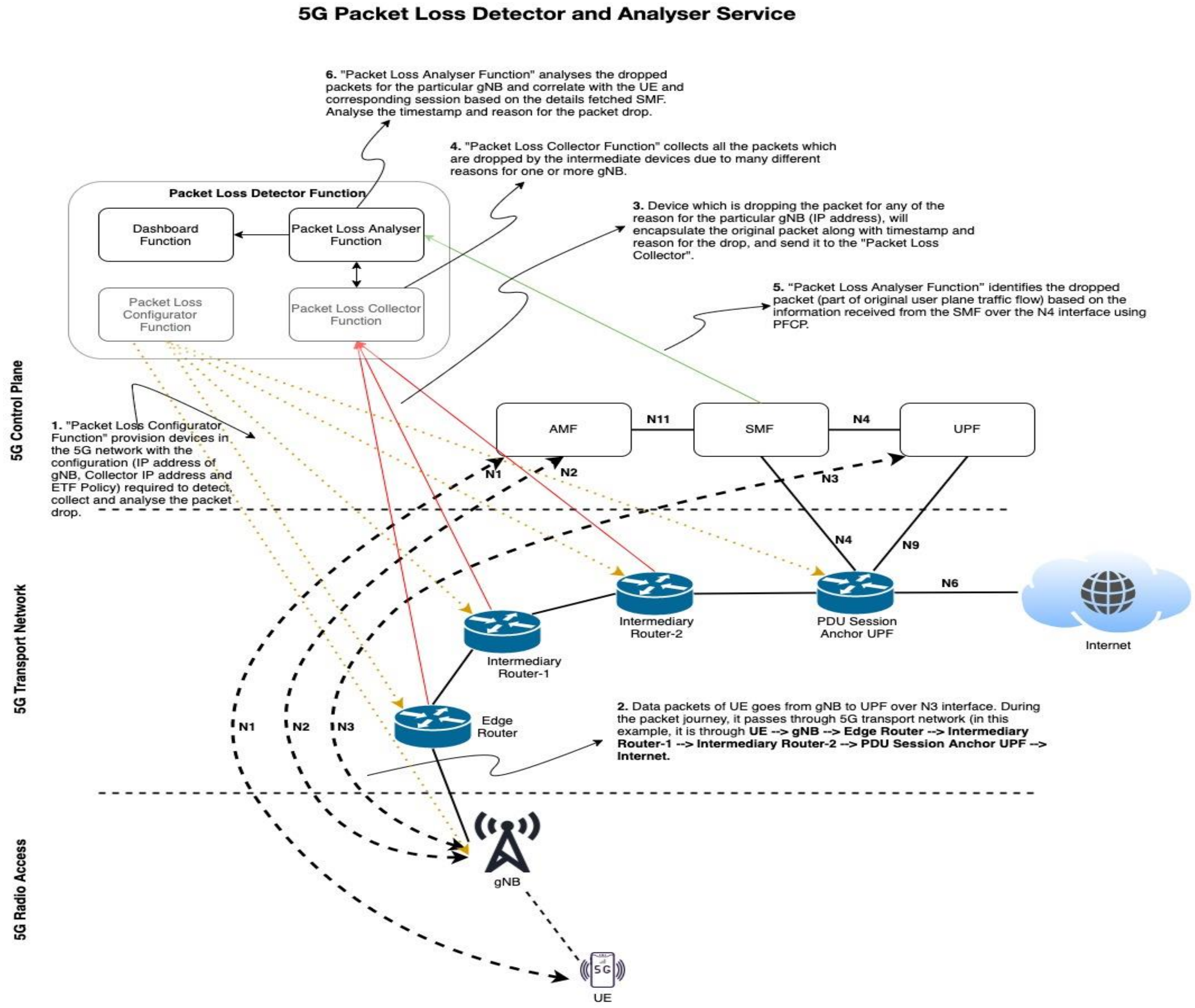
As we know, in the 5G network, N3 interface is used to exchange user data between RAN (gNB) and the User Plane Function (UPF). In other words, N3 interface uses GPRS Tunnelling Protocol for the User Plane (GTP-U) with header extensions for 5G to transport user data between RAN and the core network. And the UPF identifies user plane traffic flow based on the information received from the SMF over the N4 interface, which uses Packet Forwarding Control Protocol (PFCP). PFCP sessions established between SMF and the UPF would define, how packets are identified (Packet Detection Rule [PDR]), forwarded (Forwarding Action Rules [FARs]), processed (Buffering Action Rules [BARs]), marked (QoS Enforcement Rules [QERs]), and reported (Usage Reporting Rules [URRs]). The techniques presented below uses this information for packet loss detection and analysis.

The techniques presented herein defines a method to allow 5G operators to detect the intermediate devices which are dropping packets of the user plane traffic. Also, the technique incorporate method to know the root cause (reason) for the packet drop with some more information that would help the operators to fix the issue. The method is based on the new service running in the 5G control plane called “Packet Loss Detector Function (PLDF)”, which internally has “Packet Loss Configurator”, “Packet Loss Collector” and “Packet Loss Analyser” functionality.

The PLDF is responsible for provisioning all the devices in the 5G network (RAN, Transport and Control Plane) with the required information to detect the packet loss in the network as well as root cause (reason) for the packet drop. It is also responsible for collecting packet drop information from these devices, analyse them and provide the consolidated information about the devices where packet drop has happened along with the reasons for the packet drop to the operator.

- "Packet Loss Configurator Function" provision devices in the 5G network with the configuration required to detect, collect, and analyse the packet drop. Configuration includes IP address of the gNB, Collector IP address and ETF (Encapsulate, Timestamp, Forwarding) Policy.
- As we know, data packets of UE go from gNB to UPF over N3 interface (GTP-U encapsulated). During the packet journey, it passes through 5G transport network. As per the diagram, it is through UE --> gNB --> Edge Router --> Intermediary Router-1 --> Intermediary Router-2 --> PDU Session Anchor UPF --> Internet). Note: For simplicity not considered Intermediary UPF (iUPF) or Branching/Crossover point required for service and session continuity.
- Intermediate device which is dropping the packet for any of the reasons mentioned earlier, will encapsulate the original GTP packet along with timestamp and reason for the drop, and send it to the "Packet Loss Collector Function".
- "Packet Loss Collector Function" collects all the packets which are dropped by the intermediate devices due to many different reasons for the gNB and update the "Packet Loss Analyser Function".
- "Packet Loss Analyser Function" would fetch the details of the gNB, UE and corresponding session information from the SMF. "Packet Loss Analyser Function" identifies the dropped packet (i.e., which was part of original user plane traffic flow) based on the information received from the SMF over the N4 interface using PFCP (this is like, how UPF identifies user plane traffic flow based on information received from the SMF).
- "Packet Loss Analyser Function" analyses the dropped packets for the gNB and correlate with the UE and corresponding PFCP sessions based on the details fetched from SMF. It analyses the timestamp and identify the reason for the packet drop.

Figure-1 describe the overall flow involved in 5G packet loss detector and analyser functionality.



5G Packet Loss Detector and Analyser Service

6. "Packet Loss Analyser Function" analyses the dropped packets for the particular gNB and correlate with the UE and corresponding session based on the details fetched SMF. Analyse the timestamp and reason for the packet drop.

4. "Packet Loss Collector Function" collects all the packets which are dropped by the intermediate devices due to many different reasons for one or more gNB.

3. Device which is dropping the packet for any of the reason for the particular gNB (IP address), will encapsulate the original packet along with timestamp and reason for the drop, and send it to the "Packet Loss Collector".

5. "Packet Loss Analyser Function" identifies the dropped packet (part of original user plane traffic flow) based on the information received from the SMF over the N4 interface using PFCP.

1. "Packet Loss Configurator Function" provision devices in the 5G network with the configuration (IP address of gNB, Collector IP address and ETF Policy) required to detect, collect and analyse the packet drop.

2. Data packets of UE goes from gNB to UPF over N3 interface. During the packet journey, it passes through 5G transport network (in this example, it is through **UE --> gNB --> Edge Router --> Intermediary Router-1 --> Intermediary Router-2 --> PDU Session Anchor UPF --> Internet.**

Figure-1

The techniques presented herein is explained in detail as below:

1. "Packet Loss Detector Function (PLDF)" provisions all the devices in the 5G network with the following configuration:
    a. IP address of the gNB: This is used to identify the packet which is getting dropped (due to any of the reasons mentioned above), by comparing source IP address of the packet with the configured IP address of the gNB.
    b. IP address of Packet Loss Collector: This is used to install a FIB entry on all the intermediate devices and used later to send dropped packet information to the "Packet Loss Collector Function".

   c. ETF (Encapsulate, Timestamp, Forwarding) Policy: This is used to encapsulate the original GTP packet which is getting dropped along with timestamp and reason for the drop, and forwarding to the “Packet Loss Collector Function” running on the PLDF.

2. “Packet Loss Collector Function” receives the encapsulated packet (containing the original GTP packet from the gNB, timestamp, reason for the packet drop) from the device where it is getting dropped.
3. “Packet Loss Analyser Function” processes all the packets dropped on the intermediate device for the gNB (provisioned earlier by PLDF) to provide complete information about, how many packets are dropped, what is the drop rate and the reason for the drop.
4. For each type of packet loss, the “Packet Loss Analyser Function” provides different types of additional information specific to the packet loss.
    a. The devices which are dropping packets because of the FIB lookup issues, it shows the Destination Address (DA) of the packet.
    b. The devices which are dropping packets because of the TTL/HL expiration, it shows the TTL/HL value of the dropped packet. [TTL/HL does not have to be zero, some operators may configure devices to drop packet with TTL/HL less than a given value (using the ACL) based on their network topology.
    c. The devices which are dropping packets because of unhandled MTU sizes (due to don’t fragment or PMTU), it shows the MTU size of the dropped packet.
    d. The devices which are dropping packets at the ingress or egress interface due to queue full or low buffers (especially due to maintaining priority queues for providing QoS etc.,), it shows where packet is dropped (ingress/egress and their queue priority etc.,).
    e. For other types of packet loss, it shows the relevant information to help the operator to fix the issue.
5. Overall, PLDF provides a dashboard which shows the devices that are experiencing the packet loss, reason for the packet loss and some additional information that would help the 5G operator in troubleshooting the issue.

The techniques presented herein define method which helps to find the exact device where packet loss experienced by the customer’s user plane traffic (data packets). With this method, able to identify many different reasons and conditions that can result in packet loss and provides an immediate alert to the operator about the device dropping packets using the automation (by provisioning, collecting, and analysing the packet drop information). Moreover, this method is scalable as it is enabled, only if “packet loss monitoring” is provisioned by the PLDF (by adding IP address of the gNB to the devices in the 5G network) and the ETF behaviour that encapsulates the dropped packets and forwarding them to the “Packet Loss Collector Function” is done in the fast data path of the devices hence does not bring any scaling issue. There is no packet punting or control plane involvement. This method immediate detect any security attack on a device that results in dropping of packets.