CUBRO
NETWORK VISIBILITY

Ebook 2023

5G SA Network Visibility Challenges and Current Alternatives

Content

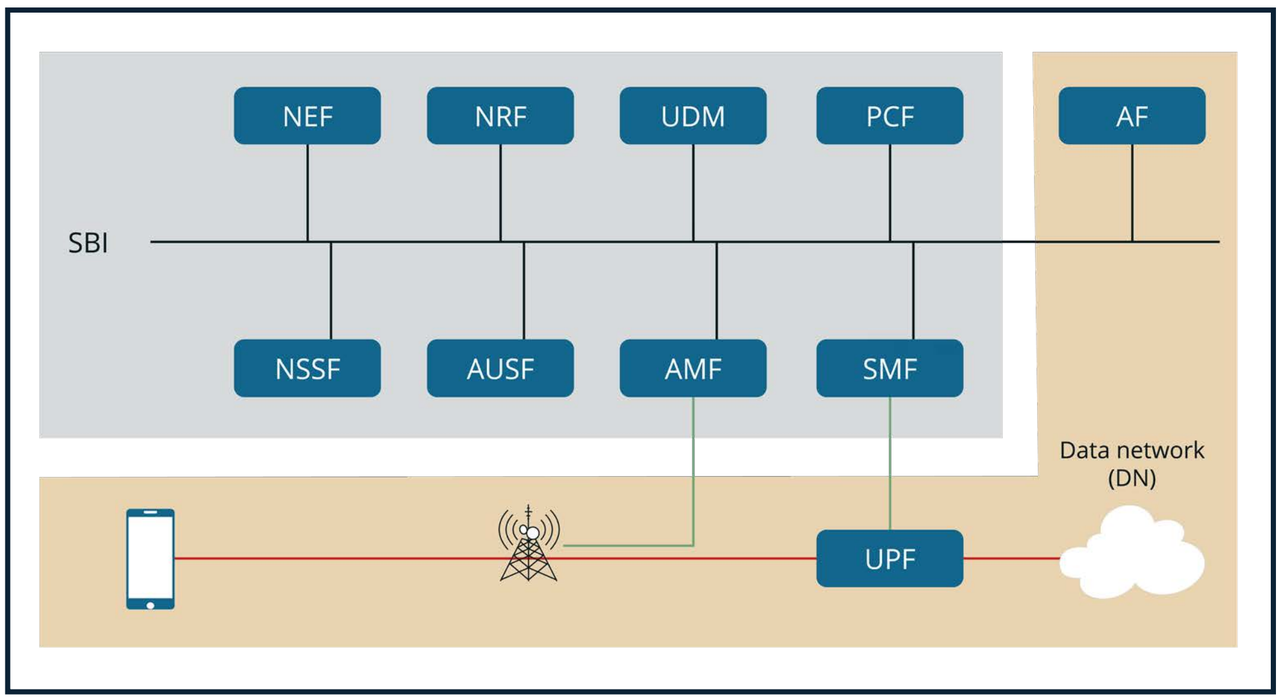
1. Introduction

According to GSMA report '2022 The Mobile Economy' there were 8.3 Bn SIM connections excluding licenced IoT in 2021. The expectation is to have 8.8 Bn connections in 2025. 5G was 8% of those connections in 2022 and the forecasted portion in 2025 is 25%. The same report states that after CSPs started initially their 5G deployments with the non-standalone (NSA), there were 22 commercial 5G standalone (SA) deployments at the end of 2021. STL Partners estimates 66 5G SA networks to be live in 2023.

The importance of the 5G SA lies in the 5G promise of fully supporting enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC) and massive IoT use cases. Technologically 5G SA is a completely new core architecture defined by 3GPP introducing Service Based Architecture (SBA) with cloud-native software approach for building, deploying and managing applications in cloud computing environments.

2. Challenges with 5G SA visibility

In 5G NSA, 4G and previous telecom technology generations it was straightforward to get a copy of the network traffic on packet level, and correlate control- and user-plane traffic with enrichment of application information. This data with unique subscriber identity, in most cases in hashed form, can be used in analytics and monitoring systems to understand hot-spots, used services, bandwidth and user behavior. Many customer experience management systems create insights based on this input.



5G SA

The new 5G SA architecture has created lots of enthusiasm, but with every new technology there are also challenges. There is no lack of open source tools for various purposes such as Metrics (Prometheus), Logs (Grafana Logs), Traces (Jaeger), Flows (Istio, eBPF) and service topology.

While these or similar tools are definitely needed to understand a distributed system, they don't answer the question of subscriber behavior. For example, what are the services that subscribers are using at a certain point in time, at a specific location?

3. Subscriber monitoring solutions

5G SA has made data extraction more complicated. When previously a link could be physically tapped to get a copy of the packets, it is no longer possible with 5G SA. 5G SA CNFs communicate with each other using encrypted HTTP2 messages. There is no 3GPP defined standard for getting mirrored CNF messages in a similar way as in 4G.

One suggested solution to address the monitoring needs was to define **Network Data Analytics Function (NWDAF)**. It was designed to streamline the way core network data is produced and consumed as well as to generate insights and take actions to enhance end-user experience. NWDAF is optional, implemented as a CNF thus not necessarily available in every 5G SA network.

NWDAF has an interface for data collection from CNFs, it does predefined analytics and provides data exposure interface for consumers. It is possible to find several NWDAF success stories, but on the other hand there are concerns about the data availability and granularity, its impact on the network - the CNFs need to report to NWDAF, the cost of introducing NWDAF, integration to CNFs and the alignment to 3GPP standards. The main concern for subscriber experience monitoring is if NWDAF will have high enough granularity to provide information for understanding subscriber behavior. So far the press hasn't published any NWDAF use cases of that kind.

It is possible to use a proxy between all the CNF communication and that is what Service Communication Proxy (SCP) is about. SCP is a CNF, often implemented as part of service mesh using as an example Envoy. While SCP might look like a perfect solution for mirroring traffic, it requires resources and like all proxies it increases latency.

Another principle used by network vendors is to make a copy of the message on the CNF level before the message gets encrypted. These messages are forwarded to a data extractor that streams the data towards recipients. The implementations vary greatly, even on transport protocols - TCP and GRE are used by vendors. Also, some vendors provide the data as HTTP2 while others provide JSON based payload.

Vendors with a more IT centric approach are offering solutions that are purely cloud native offering mirrored messages in decrypted format. The solutions use CNFs to mirror the messages or use eBPF technology to fetch messages before they get encrypted. Those solutions may or may not offer data extraction outside 5G SBI.

At this point of time the visibility is in most cases limited to AMF and SMF only. Multi-vendor CNF doesn't make things any easier from the visibility point of view - it may force the use of several data mirroring solutions which are not the same by design.

4. Conclusion

While 5G SA uses modern Software technology and has received an ample upgrade in security the need to understand subscribers and provide the best possible service is even more important than before. All the solutions described earlier intend to extract detailed information about the messages that can be used for subscriber behavior analysis. Data extraction output needs to be decrypted, but when exposing it outside of SBA, some CSPs find that the data is not secure. Technically it may look a bit strange that first everything is competently encrypted, then the data needs to be exposed in decrypted format, after which it has to be encrypted again for transit and once received it will be again decrypted.

Based on the forecasts 5G SA will gain more popularity in the coming years, but the lack of standardization in terms of decrypted message extraction is slowing down the analytics. Most likely many CSPs and network vendors would be happy to see a standard that would make this simpler without risking the compliance with GDPR and other regulations.