Solution Brief

Mobile Network Operators
Network Security and Analytics

Niagara Networks Integrates R&S®GSRM for 4G/5G Network Visibility

Niagara Networks is collaborating with Rohde & Schwarz to add its R&S®GSRM mobile subscriber awareness software to its Open Visibility Platform (OVP), powered by Intel® processors, for mobile network management.

Mobile data traffic volumes are growing exponentially, a trend that is expected to continue as more high-speed networks come online enabling more video streaming, internet of things (IoT) sensors, new private network use cases and other new applications.

Mobile network operators (MNO) require an advanced set of visibility tools to streamline mobile network operations, perform mobile service optimizations, and increase network security posture. By implementing advanced network packet brokers (NPB), MNOs can easily and efficiently operate, administer and deliver mobile subscriber traffic to multiple cybersecurity and monitoring tools with service scale and flexibility while reducing operational expenses and downtime.

NPBs sit between the production network (connected by switched port analyzer (SPAN) ports or physical and virtual test access ports (TAPs)) and security and analytics tools. The SPAN or TAP forwards data flows to the NPB, which filters them and, using networking policies, directs them to the right security or analytics tool for further processing.

On the eve of the 5G revolution, MNOs are facing challenges that make selecting the right network visibility tool even more important. These challenges include:

- **High data throughput:** As mentioned above, added mobile data makes high throughput to tools important. With more packets and more users, the capacity of visibility tools must be expanded to accommodate the increased data flows and connected users.
- **More tools:** Network analytic and security tools are becoming even more specialized leading to "tool sprawl" as cybersecurity, probes, network performance management, forensics, application performance and other tools need access to network packet streams. NPBs manage this growing number of tools making it easier to add them to the network.
- **Infrastructure diversity:** The old way of building a cellular network using a single-vendor, proprietary radio access network (RAN) system is being challenged by Open RAN* technology. Open RAN uses open interfaces and software running on Intel architecture-based commercial-off-the-shelf (COTS) servers. Open RAN solutions can involve an ecosystem of vendors driving down costs and improving innovation – but also requiring network visibility to facilitate flawless network performance.

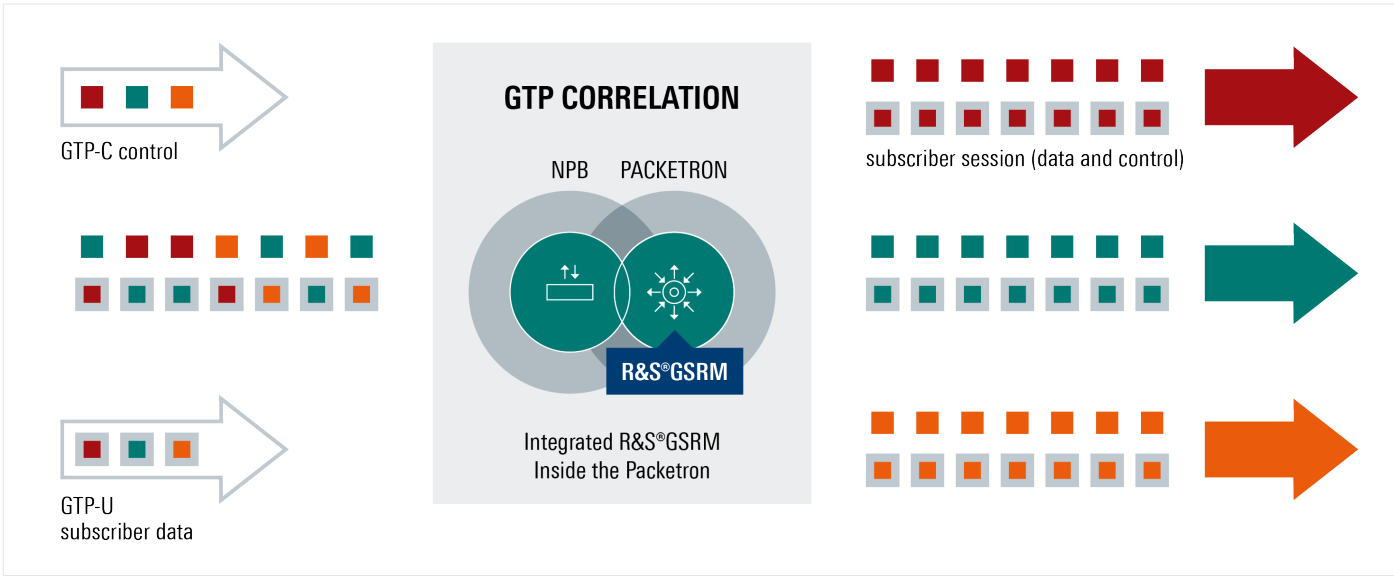

Figure 1. With subscriber awareness, the NPB can keep together all the packets from a data flow so that the tool receives both the data plane and control plane information.

Mobile data flows (see Figure 1) have separate control plane packets that provide essential information on network performance and are transported using the general packet radio service (GPRS) tunneling protocol (GTP). To enable subscriber reconciliation for its high-performance network visibility tool, Niagara Networks has partnered with ipoque, a Rohde & Schwarz company, an Intel® Network Builders ecosystem partner, to integrate its R&S®GSRM mobile subscriber reconciliation software into the Niagara Networks Open Visibility Platform (OVP) to provide proven subscriber-aware network intelligence needed for a complete mobile network visibility solution.

Niagara Networks Open Visibility Platform

Niagara Networks' Open Visibility Platform (OVP) is a software framework for hosting virtualized security and traffic analytics tools and applications. The OVP provides a Deployment Hub that can host any and all virtualized networking or security applications. OVP also manages low-level processing tasks such as TLS decryption, packet de-duplication, data masking and other utility processing – offloading this from the applications and improving their performance.

There are two components to the OVP (see Fig. 2):

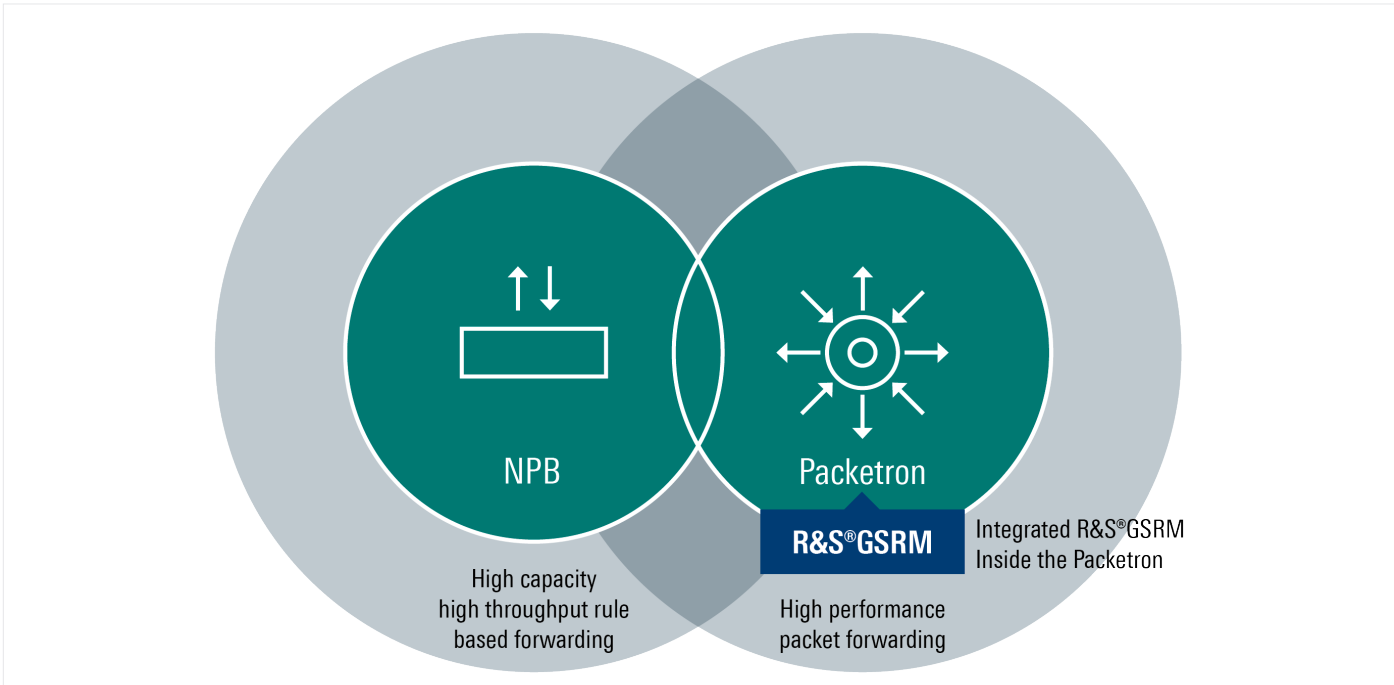

Figure 2. OVP relies on two software components the NPB and Packetron packet processing accelerator.

The packet processing appliance provides packets for test tools by supporting network packet broker (NPB), active/passive TAP or switch bypass functionality. The packet processing appliance sits on the network infrastructure. Typically, this function is deployed in mobile Evolved Packet Core (EPC) to perform an intelligent inspection of the control plane to identify subscriber data sessions and to link them to specific user plane (data) traffic itself.

The Niagara Networks platform defines this process as a mobile subscriber correlation. The packet processing platform is designed for very high performance and reliability and delivers network traffic to in-line or out-of-band security or testing software that is running in the Deployment Hub, or steering function performed to specific cluster of mobile Network Operations Center (NOC) tools.

Packetron* is the processing engine for OVP and is a requirement for any OVP deployment. Packetron provides the packet processing acceleration needed for solution hosting and traffic processing utilities. The software is scalable as additional modules can be added to support more solutions, traffic processing and load. The performance provided by the Packetron acceleration module lets network operations teams deploy a wide selection of network intelligence and OVP applications in order to adapt to their particular deployment needs.

The flexibility of the Deployment Hub means it supports more than open standards-based test tools; it also works with third-party commercial solutions or those that were developed in house by the MNO's DevOps team.

In addition to this hosting capability, OVP delivers intelligent traffic delivery capabilities. Intelligent traffic delivery enables policies that can deliver traffic to the right tool using policies and rules, and combine to create traffic flow for each packet.

Niagara Networks specifies the use of servers based on the Intel® Xeon® processor product family to deliver the performance, core count and memory bandwidth needed for optimal performance. Next-gen Intel Xeon processors bring optimized performance, scale, and efficiency across a broad range of data center, edge, and workstation workloads.

OVP is designed for all networks, but for wireless 4G/5G it needed some specialized software to perform general packet radio service (GPRS) tunneling protocol (GTP) services. To deliver GTP session correlation, Niagara Networks chose the R&S®GSRM.

R&S®GSRM: OEM Software for Subscriber Data Correlation

R&S®GSRM is a software module that can be integrated into third-party frameworks, like OVP, to provide mobile user correlation of control and user plane data on packets flowing through 4G/5G NSA mobile core networks, with a future upgradeable option to 5G SA.

Many security or analytics tools need subscriber awareness because packets from one data flow of a specific Mobile User Equipment will be split randomly to any instance and across multiple tool instances. This reduces the visibility the tools have to control information that contains usage data such as bandwidth consumed, video / audio contents and more. The R&S®GSRM adds intelligence to the NPB to identify which packets are from the same subscriber and so send them only to one tool instance.

Some of the key features of the R&S®GSRM include:

- GTP correlation in real time based on subscriber ID (IMSI)
- Multicore architecture with linear scalability to satisfy high bandwidth demands
- Supports 2G (GSM), 3G (UMTS), 4G LTE and 5G non standalone (NSA) networks including GTPv1 and GTPv2
- Easy-to-use REST APIs
- Configurable input buffer and filter
- Session metadata including cell location and bearer fields
- Support of all standard network interfaces such as Gn, S1U, S11 and S5

Why is GTP So Important

MNOs use general packet radio service (GPRS) tunneling protocol (GTP) to transport data through mobile core networks. It is a key innovation that enables users to roam.

There are GTP standards for both user (GTP-U) and control (GTP-C) traffic that create a tunnel from access networks all the way to the core and within the core. After this the data flow is de-tunneled and routed out to the destination.

When GTB data comes to an NPB to get access to a security tool or load balancer, the NPB must distribute the packets based on packet attributes including data rate, total traffic, bandwidth, or by a logical sequence such as round robin or by stateless hashing.

Sometimes packets from a single data flow can end up on different test tools, which don't have the benefit of all of the control data from all the packets in the data flow. This means the network equipment is blind to total usage. By resolving the subscriber and the packet, the R&S®GSRM adds intelligence into this system that enables the NPB to identify the packets that come from the same subscriber, even though it is tunneled, and intelligently direct that data flow to the right analytics tools.

Subscriber Awareness for 5G SA Networks

The coming years will see the rapid deployments of standalone (SA) 5G networks. Unlike 5G NSA and its 4G predecessors, 5G SA will involve the use of new protocols including the Packet Forwarding Control Function and HTTP/2 to replace GTP.

To deliver subscriber awareness for these protocols, ipoque is developing the 5G Subscriber Revolving Module (R&S®5GSRM), which will be deployed in the 5G core network (5GC) which allow the functionality to be deployed in a 5G standalone network. When available, the R&S®5GSRM will further enhance the suite of visibility tools provided by ipoque, specifically for subscriber awareness. This becomes increasingly critical as 5G service classes such as massive machine-type communications (mMTC) introduce millions of new sessions into the network.

Integrated Solution

The R&S®GSRM enables session-aware functionality in a number of the applications that are hosted in the OVP (see Figs. 2 and 3). In a mobile network, Niagara's Mobile Visibility application (which is part of the OVP offering) provides pre-filtering of the data to identify it as coming from a mobile network then sends it to the R&S®GSRM correlation and processing unit for all the traffic. The subscriber-level traffic identifiers provided by the R&S®GSRM enable MNOs to use the robust filtering options including filtering by location and type of service in addition to the primary subscriber identifiers.

Moreover, advanced sampling techniques and approval lists provide customers with tools to handle high performance deployments efficiently. An integrated configurable buffer helps to provide increased visibility of all subscriber-aware data traffic from the very first packet.

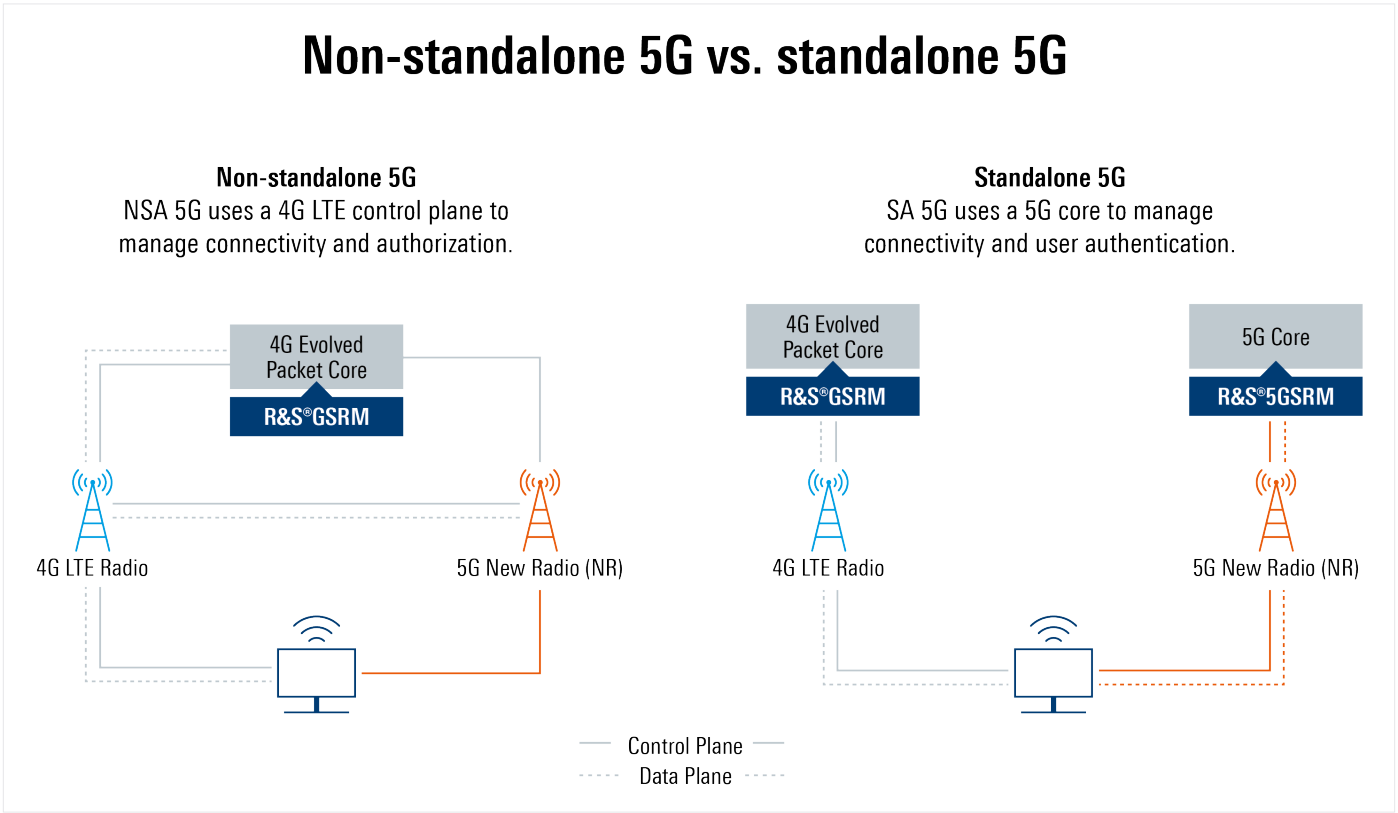

Figure 3. Data flow through a 5G core network.

Conclusion

More mobile network throughput, more network tools and diverse 4G/5G network infrastructure are trends that put a new emphasis on network visibility. Niagara Network's OVP is a network visibility system with built in deployment hub to make it easy to attach new virtualized security tools to the network. With its Packetron software, MNOs can increase packet performance and add additional utility computing functions. By adding ipoque's R&S®GSRM to the OVP, Niagara is able to add the GTP subscriber reconciliation features required for these networks.

Learn More

Niagara Network Open Visibility Platform

Rohde & Schwarz R&S®GSRM Software

Intel® Xeon® Processors

Intel® Network Builders

1022/TM/HO9/PDF ♻Please Recycle 352384-001US